THE PORT AUTHORITY OF NY & NJ

PROCUREMENT DEPARTMENT
ATTN: BID/PROPOSAL CUSTODIAN
TWO MONTGOMERY STREET, 3RD FLOOR
JERSEY CITY, NEW JERSEY 07302

REQUEST FOR PROPOSALS

ISSUE DATE: March 19, 2013

TITLE: SECURITY AUDIT SERVICES AT JOHN F. KENNEDY INTERNATIONAL (JFK), NEWARK LIBERTY INTERNATIONAL (EWR), LAGUARDIA (LGA), TETERBORO (TEB), AND STEWART INTERNATIONAL (SWF) AIRPORTS AND THE WORLD TRADE CENTER (WTC) SITE

RFP NO.: 32792

SUBMIT PROPOSALS NO LATER THAN THE DUE DATE AND TIME TO THE ABOVE ADDRESS

PRE-PROPOSAL MEETINGS/SITE INSPECTIONS:

April 1, 2013 -	**Stewart International Airport (SWF) - 10:30AM**
April 2, 2013 -	**LaGuardia Airport (LGA) - 9:00AM** **John F. Kennedy International Airport (JFK) - 1:00PM**
April 3, 2013 -	**Newark Liberty International Airport (EWR) - 10:00AM**
April 4, 2013 -	**World Trade Center (WTC) - 9:30AM**

QUESTIONS DUE BY:	**April 8, 2013**	**TIME:**	**3:00 P.M.**
PROPOSAL DUE DATE:	**April 18, 2013**	**TIME:**	**2:00 P.M.**

BUYER: LESLEY BROWN
PHONE: (201) 395-3469
FAX: (201) 395-3470
EMAIL: lbrown@panynj.gov

TABLE OF CONTENTS

1. INFORMATION FOR PROPOSERS ON THIS REQUEST FOR PROPSALS 5

A. General Information: The Port Authority of New York and New Jersey 5

B. Brief Summary of Scope of Work 5

C. Deadline for Receipt of Proposals 6

D. Vendor Profile 6

E. Submission of Proposals 6

F. Communications Regarding this RFP 7

G. Proposal Acceptance or Rejection 7

H. Union Jurisdiction 7

I. City Payroll Tax 7

J. Pre-Proposal Meeting(s)/Site Inspection(s) 8

K. Available Documents 9

L. Additional Proposer Information 9

M. Contractor Staff Background Screening 9

2. SCOPE OF WORK 10

3. PROPOSER PREREQUISITES 10

4. FINANCIAL INFORMATION 11

5. EVALUATION CRITERIA AND RANKING 12

6. M/WBE SUBCONTRACTING PROVISIONS 13

7. CERTIFICATION OF RECYCLED MATERIALS PROVISION 15

8. PROPOSAL SUBMISSION REQUIREMENTS 16

A. Letter of Transmittal 16

B. Executive Summary 16

C. Agreement on Terms of Discussion 17

D. Certifications With Respect to the Contractor's Integrity Provisions 17

E. Documentation of Proposer Prerequisites 17

F. Proposal 17

G. Acknowledgement of Addenda 20

H. Acceptance of Standard Contract Terms and Conditions 21

I. M/WBE Plan 21

9. CONDITIONS FOR THE SUBMISSION OF A PROPOSAL 21

A. Changes to this RFP 21
B. Proposal Preparation Costs 21
C. Disclosure of Proposal Contents/Use of Ideas and Materials 21
D. Ownership of Submitted Materials 21
E. Subcontractors 21
F. Conflict of Interest 21
G. Authorized Signature 22
H. References 22
I. Evaluation Procedure and Negotiation 22
J. Taxes and Costs 22
K. Most Advantageous Proposal/No Obligations to Award 22
L. Multiple Contract Awards 23
M. Right to Extend Contract 23
N. Rights of the Port Authority 23
O. No Personal Liability 24

ATTACHMENT A - Agreement on Terms and Discussion

ATTACHMENT B

Part I - Contract Specific Terms And Conditions

Part II - General Contract Provisions

Part III - Cost Proposal Form

ATTACHMENT C - Proposer Reference Form

ATTACHMENT D - M/WBE Participation Plan

ATTACHMENT E - Statement of Subcontractor Payments

ATTACHMENT F - Certified Environmentally Preferable Products/Practices

ATTACHMENT G - Port Authority Information Security Handbook

ATTACHMENT H - Port Authority Customer Care Requirements

ATTACHMENT I - Port Authority Customer Care Manual

ATTACHMENT J - Port Authority Technology Services Department Standards and Guidelines

ATTACHMENT K - Port Authority Technology Services Department System Administration Guide

1. INFORMATION FOR PROPOSERS ON THIS REQUEST FOR PROPOSALS

A. General Information: The Port Authority of New York and New Jersey

The Port Authority of New York and New Jersey (the "Port Authority" or the "Authority") is an agency of the States of New York and New Jersey, created and existing by virtue of the Compact of April 30, 1921, made by and between the two States, and thereafter consented to by the Congress of the United States. It is charged with providing transportation, terminal and other facilities of trade and commerce within the Port District. The Port District comprises and area of about 1,500 square miles in both States, centering about New York Harbor. The Port District includes the Cities of New York and Yonkers in New York State, and the cities of Newark, Jersey City, Bayonne, Hoboken and Elizabeth in the State of New Jersey, and over 200 other municipalities, including all or part of seventeen counties, in the two States. The Port Authority manages and/or operates all of the region's major commercial airports (Newark Liberty International, John F. Kennedy International, Teterboro, LaGuardia and Stewart International Airports), marine terminals in both New Jersey and New York (Port Newark and Elizabeth, Howland Hook and Brooklyn Piers); and its interstate tunnels and bridges (the Lincoln and Holland Tunnels; the George Washington, Bayonne, and Goethals Bridges; and the Outerbridge Crossing), which are vital "Gateways to the Nation."

In addition, the Port Authority operates the Port Authority Bus Terminal in Manhattan, the largest facility of its kind in the world, and the George Washington Bridge and Journal Square Transportation Center bus stations. A key link in interstate commuter travel, the Port Authority also operates the Port Authority Trans-Hudson Corporation (PATH), a rapid rail transit system linking Newark, and the Jersey City and Hoboken waterfronts, with midtown and downtown Manhattan. A number of other key properties are managed by the agency including but not limited to a large satellite communications facility (the Teleport) in Staten Island, and a resource recovery co-generation plant in Newark. Prior to September 11, 2001, the Port Authority's headquarters were located in the World Trade Center, and that complex is still owned and being partially redeveloped by the Authority.

The Port Authority is hereby seeking proposals from qualified firms to provide security audit services as more fully described herein.

B. Brief Summary of Scope of Work

The Port Authority is seeking to enter into a Contract with a qualified firm to provide security audit services at John F. Kennedy International (JFK), Newark Liberty International (EWR), LaGuardia (LGA), Teterboro (TEB), Stewart International (SWF), and the World Trade Center (WTC) Site (collectively the "Facilities"), as more fully set forth in the Attachment B, Part I, of this RFP entitled "Contract Specific Terms and Conditions for the Security Auditing Program." Such services will support airport and airline obligations under Title 49 CFR Part 1542.

Such services will support airport and airline obligations under Title 49 CFR Part 1542. For more information regarding Title 49 CFR Part 1542, please refer to the Electronic Code of Federal Regulations website: http://www.ecfr.gov/cgi-bin/text-idx?tpl=%2Findex.tpl

The contract is expected to commence on or about 12:01 a.m. on August 29, 2013 (said date and time hereinafter sometimes collectively called "the Commencement Date"). The Base Term of this contract is five (5) years. There are two (2) one (1) year option periods

and the Port Authority has the right to extend the base term for an additional one hundred and twenty (120) days.

C. Deadline for Receipt of Proposals
The due date specified on the cover page is the Proposal Due Date. Proposals must be received by 2:00 P.M., Eastern Daylight Saving Time (EDT).

The Port Authority assumes no responsibility for delays caused by any delivery service.

D. Vendor Profile
To ensure maximum opportunities, it is vitally important that Proposers keep their vendor profiles up to date with an appropriate e-mail address, as this will enable their firm to receive timely notice of advertisements, reminders, solicitations and addenda. Proposers may update their vendor profile or register as a Port Authority Vendor by accessing the online registration system at https://panynjprocure.com/VenLogon.asp.

E. Submission of Proposals
One (1) reproducible original (containing original signatures and clearly designated as such) and eleven (11) double-sided copies of the proposal must be submitted on or before the due date and time in accordance with the information on the cover page of this RFP and sent or delivered to the RFP Custodian at the address specified on the cover page. Each copy of the proposal as well as the parcel(s) used for shipping must be conspicuously marked with the Proposer's name and address as well as the Proposer's Vendor Number, if available. In addition, the outside of the package must clearly state the title of this RFP, the number of this RFP and the Proposal Due Date. Failure to properly label proposal submissions may cause a delay in identification, misdirection or disqualification of proposal submissions.

It is necessary to carry valid photo identification when attempting to gain access into the building to hand deliver proposals.

Consistent with environmentally preferable procurement practices, the Port Authority requests all documents submitted to be in a form that can be easily recycled (i.e., no plastic covers or binding) and to provide only supporting literature which directly relates to the proposal being submitted.

F. Communications Regarding this RFP
All communications concerning this RFP should be directed to the Buyer listed on the cover page. All questions regarding this RFP should be submitted in writing to the Buyer at the address or facsimile number listed on the cover page no later than 3:00 p.m. (EDT) on April 8, 2013.

The Buyer is authorized only to direct the attention of prospective Proposers to various portions of this RFP so that they may read and interpret such portions themselves.

Neither the Buyer nor any other employee of the Port Authority is authorized to interpret the provisions of this RFP or give additional information as to its requirements. If interpretation or other information is required, it will be communicated to Proposers by written addenda and such writing shall form a part of this RFP.

G. Proposal Acceptance or Rejection
Acceptance shall be only by mailing to or delivering at the office designated by the Proposer in its proposal, a notice in writing signed by an authorized representative on behalf of the Port Authority specifically stating that the proposal is accepted or by execution of an agreement covering the subject matter of this RFP signed by authorized representatives of the Port Authority and the Proposer. No other act of the Port Authority, its Commissioners, officers, agents, representatives, or employees shall constitute acceptance of a proposal. Rejection of a proposal shall be only by either (a) a notice in writing specifically stating that the proposal is not accepted, signed by an authorized representative of the Port Authority and mailed to or delivered to the Proposer at the office designated in the Proposal, or (b) omission of the Port Authority to accept the proposal within one hundred and eighty (180) days after the Proposal Due Date. No other act of the Port Authority, its Commissioners, officers, agents, representatives or employees shall constitute rejection of a proposal.

H. Union Jurisdiction
Proposers are advised to ascertain whether any union now represented or not represented at the facility will claim jurisdiction over any aspect of the operations to be performed hereunder and their attention is directed to the Section of this RFP entitled "Harmony" included in the "General Contract Provisions" hereunder.

I. City Payroll Tax
Proposers should be aware of the payroll tax imposed by the:

a. City of Newark, New Jersey for services performed in Newark, New Jersey;
b. City of New York, New York for services performed in New York, New York; and
c. City of Yonkers, New York for services performed in Yonkers, New York.
d. City of Newburgh, New York for services performed in Newburgh, New York and
e. Town of New Windsor, New York for services performed in New Windsor, New York.

These taxes, if applicable, are the sole responsibility of the Contractor. Proposers should consult their tax advisors as to the effect, if any, of these taxes. The Port authority provides this notice for informational purposes only and is not responsible for either the imposition or administration of such taxes. The Port Authority exemption set forth in the Paragraph entitled "Tax Exemptions" in the "General Contract Provisions" included herein, does not apply to these taxes.

J. Pre-Proposal Meeting(s)/Site Inspection(s)
The **Pre-Proposal Meetings/Site Inspections** are scheduled as follows:

April 1, 2013:
- Stewart International Airport (SWF) - 10:30AM

April 2, 2013:
- LaGuardia Airport (LGA) - 9:00AM
- John F. Kennedy International Airport (JFK) - 1:00PM

April 3, 2013:

- Newark International Airport (EWR) - 10:00AM

April 4, 2013:

- World Trade Center (WTC) - 9:30AM

Any questions concerning this RFP should be submitted in writing prior to the meeting so that the Port Authority may prepare responses in advance of the meeting. Additional questions may be permitted at the meeting; however, responses may be deferred and provided at a later date by written addenda.

A site inspection allows Proposers to tour and physically inspect the actual site(s) of work prior to the submission of proposals. No questions will be taken during a site inspection.

Attendance is strongly recommended. Information conveyed may be useful to Proposers in preparing their proposals and Proposers not attending assume all risks which may ensue from non-attendance.

Attendees interested in attending should RSVP to Ms. Courtney Fong at cfong@panynj.gov no later than 12 noon (EDT) of the business day preceding the scheduled date(s) to confirm their attendance and/or receive traveling directions.

Maximum two (2) individuals per company are allowed to attend. Two (2) valid forms of photo ID are required with one form being a driver license/state identification card or passport to attend the pre-submittal meeting and facility inspections.

Individuals should RSVP and must include **all** of the following information:

a. Legal First and Last name
b. Company Name
c. Date of Birth
d. Phone Numbers (office and/or cell)
e. Email address
f. Which site inspection(s) he/she will attend

Please note buses may be reserved for the site inspections. Therefore, it is imperative that interested individuals RSVP in advance. Failure to provide complete and correct information may result in individuals being denied attendance.

It is highly recommended attendees arrive thirty (30) minutes prior to the start of the Pre-Proposal Meetings and Site Inspections.

K. Available Documents

The following documents will be made available for reference and examination:

A conformed copy of the existing Security Audit and Training Services Contract, contract # 4600006735.

The above document will be made available for examination at the Park Avenue South location. Contact Ms. Courtney Fong at cfong@panynj.gov Monday through Friday.

Appointments must be made at least twenty four (24) hours in advance of the requested Contract examination date. The contract may not be duplicated or removed from the Park Avenue South facility. The contract may only be viewed between the hours of 8:30 a.m. to 4:00 p.m. Individuals are limited to a one (1) hour contract review period.

The available documents were not prepared for the purpose of providing information for Proposers on this RFP, but they were prepared for other purposes, such as for other contracts or for design purposes for this or other contracts, and they do not form a part of this RFP. The Port Authority makes no representation or guarantee as to, and shall not be responsible for, their accuracy, completeness or pertinence, and, in addition, shall not be responsible for inferences or conclusions drawn therefrom. They are made available to Proposers merely for the purpose of providing them with such information, whether or not such information may be accurate, complete, pertinent or of any value to Proposers.

L. Additional Proposer Information

Prospective Proposers are advised that additional vendor information, including, but not limited to forms, documents and other information, including M/WBE Participation Plan Submission Forms and protest procedures, may be found on the Port Authority website at: http://www.panynj.gov/business-opportunities/become-vendor.html

M. Contractor Staff Background Screening

The Contractor awarded this Contract will be required to have its staff, and any subcontractor's staff working under this Contract, authorize the Authority or its designee to perform background checks. Such authorization shall be in a form acceptable to the Authority. The Contractor (and subcontractor) may also be required to use an organization designated by the Authority to perform the background checks. The cost for said background checks for staff that pass and are granted a credential shall be reimbursable to the Contractor (and its subcontractors) as an out-of-pocket expense as provided herein. Staff that are rejected for a credential for any reason are not reimbursable.

As of January 29, 2007, the Secure Worker Access Consortium (S.W.A.C.) is the only Port Authority approved provider to be used to conduct background screening, except as otherwise required by federal law and/or regulation. Information about S.W.A.C., instructions, corporate enrollment, online applications, and location of processing centers can be found at http://www.secureworker.com, or S.W.A.C. may be contacted directly at (877)522-7922.

2. SCOPE OF WORK

The Contractor shall provide security audit services at Port Authority's Aviation facilities and the WTC Site. Please refer to Attachment B for full description of services required under the Contract.

3. PROPOSER PREREQUISITES

The Port Authority shall only consider proposals from Proposers demonstrating compliance with the following:

A. The Proposer shall have had at least five (5) years of continuous experience immediately prior to the date of the submission of its proposal in the management and operation of a security audit business engaged in providing these services to commercial and industrial accounts under contract.

The Proposer may fulfill this prerequisite if it can demonstrate that the persons or entities owning and controlling the Proposer have had a cumulative total of at least the same number of years and type of direct continuous experience immediately prior to the submission of this proposal as is required of the Proposer, or has owned and controlled other entities which meet the requirement.

B. During the time period stated in (A) above, the Proposer shall demonstrate satisfactory performance of at least one (1) contract for security auditing services, but may be fulfilled by experience in industries other than aviation.

C. The Proposer shall demonstrate that it has earned gross revenues of at least two million five hundred thousand dollars ($2,500,000) for each of the last three (3) fiscal or calendar year(s) from the type of services or products described herein.

In the event a proposal is submitted by a joint venture the foregoing prerequisites will be considered with respect to such Proposal as follows:

With respect to subparagraph (A) and (B) above, the prerequisite will be considered satisfied if the joint venture itself, or any of its participants individually, can meet the requirements. With respect to subparagraph (C), the gross income of the joint venture itself may meet the prerequisites or the gross income of the participants in the joint venture may be considered cumulatively to meet the prerequisite.

If the proposal is submitted by a common law joint venture, meaning, a joint venture that has not been established as a distinct legal entity, each participant of the joint venture shall be held jointly and severally liable and must individually execute and perform all acts required by this proposal. Documents signed by a common law joint venture, in connection with this proposal, shall include the names of all participants of the joint venture followed by the words "acting jointly and severally." All joint venture proposers must provide documentation of their legal status.

All Proposers must include documentation that they meet the above prerequisites. By furnishing this solicitation document to Proposers, the Port Authority has not made a determination that the Proposers have met the prerequisites or have otherwise been deemed qualified to perform the services. In addition, a determination that a Proposer has met the prerequisites is no assurance that they will be deemed qualified in connection with other proposal requirements included herein.

4. FINANCIAL INFORMATION

The Proposer will be required to demonstrate that it is financially capable of performing the contract resulting from this RFP ("Contract"). The determination of the Proposer's financial qualifications and ability to perform this Contract will be in the sole discretion of the Port Authority. The Port Authority may require a form of financial guarantee as part of its determination hereunder, such as a Letter of Credit. The Proposer shall submit, with its proposal, the following:

A. (1) Certified financial statements, including applicable notes, reflecting the Proposer's assets, liabilities, net worth, revenues, expenses, profit or loss and cash flow for the most recent year or the Proposer's most recent fiscal year.

(2) Where the certified financial statements in (1) above are not available, then either reviewed statements from an independent accountant setting forth the aforementioned information shall be provided.

Where the statements submitted pursuant to subparagraphs (1) and (2) aforementioned do not cover a period which includes a date not more than forty-five (45) days prior to the Proposal Due Date, then the Proposer shall also submit a statement in writing, signed by an executive officer or his/her designee, that the present financial condition of the Proposer is at least as good as that shown on the statements submitted.

B. A statement of work which the Proposer has, including any work on which a bid and/or proposal has been submitted, containing a description of the work, the annual dollar value, the location by City and State, the current percentage of completion, the expected date for completion, and the name of an individual most familiar with the Proposer's work on these jobs.

C. The name and address of the Proposer's banking institution, chief banking representative handling the Proposer's account, the Proposer's Federal Employer Identification Number (i.e., the number assigned to firms by the Federal Government for tax purposes), the Proposer's Dun and Bradstreet number, if any, the name of any credit service to which the Proposer furnished information and the number, if any, assigned by such service to the Proposer's account.

5. EVALUATION CRITERIA AND RANKING

All proposals will be reviewed by the Port Authority to determine if they adhere to the format required in this RFP, if they contain all required submissions and if the Proposer meets the prerequisites. For Proposals meeting such requirements, the following criteria, set forth in order of importance, will be utilized in the evaluation of proposals.

A. Cost:

The Total Estimated Contract Price as submitted on the Cost Proposal Form

B. Technical Expertise and Experience:

The degree and extent to which the Proposer and its management has demonstrated:

i. Prior experience, technical expertise and skills in performing security audits; implementing security audit programs and managing security auditing contracts;

ii. Knowledge of security audits, methods, criteria and related regulations;

iii. Experience and Qualifications of Proposer's Management in the performance of security auditing services.

C. Staffing and Management Approach:

The clarity, quality and feasibility of the Proposal to supply the contemplated services, which shall include the Proposer's management philosophy and management approach towards:

a. performing the security audit services described in the RFP; and

b. implementing the auditing services in the time frame described herein;

c. proposed service standards, concepts or procedures that Proposer intends to implement in order to provide the highest level of service;

d. approach to conducting trend analysis, analyzing security audit testing results and presenting such analysis(es) to the Port Authority.

e. the qualifications and relevant experience of the staff Proposed to be dedicated to this contract;

f. managing its staff through:
   1. quality assurance and control programs;
   2. conducting trainings;
   3. recruiting and retention procedures;
   4. self-assessment plan;
   5. workplace safety programs.

D. Business Risk:

The degree of business risk assumed by the Port Authority, including but not limited to, assessment of the impact resulting from the possible failure of the Contractor to perform under the terms and conditions of this Contract and the Port Authority's assessment of its ability to immediately replace the Contractor in a manner that maintains or improves the quality and continuity of the security auditing services at each facility.

E. Contractor Identity Check/Background Screening Plan: The Proposer's Contractor Identity Check and Background Screening Plan, which includes its effectiveness, thoroughness and the extent to which it ensures employees' identities are checked and confirmed. The system and manner in which employee background information will be measured/screened against the Contractor Identity Check/Background Screening Plan criteria, and how employees who successfully pass the criteria will be properly credentialed to perform the services herein. The submitted Plan shall become part of the Contract, will be a Contract requirement and shall be applicable to all years of the Contract. This will be evaluated on a pass/fail basis.

6. M/WBE SUBCONTRACTING PROVISIONS

The Port Authority has a long-standing practice of making its business opportunities available to Minority Business Enterprises (MBEs) and Women-Owned Businesses (WBEs) and has taken affirmative steps to encourage such firms to seek business

opportunities with the Port Authority. The successful Proposer will use good faith efforts to provide for meaningful participation by the Port Authority certified M/WBEs as defined in this document, in the purchasing and subcontracting opportunities associated with this contract, including purchase of equipment, supplies and labor services.

Minority Business Enterprise (MBE) - shall mean a business entity which is at least 51% owned and controlled by one or more members of one or more minority groups, or, in the case of a publicly held corporation, at least 51% of the stock of which is owned by one or more minority groups, and whose management and daily business operations are controlled by one or more such individuals who are citizens or permanent resident aliens.

"Minority Group" means any of the following racial or ethnic groups:

(a) Black persons having origins in any of the Black African racial groups not of Hispanic origin;

(b) Hispanic persons of Mexican, Puerto Rican, Dominican, Cuban, Central or South American culture or origin, regardless of race;

(c) Asian and Pacific Islander persons having origins in any of the original peoples of the Far East, Southeast Asia, The Indian Subcontinent, or the Pacific Islands;

(d) Native American or Alaskan native persons having origins in any of the original peoples of North America and maintaining identifiable tribal affiliations through membership and participation or community identification.

Women-Owned Business Enterprise (WBE) - shall mean a business enterprise which is at least 51% owned by one or more women, or, in the case of a publicly held corporation, at least 51% of the stock of which is owned by one or more women and whose management and daily business operations are controlled by one or more women who are citizens or permanent or resident aliens.

The Contractor shall use good faith efforts to achieve participation equivalent to 12% of the total Contract price for MBEs and 5% of the total Contract price for WBEs.

Good faith efforts to include participation by M/WBEs shall include, but not be limited to the following:

1) Dividing the services and materials to be procured into small portions where feasible;
2) Giving reasonable advance notice of specific subcontracting and purchasing opportunities to such firms as may be appropriate;
3) Soliciting services and materials from M/WBEs, which are certified by the Port Authority;
4) Ensuring that provision is made for timely progress payments to the M/WBEs and;
5) Observance of reasonable commercial standards of fair dealing in the respective trade or business.

Proposers are directed to use form PA3749B as the recording mechanism for the M/WBE participation Plan, annexed hereto as Attachment D or may be downloaded at http://www.panynj.gov/business-opportunities/become-vendor.html

The M/WBE Plan submitted by the Contractor to the Port Authority shall contain, at a minimum, the following:

- Identification of M/WBE's: Provide the names and addresses of all M/WBEs included in the Plan. If none are identified, describe the process for selecting participant firms in order to achieve the good faith goals under this Contract.
- Level of Participation: Indicate the percentage of M/WBE participation expected to be achieved with the arrangement described in the Plan.
- Scope of Work: Describe the specific scope of work the M/WBE's will perform.
- Previous M/WBE Participation: Describe any previous or current M/WBE participation, which the Proposer has utilized in the performance of its contracts.

All M/WBE subcontractors listed on the M/WBE Participation Plan must be certified by the Port Authority in order for the Contractor to receive credit toward the M/WBE goals set forth in this Contract. Please go to http://www.panynj.gov/business-opportunities/supplier-diversity.html to search for M/WBEs by a particular commodity or service. The Port Authority makes no representation as to the financial responsibility of such firms or their ability to perform Work under this Contract.

Proposers shall include their M/WBE Participation Plan with their proposals, to be reviewed and approved by the Authority's Office of Business Diversity and Civil Rights (OBDCR).

Proposers may request a waiver of the M/WBE participation goals set forth in this Contract by providing with its proposal, information in accordance with this provision and the provision entitled "M/WBE Good Faith Participation" in the Standard Terms and Conditions of this Contract.

If the Contractor wishes to subcontract a portion of the Work through a firm not listed in the Directory, but which the Contractor believes should be eligible because it is (1) an M/WBE, as defined above and (2) competent to perform portions of the Work, the Contractor shall submit an M/WBE Uniform Certification Application to the Port Authority of New York and New Jersey, Office of Business Diversity and Civil Rights (OBDCR), 233 Park Avenue South, 4th Floor, New York, NY 10003. The application is available online at http://www.panynj.gov/business-opportunities/sd-become-certified.html. In addition, to update your certification file and to advise OBDCR of changes to any information, please email these changes to certhelp@panynj.gov. Credit toward applicable goals will be granted only to Port Authority certified vendors. For more information about M/WBE Programs, call (212) 435-7819.

7. CERTIFICATION OF RECYCLED MATERIALS PROVISION

Proposers shall submit, with their proposal, Attachment F the Certified Environmentally Preferable Products / Practices Form attesting that the products or items offered by the Proposer contain the minimum percentage of post-consumer recovered material in accordance with the most recent guidelines issued by the United States Environmental

Protection Agency (EPA), or, for commodities not so covered, the minimum percentage of post-consumer recovered materials established by other applicable regulatory agencies.

Recycling Definitions:
For purposes of this solicitation, the following definitions shall apply:

a. "Recovered Material" shall be defined as any waste material or by-product that has been recovered or diverted from solid waste, excluding those materials and by-products generated from, and commonly reused within, an original manufacturing process.

b. "Post-consumer Material" shall be defined as any material or finished product that has served its intended use and has been discarded for disposal or recovery having completed its life as a consumer item. "Post-consumer material" is included in the broader category of "Recovered Material."

c. "Pre-consumer Material" shall be defined as any material or by-product generated after the manufacture of a product but before the product reaches the consumer, such as damaged or obsolete products. Pre-consumer Material does not include mill and manufacturing trim, scrap, or broken material that is generated at a manufacturing site and commonly reused on-site in the same or another manufacturing process.

d. "Recycled Product" shall be defined as a product that contains the highest amount of post-consumer material practicable, or when post-consumer material is impracticable for a specific type of product, contains substantial amounts of Pre-consumer Material.

e. "Recyclable Product" shall be defined as the ability of a product and its packaging to be reused, reconditioned for use, or recycled through existing recycling collection programs.

f. "Waste Reducing Product" shall be defined as any product that will result in less waste generated due to its use rather than another product designed to serve the same function with an greater waste generation rate. This shall include, but not be limited to, those products that can be reused, refilled or have a longer life expectancy and contain a lesser amount of toxic constituents.

8. PROPOSAL SUBMISSION REQUIREMENTS

In order to expedite the evaluation of proposals, the Proposer's response to this RFP shall follow the format and order of items, using the same paragraph identifiers, as set forth below.

In order to expedite the evaluation of proposals, the Proposer's response to this RFP shall follow the format and order of items, using the same paragraph identifiers, as set forth below.

A. Letter of Transmittal

The Proposer shall submit a letter on its letterhead, signed by an authorized representative, stating its experience and qualifications in meeting the requirements of this RFP. This letter shall include a statement on whether the

Proposer is submitting a proposal as a single entity, a joint venture, or is partnering with another firm in a prime/subcontracting relationship. In all cases, information required for a single entity is required for each participant in a joint venture.

The Letter of Transmittal shall contain:

(1) Name and address of the Proposer and an original signature on the Letter of Transmittal by an authorized representative on behalf of the Proposer;

(2) Name(s), title(s) and telephone number(s) of the individual(s) who are authorize to negotiate and execute the Contract;

(3) Name, title and telephone number of a contact person to which the Port Authority can address questions or issues related to this RFP;

(4) Name and address of proposed subcontractors, if any;

(5) If a corporation: (a) a statement of the names and residences of its officers, and (b) a copy of its Certificate of Incorporation, with a written declaration signed by the secretary of the corporation, with the corporate seal affixed thereto, that the copy furnished is a true copy of the Certificate of Incorporation as of the date of the opening of the Proposals;

If a partnership: a statement of the names and residences of its principal officers, indicating which are general and which special partners are;

If an individual: a statement of residence;

If a joint venture: information on each of the parties consistent with the information requested above; if the Contract is awarded to each member will be jointly and severally liable under the Contract.

B. Executive Summary

The Proposer shall submit a summary presenting the major features of its proposal and how the proposal satisfies the requirements contained in this RFP, as well as the special competencies and expertise of the Proposer to meet the requirements of this RFP.

C. Agreement on Terms of Discussion

The Proposer shall submit a copy of the "Agreement on Terms of Discussion," signed by an authorized representative of the Proposer. The Agreement format is included as Attachment A and shall be submitted by the Proposer without any alterations or deviations. Any Proposer who fails to sign the Port Authority's "Agreement on Terms of Discussion" will not have its proposal reviewed. If the Proposer is a joint venture, an authorized representative of each party must sign the Agreement.

D. Certifications With Respect to the Contractor's Integrity Provisions
The Proposer, by signing the Letter of Transmittal, makes the certifications in the "Contractor's Integrity Provisions," included as Attachment B, General Contract Provisions this RFP. If the Proposer cannot make any such certifications, it shall enclose an explanation of that inability.

E. Documentation of Proposer Prerequisites
The Proposer shall submit documentation to demonstrate that it meets all prerequisites, if any, included herein.

F. Proposal
The Proposer must submit a proposal that details and clearly describes its experience and capability to perform the security auditing services described in this RFP, its approach to such work and the cost of such work to the Port Authority. At a minimum, the proposal shall address the following:

1) Cost:
The Proposer shall submit a cost proposal indicating the compensation it expects to receive. The Cost Proposal shall be complete, include all Cost Proposal Forms supplied in this solicitation, and be inclusive of all work required in this RFP and shall include, but not be limited to, material and labor costs, any wages, salaries, health benefits and other supplemental benefits, overheads, profits, etc.

2) Technical Expertise and Experience:
The Proposer shall submit information to allow the Port Authority to evaluate it with respect to the technical expertise and experience as more fully set forth in Section 5 above "Evaluation Criteria and Ranking". The Proposal should include:

a. A listing of all security auditing contracts that were performed by or are currently being performed by the Proposer within the last five (5) years. For each Contract listed, include:
    1. The name and address of the Contracting party
    2. The locations where the work was performed
    3. Duration of the Contract
    4. The approximate dollar amount of the Contract
    5. The annual staff hours of full and part time labor expended in the performance of the Contract
    6. A summary of the types of work performed
    7. The names, addresses and telephone numbers of the owners and contract administrators
    8. Representatives familiar with the work that the Port Authority may contact

b. The Proposer shall submit relevant experience of Proposer's management team in managing similar security auditing programs, including, utilization of technological advances in security auditing services;

c. The Proposer shall submit to the Port Authority, a detailed itemized description explaining technical expertise and past experience the firm has in the following areas:
    1. Utilization of technological advances, or other tools in unarmed, uniformed security guard services and resulting benefits;

    2. Management of Unarmed, Uniformed Security Guard Services in buildings and facilities of similar size.

    3. Highlight any and all aviation/airport experience, although such experience is not required.

    4. Describe any Safety Act experience, designations or certifications Proposer has been awarded or expects to be awarded. Include a copy of any Safety Act application(s), designations or certifications and related supporting documents which may be applicable to the services being provided under this Contract.

d. The Proposer should provide documentation relevant to establish the Proposer's capability to meet all terms and conditions set forth herein, including insurance requirements.

e. The Proposer shall submit risk assessment, succession plans and any other relevant documentation that assess the Proposer's business risk in taking on the significant amount of new work that will be required under this Contract. The risk assessment plan should take into account all work currently under contract, as well as work that is under contract to companies which the Proposer owns, controls or has an interest. The assessment should provide sufficient information to allow the Port Authority to assess the impact resulting from the possible failure of the Contractor to perform under the terms and conditions of the Contract.

f. The Proposer shall submit information establishing that it is financially capable of performing the Contract and possesses the corporate infrastructure to support the services required set forth in this solicitation.

    1. Knowledge of security audits

    2. Qualifications of staff
        a. Length of service with the Proposer
        b. Anticipated function of each individual on the Contract

    3. Contracts performed in the past five (5) years

3) **Staffing and Management Approach:**
The Proposer must submit information, which clearly describes its management approach to perform the security audit services described in the RFP and its approach to such work for the Port Authority. The Proposer shall provide:

a. A description of how Proposer will deliver/implement auditing services described in the RFP

b. Service standards, concepts or procedures that the Proposer intends to implement in order to provide the highest level of service

c. A description of how the Proposer will perform trend analysis on security audit testing results and present such analysis(es) to the Port Authority

d. A description of how the Proposer will evaluate its auditing methods and practices, to verify the effectiveness of the proposed services and sample audit result reports, audit forms, monthly audit summary reports, etc. to support the required services herein.

e. A description of how the Contractor will manage its staff through:
    1. quality assurance and control programs
    2. recruiting and retention procedures
    3. conducting trainings
    4. self-assessment plan
    5. workplace safety programs

f. An organization chart which shows how the Proposer will implement and provide the services in the RFP

g. A description of the Proposer's ability to provide services concurrently at five (5) airports

h. A description of how it will meet:
    1. General liability insurance
    2. The proposed M/WBE Participation Plan
    3. The proposed Certified Environmentally Preferable Products/Practices Form

4) **Business Risk**
The Proposer shall submit risk assessment, succession plans and any other relevant documentation that assess the Proposer's business risk in taking on the significant amount of new work that will be required under this Contract. The risk assessment plan should take into account all work currently under contract, as well as work that is under contract to companies which the Proposer owns, controls or has an interest. The assessment should provide sufficient information to allow the Port Authority to assess the impact

resulting from the possible failure of the Contractor to perform under the terms and conditions of the Contract.

The Proposer shall provide any information related to business risk which the Firm believes would be helpful to the Port Authority in the evaluation of its submittal.

5) Contractor Identity Check/Background Screening Plan

The Proposer shall submit a Contractor Identity Check/Background Screening Plan, which demonstrates with specificity how the Proposer will ensure that only employees who were successfully prescreened and properly credentialed perform the services herein. This Plan shall be applicable to all years of the Contract and shall include, but not be limited to, the following:

- Specify sources, details and criteria for the check, such as criminal records searches conducted, immigration status, job history, reference checking;
- Specific measures, services or reviews undertaken to verify employees' identities;
- The length of time researched for the identity check/background screening on new hires, which shall be at a minimum of 10 years of employment history or verification of what an employee documented he/she has done in the last 10 years preceding the date of the investigation;
- Identification of specific resources, technology, subcontractors or firms utilized in the performance of said services;
- The frequency with which employee checks are conducted (example: upon hiring and every six (6) months thereafter).

The Proposer shall provide any other information that is related to the requirements in this Section (Section F), that the Proposer believes would be helpful to the Port Authority in the evaluation of its Proposal.

G. Acknowledgment of Addenda

If any Addenda are posted or sent as part of this RFP, the Proposer shall complete, sign and include with its Proposal the addenda form(s). In the event any Proposer fails to conform to these instructions, its proposal will nevertheless be construed as though the Addenda had been acknowledged.

If the Proposer downloaded this RFP document, it is the responsibility of the Proposer to periodically check the Port Authority website at http://www.panynj.gov/business-opportunities/bid-proposal-advertisements.html and download any addenda that might have been issued in connection with this solicitation.

H. Acceptance of Standard Contract Terms and Conditions
The Port Authority has attached to this RFP as Attachment B, General Contract Provisions governing the Contract. The Proposer is expected to agree with these General Contract Provisions. However, if the Proposer has any specific exceptions, such exceptions should be set forth in a separate letter included with its response to this RFP. After the proposal due date, the Proposer will be precluded from raising any exceptions unless such exceptions are justified by and directly related to substantive changes in the business or technical requirements and are agreed to by the Proposer and the Port Authority.

I. M/WBE Plan
The Proposer shall submit an M/WBE Plan in accordance with the M/WBE Subcontracting Provisions hereunder.

9. CONDITIONS FOR THE SUBMISSION OF A PROPOSAL

In addition to all other requirements of this RFP, the Proposer agrees to the following conditions for the submission of its proposal.

A. Changes to this RFP
At any time, in its sole discretion, the Port Authority may by written addenda, modify, correct, amend, cancel and/or reissue this RFP. If an addendum is issued prior to the date proposals are due, it will be provided to all parties in the medium in which the parties obtained the RFP. If an addendum is issued after proposals have been received, the addendum will be provided only to those whose proposals remain under consideration at such time.

B. Proposal Preparation Costs
The Port Authority shall not be liable for any costs incurred by the Proposer in the preparation, submittal, presentation, or revision of its proposal, or in any other aspect of the Proposer's pre-contract activity. No Proposer is entitled to any compensation except under an agreement for performance of services signed by an authorized representative of the Port Authority and the Proposer.

C. Disclosure of Proposal Contents / Use of Ideas and Materials
Proposal information is not generally considered confidential or proprietary. All information contained in the proposal is subject to the "Agreement on Terms of Discussion" attached hereto as Attachment A.

D. Ownership of Submitted Materials
All materials submitted in response to or in connection with this RFP shall become the property of the Port Authority. Selection or rejection of a Proposal shall not affect this right.

E. Subcontractors
If a Proposer intends to use subcontractor(s) the Proposer must identify in its proposal the names of the subcontractor(s) and the portions of the work the subcontractor(s) will perform.

F. Conflict of Interest

If the Proposer or any employee, agent or subcontractor of the Proposer may have a possible conflict of interest, or may give the appearance of a possible conflict of interest, the Proposer shall include in its proposal a statement indicating the nature of the conflict. The Port Authority reserves the right to disqualify the Proposer if, in its sole discretion, any interest disclosed from any source could create a conflict of interest or give the appearance of a conflict of interest. The Contractor awarded this Contract may not participate in any future solicitations issued by the Port Authority, or perform services as a prime or subcontractor, relating to the provision of guard services, security services, security auditing services, or related services, at any Port Authority owned or operated airports during the duration of this Contract, including any options or extensions. The Port Authority's determination regarding any questions of conflict of interest shall be final.

G. Authorized Signature

Proposals must be signed by an authorized corporate officer (e.g., President or Vice President), General Partner, or such other individual authorized to bind the Proposer to the provisions of its proposal and this RFP.

H. References

The Port Authority may consult any reference familiar with the Proposer regarding its current or prior operations and projects, financial resources, reputation, performance, or other matters. Submission of a proposal shall constitute permission by the Proposer for the Port Authority to make such inquiries and authorization to third parties to respond thereto.

I. Evaluation Procedures and Negotiation

Only Proposers which meet the prerequisites, if any, may have their proposals evaluated based on the evaluation criteria set forth in this RFP. The Port Authority may use such procedures that it deems appropriate to evaluate such proposals. The Port Authority may elect to initiate contract negotiations with one or more Proposers including negotiation of costs/price(s) and any other term or condition, including modifying any requirement of this RFP. The option of whether or not to initiate contract negotiations rests solely with the Port Authority.

J. Taxes and Costs

Purchases of services and tangible personal property by the Port Authority in the States of New York and New Jersey are generally exempt from state and local sales and compensating use taxes, and from most federal excises (Taxes). All costs associated with the Contract must reflect this exemption and be stated in U.S currency.

K. Most Advantageous Proposal/No Obligation to Award

The Port Authority reserves the right to award the Contract to other than the Proposer proposing the lowest price. The Contract will be awarded to the Proposer whose proposal the Port Authority believes, in its sole discretion, will be the most advantageous to the Port Authority. Neither the release of this RFP nor the acceptance of any response thereto shall compel the Port Authority to accept any proposal. The Port Authority shall not be obligated in any manner whatsoever

to any Proposer until a proposal is accepted by the Port Authority in the manner provided in the Section of this RFP entitled "Proposal Acceptance or Rejection."

Multiple Contract Awards

The Port Authority reserves the right to award multiple Contracts for the products, work and/or services that are the subject matter of this RFP and Proposers are hereby given notice that they may not be the Port Authority's only contractor for such products, work and/or services.

L. Right to Extend Contract

If this is a proposal for a contract for a term of years, including specified options for renewal, the Port Authority reserves the additional right to extend the contract term for an additional one-hundred twenty (120) days, upon the same terms and conditions of the original Contract negotiated between the Port Authority and the successful Proposer.

M. Rights of the Port Authority

(1) The Port Authority reserves all its rights at law and equity with respect to this RFP including, but not limited to, the unqualified right, at any time and in its sole discretion, to change or modify this RFP, to reject any and all proposals, to waive defects or irregularities in proposals received, to seek clarification of proposals, to request additional information, to request any or all Proposers to make a presentation, to undertake discussions and modifications with one or more Proposers, or to negotiate an agreement with any Proposer or third person who, at any time, subsequent to the deadline for submissions to this RFP, may express an interest in the subject matter hereof, to terminate further participation in the proposal process by a Proposer or to proceed with any proposal or modified proposal, which in its judgment will, under all circumstances, best serve the Port Authority's interest. The Port Authority may, but shall not be obliged to, consider incomplete proposals or to request or accept additional material or information. The holding of any discussions with any Proposer shall not constitute acceptance of a proposal, and a proposal may be accepted with or without discussions.

(2) No Proposer shall have any rights against the Port Authority arising from the contents of this RFP, the receipt of proposals, or the incorporation in or rejection of information contained in any proposal or in any other document. The Port Authority makes no representations, warranties, or guarantees that the information contained herein, or in any addenda hereto, is accurate, complete, or timely or that such information accurately represents the conditions that would be encountered during the performance of the contract. The furnishing of such information by the Port Authority shall not create or be deemed to create any obligation or liability upon it for any reason whatsoever and each Proposer, by submitting its proposal, expressly agrees that it has not relied upon the foregoing information, and that it shall not hold the Port Authority liable or responsible therefor in any manner whatsoever. Accordingly, nothing contained herein and no representation, statement or promise, of the Port Authority, its directors, officers, agents, representatives, or employees, oral or in writing, shall impair or limit the effect of the

warranties of the Proposer required by this RFP or Contract and the Proposer agrees that it shall not hold the Port Authority liable or responsible therefor in any manner whatsoever.

(3) At any time and from time to time after the opening of the proposals, the Port Authority may give oral or written notice to one (1) or more Proposers to furnish additional information relating to its proposal and/or qualifications to perform the services contained in this RFP, or to meet with designated representatives of the Port Authority. The giving of such notice shall not be construed as an acceptance of a proposal. Information shall be submitted within three (3) calendar days after the Port Authority's request unless a shorter or longer time is specified therein.

N. No Personal Liability

Neither the Commissioners of the Port Authority, nor any of them, nor any officer, agent or employee thereof shall be charged personally with any liability by a Proposer or another or held liable to a Proposer or another under any term or provision of this RFP or any statements made herein or because of the submission or attempted submission of a proposal or other response hereto or otherwise.

ATTACHMENT A

AGREEMENT ON TERMS OF DISCUSSION

The Port Authority's receipt or discussion of any information (including information contained in any proposal, vendor qualification, ideas, models, drawings, or other material communicated or exhibited by us or on our behalf) shall not impose any obligations whatsoever on the Port Authority or entitle us to any compensation therefor (except to the extent specifically provided in such written agreement, if any, as may be entered into between the Port Authority and us). Any such information given to the Port Authority before, with or after this Agreement on Terms of Discussion ("Agreement"), either orally or in writing, is not given in confidence. Such information may be used, or disclosed to others, for any purpose at any time without obligation or compensation and without liability of any kind whatsoever. Any statement which is inconsistent with this Agreement, whether made as part of or in connection with this Agreement, shall be void and of no effect. This Agreement is not intended, however, to grant to the Port Authority rights to any matter, which is the subject of valid existing or potential letters patent. The foregoing applies to any information, whether or not given at the invitation of the Authority.

Notwithstanding the above, and without assuming any legal obligation, the Port Authority will employ reasonable efforts, subject to the provisions of the Port Authority Freedom of Information Code and Procedure adopted by the Port Authority's Board of Commissioners on March 29, 2012, which may be found on the Port Authority website at: *http://www.panynj.gov/corporate-information/pdf/foi-code.pdf*, not to disclose to any competitor of the undersigned, information submitted which are trade secrets or is maintained for the regulation or supervision of commercial enterprise which, if disclosed, would cause substantial injury to the competitive position of the enterprise, and which information is identified by the Proposer as proprietary, which may be disclosed by the undersigned to the Port Authority as part of or in connection with the submission of a proposal.

_____

(Company)

_____

(Signature)

_____

(Title)

_____

(Date)

ATTACHMENT B
PART I - CONTRACT SPECIFIC TERMS AND CONDITIONS FOR SECURITY AUDITING PROGRAM

1) General Agreement 26
2) Specific Definitions and Acronyms 26
3) Description of Services 27
4) Duration of Contract 28
5) Payment 28
6) Escalation/Price Adjustment 30
7) Extra Work 31
8) Insurance 34
9) Holidays 35
10) Increase or Decrease in Areas or Frequencies 36
11) Liquidated Damages 36
12) Specifications 38
13) Job Classifications 39
14) Specific Skill Personnel Requirements 39
15) Duties of Staff 42
16) Management Authority 47
17) Attendance Records for Contractor Employees 47
18) Training Requirements 47
19) Materials, Supplies and Equipment 49
20) Drug and Alcohol Testing and Physical Examination Requirements 49
21) Identification Requirements 50
22) Ineligibility for Challenge (Bogus Bob/Babs) and Airport Community Crime and Security Watch Awards 50
23) Security Audit Reporting System: Report Development, Procedures and Record Retention 51
24) Security of Information Plan 51
25) Confidentiality - Proprietary Information 52
26) Space Provided to the Contractor 52
27) Contractor's Vehicles - Parking 53
28) Employee Uniforms and Appearance 53
29) Transitioning Services at Start/Termination of the Contract 54
30) Safety Provisions 54

31) Site Specific Recycling and Trash Removal 54
32) Limitation on Future Contracting 54

PART I – CONTRACT SPECIFIC TERMS AND CONDITIONS FOR SECURITY AUDITING PROGRAM

Section 1. General Agreement

Subject to all of the terms and conditions of this Contract, the undersigned (hereinafter called the "Contractor") hereby offers and agrees to provide all the necessary supervision, personnel, equipment, materials and all other things necessary to perform the Services required by this Contract as more fully described herein, at the location(s) listed herein, and do all other things necessary or proper therefor or incidental thereto, all in strict accordance with the provisions of the Contract Documents and any future changes therein; and the Contractor further agrees to assume and perform all other duties and obligations imposed upon it by this Contract.

In addition, all things not expressly mentioned in the Specifications but involved in the carrying out of their intent and in the complete and proper execution of the matters referred to in and required by this Contract are required by the Specifications, and the Contractor shall perform the same as though they were specifically delineated, described and mentioned therein.

Section 2. Specific Definitions and Acronyms

To avoid undue repetition, the following terms, as used in this Contract, shall be construed as follows:

"**API**" shall refer Application Programming Interface

The term **"ASM", "Airport Security Manager", "Airport Security Managers", "Director", "General Manager", "Manager", "Port Authority Manager" and "WTC Manager"**, shall mean the person designated by the Port Authority to manage all aspects of this Contractor or his/her successor in duties for this purpose of this Contract, acting personally or through his/her duly authorized representative.

"**Basic Lease**" shall mean the agreement between the Port Authority and the City of New York dated April 17, 1947 as the same from time to time may have been or may be supplemented, amended or extended, by which LaGuardia and John F. Kennedy International Airports were leased by the City of New York to the Port Authority. Said agreement dated April 17, 1947 has been recorded in the office of the Register of the City of New York, County of Queens, on May 22, 1947, in Liber 5402 of Conveyances, on page 319 et seq. No greater rights or privileges are hereby granted to the Permittee than the Port Authority has the power to grant under said agreement as supplemented or amended as aforesaid.

"**BOR**" shall refer to Breach of Rules

"CFR" shall refer to Code of Federal Regulations

"**Contractor**" shall mean the Port Authority's Contractor to provide security audit services

"**Employees**" as used herein means only the employees of the Contractor.

"**EWR**" shall refer to Newark Liberty International Airport

"**FAA**" shall refer to the Federal Aviation Administration

"**Facility**" or "**Facilities**" shall mean:

a) **John F. Kennedy International (JFK) and LaGuardia (LGA) Airports** located in the borough and county of Queens in the city and state of New York
b) **Newark Liberty International (EWR) airport** in the cities of Newark (Essex County) and Elizabeth (Union County), state of New Jersey
c) **Stewart International (SWF) Airport** located in the county of Orange in the city of Newburgh in the state of New York
d) **World Trade Center (WTC)** located in the borough of Manhattan in the city and state of New York
e) **Teterboro (TEB) Airport** located in the county of Bergen in the cities of Teterboro and Moonachie, state of New Jersey

"**IMCS**" shall refer to Identity Management Credentialing System

"**IO**" shall refer to Issuing Officers/Signatory Authority

"**JFK**" shall refer to John F. Kennedy International Airport

"**LGA**" shall refer to LaGuardia Airport

"**MMF**" shall refer to Monthly Management Fee

"**ODBC**" shall refer to Open Database Connectivity

"**PA**" or "**Port Authority**" shall refer to Port Authority of New York & New Jersey

"**PONYA**" shall refer to Port of New York Authority

"**RON**" shall refer to Remain Overnight

"**SD**" shall refer to Security Directives issued by the TSA

"**SIDA**" shall refer to Security Identification Display Area

"**SOC**" shall refer to Security Operations Console

"**SWF**" shall refer to Stewart International Airport

"**TEB**" shall refer to Teterboro Airport

"**TSA**" shall refer to the Transportation Security Administration

"**TSR**" shall refer to Transportation Security Administration Regulation

"**WTC**" shall refer to the World Trade Center

Section 3. Description of Services

The Contractor shall provide on-site security auditing services at the Facilities", as determined by Manager.

Section 4. Duration of Contract

(a) The term of the Contract (hereinafter called the "Base Term") is for five (5) year period and is estimated to commence on August 29, 2013 at 12:01 a.m. (said date and time hereinafter sometimes called "the Commencement Date") and unless sooner terminated or revoked or extended as provided in Paragraph (b) and (c) hereof shall expire on August 31, 2018 at 11:59 p.m. (said date and time hereinafter sometimes called the "Expiration Date").

(b) The Port Authority shall have the right to extend this Contract for two (2) one (1) year Option Periods to August 31, 2020 (hereinafter called the "Option Period") following the Expiration Date, upon the same terms and conditions subject only to adjustments of charges, if applicable to this Contract, as may be hereinafter provided in the paragraph entitled "Escalation/Price Adjustment." If the Port Authority shall elect to exercise the Option(s) to extend this Contract, then, no later than thirty (30) days prior to the Expiration Date, the Port Authority shall send a notice that it is extending the Base Term of this Contract, and this Contract shall thereupon be extended for the applicable Option Period. If the Contract provides for more than one (1) Option Period, the same procedure shall apply with regard to extending the term of this Contract for succeeding Option Periods.

(c) The Port Authority shall have the right to extend the Base Term for an additional period of up to one hundred and twenty (120) days subsequent to the Expiration Date of the Base Term, or the Expiration Date of the final exercised Option Period (hereinafter called the "Extension Period"), subject to the same terms and conditions as the previous contract period. The prices quoted by the Contractor for the previous contract period shall remain in effect during this Extension Period without adjustment. If it so elects to extend this Contract, the Port Authority will advise the Contractor, in writing that the term is so extended, and stipulate the length of the extended term, at least thirty (30) days prior to the expiration date of the previous contract period.

Section 5. Payment

Subject to the provisions of this Contract, the Port Authority agrees to pay to the Contractor and the Contractor agrees to accept from the Port Authority as full and complete consideration for the performance of all its obligations under this Contract and as sole compensation for the Work performed by the Contractor hereunder, a compensation calculated from the actual quantities of services performed and the respective prices inserted by the Contractor in the Pricing Sheet(s), forming a part of this Contract, exclusive of compensation under the clause hereof entitled "Extra Work." The manner of submission of all bills for payment to the Contractor by the Port Authority for Services rendered under this Contract shall be subject to the approval of the Port Authority Manager in all respects, including, but not limited to, format, breakdown of items presented and verifying records. All computations made by the Contractor and all billing and billing procedures shall be done in conformance with the following procedures:

a) Payment shall be made in accordance with the prices for the applicable service (during the applicable Contract year) as they appear on the Cost Proposal Forms and Pricing Sheet(s), as the same may be adjusted from time to time as specified herein, minus any

deductions for services not performed and/or any liquidated damages to which the invoice may be subject and/or any adjustments as may be required pursuant to increases and decreases in areas or frequencies, if applicable. All Work must be completed within the time frames specified or as designated by the Manager.

The Contractor shall submit to the Manager by the fifth day of each month following the month of commencement of this Contract and on or by the fifth day of each month thereafter (including the month following the termination, revocation or expiration of this Contract) a complete and correct invoice for the Work performed during the preceding month accompanied by such information as may be required by the Manager for verification. The invoice must show the Contractor's Federal Tax Identification Number. Payment will be made within thirty (30) days of Port Authority verification of the invoice.

b) No certificate, payment, acceptance of any Work or any other act or omission of any representative of the Port Authority shall operate to release the Contractor from any obligation under or upon this Contract, or to estop the Port Authority from showing at any time that such certificate, payment, acceptance, act or omission was incorrect or to preclude the Port Authority from recovering any monies paid in excess of those lawfully due and any damage sustained by the Port Authority.

c) In the event an audit of received invoices should indicate that the correct sum due the Contractor for the relevant billing period is less than the amount actually paid by the Port Authority, the Contractor shall pay to the Port Authority the difference promptly upon receipt of the Port Authority's statement thereof. The Port Authority may, however, in its discretion elect to deduct said sum or sums from any subsequent monthly payments payable to the Contractor hereunder.

d) The manner of submission of all invoices for payment to the Contractor by the Port Authority for services rendered under this Contract shall be subject to the approval of and verification by the Port Authority in all respects, including, but not limited to, format, breakdown of items presented, supporting documentation for all work performed, and verification of records. The Port Authority shall have the authority to decide all matters of fact or questions pertaining to any invoice and shall have the right to make adjustments in compensation to such invoices as necessary to ensure correct payment to the Contractor.

e) It is expressly understood and agreed that all costs of the Contractor of whatever kind of nature and whether imposed directly upon the Contractor under the terms and provisions hereof or in any other manner whatsoever because of the requirements of the security auditing services or otherwise under this Agreement, shall be borne by the Contractor-without compensation or reimbursement from the Port Authority, except as specifically herein before set forth in this Section. The entire and complete cost and expense of the Contractor's services and operations hereunder shall be borne solely by the Contractor and under no circumstances shall the Port Authority be liable to any third party (including the Contractor's employees) for any such costs and expenses incurred by the Contractor and under no circumstances shall the Port Authority be liable to the Contractor for the same, except as specifically set forth in this Section.

f) "Final Payment", as the term is used throughout this Contract, shall mean the final payment made for services rendered in the last month of the Base Term or Extension Period. However should this Contract be terminated for any reason prior to the last month of the Base Term or Extension Period, then Final Payment shall be the payment made for services rendered in the month during which such termination becomes effective. The Contractor's acceptance of Final Payment shall act as a full and complete release to the Port Authority of all claims of and of all liability to the Contractor for all things done or furnished in connection with this Contract and for every act and neglect of the Port Authority and others relating to or arising out of this Contract, including claims arising out of breach of contract and claims based on claims of third persons. No payment, however, final or otherwise shall operate to release the Contractor from any obligations in connection with this Contract.

g) All services performed by the Project Managers and other management staff shall be included in the Monthly Management Fee and are not separately billable. Port Authority acceptable services performed by "Security Auditor" are to be paid at the agreed upon applicable rate. However, should the Project Manager delegate any of his/her job duties to any non-management Contract staff, the performance of those services will still be covered under the Monthly Management Fee.

Section 6. <u>Escalation/Price Adjustment</u>

All Contract prices submitted by the Contractor and agreed to by The Port Authority, shall be applicable to the Base Term. For the Option Period(s) that are applicable to this Contract and are exercised hereunder, (excluding the one hundred twenty (120) day Extension Period as described in Section 3 hereof entitled "Duration") the Port Authority shall adjust the compensation due to the Contractor utilizing the Consumer Price Index for all Urban Consumers; Series Id: CUURA101SA0L2; Not Seasonally Adjusted; New York-Northern New Jersey-Long Island, NY-NJ-CT-PA area; all items less shelter; 1982-1984=100, published by the Bureau of Labor Statistics of the United States Department of Labor (hereinafter called the "Price Index").

For the first year of the Option Period of the Contract, the Price Index shall be determined for the months of March 2017 and March 2018. The Contract prices for Supplemental Work and Operational Usage payable in the final year of the Base Term shall be multiplied by a fraction the numerator of which is the Price Index for March 2018 and the denominator of which is the Price Index for March 2017. The resulting product shall be the amounts payable to the Contractor in the first Option Period.

For the second year of the Option Period of the Contract, the Price Index shall be determined for the months of March 2018 and March 2019. The Contract prices for Supplemental Work and Operational Usage payable to the Contractor in the first Option Period shall be multiplied by a fraction the numerator of which is the Price Index for March 2019 and the denominator of which is the Price Index for March 2018 The resulting product shall be the amounts payable to the Contractor in the second Option Period.

In the event of a change in the basis for the computation of the said Index or the discontinuance of its publication, such other appropriate index shall be substituted as may be agreed upon by the Authority and the Contractor as properly reflecting changes in the value of the current United States money in a manner similar to that established in the said Price Index. In the event of the failure of the parties to so agree, the Port Authority may select and use such index, as it seems

appropriate. Notwithstanding the provisions of this section, in no event shall any adjustment hereunder, be greater than three percent (3%) per annum nor less zero (0%) percent per annum.

The amounts payable to the Contractor for the 120-day Extension Period shall not be subject to adjustment.

If, after an adjustment referred to in this Section the Index used for computing such adjustment shall be changed or adjusted, then the amounts payable to the Contractor for that period shall be recomputed. If such recomputation results in a smaller increase in the amount payable to such period, then after notification of the change or adjustment, the recomputed amounts shall be in effect and upon demand by the Port Authority (or PATH), the Contractor shall refund to the Port Authority excess amounts theretofore paid by the Port Authority for such period.

Section 7. Extra Work

The Contractor is required to provide separate materials, supplies, equipment and personnel for Extra Work when such is deemed necessary by the Manager. "Extra Work" as used herein shall be defined as work which differs from that expressly or impliedly required by the Specifications in their present form. Total Extra Work performed by the Contractor shall not exceed six percent (6%) of the Total Estimated Contract Price of this Contract for the entire Term of this Contract including extensions thereof, or six percent (6%) of the Total Estimated Contract Price of each Section if this Contract is awarded by separate Sections.

An increase in area or frequency does not constitute Extra Work, but shall be compensable based on the prices in the Pricing Sheet(s) and the paragraph herein titled "Increase or Decrease in Areas or Frequencies."

The Contractor is required to perform Extra Work pursuant to a written order of the Manager expressly recognizing such work as Extra Work. If Lump Sum or Unit Price compensation cannot be agreed upon by the parties in writing prior to the start of Work, the Contractor shall perform such Extra Work and the Contractor's compensation shall be increased by the sum of the following amounts and such amounts only: (1) the actual net cost, in money, of the labor, and material, required for such Extra Work; (2) ten percent (10%) of the amount under (1) above; (3) such rental as the Manager deems reasonable for plant and equipment (other than small tools) required for such Extra Work; (4) if the Extra Work is performed by a subcontractor, an additional five percent (5%) of the sum of the amounts under (1) through (3) above. As used in this numbered clause (and in this clause only):

"Labor" means laborers, mechanics, and other employees below the rank of supervisor, directly employed at the Site of the Work subject to the Manager or their designee's authority to determine what employees of any category are "required for Extra Work" and as to the portion of their time allotted to Extra Work; and "cost of labor" means the wages actually paid to and received by such employees plus a proper proportion of (a) vacation allowances and union dues and assessments which the employer actually pays pursuant to contractual obligation upon the basis of such wages, and (b) taxes actually paid by the employer pursuant to law upon the basis of such wages and workers' compensation premiums paid pursuant to law. "Employees" as used above means only the employees of one employer.

"Net Cost" shall be the Contractor's actual cost after deducting all permitted cash and trade discounts, rebates, allowances, credits, sales taxes, commissions, and refunds (whether or not any or all of the same shall have been taken by the Contractor) of all parts and materials purchased by the Contractor solely for the use in performing its obligation hereunder provided, where such purchase has received the prior written approval of the Manager as required herein. The Contractor shall promptly furnish to the Manager such bills of sale and other instruments as the Manger may require, executed, acknowledged and delivered, assuring to the Manager title to such materials, supplies, equipment, parts, and tools free of encumbrances.

"Materials" means temporary and consumable materials as well as permanent materials; and "cost of materials" means the price (including taxes actually paid by the Contractor pursuant to law upon the basis of such materials) for which such materials are sold for cash by the manufacturers or producers thereof, or by regular dealers therein, whether or not such materials are purchased directly from the manufacturer, producer or dealer (or if the Contractor is the manufacturer or producer thereof, the reasonable cost to the Contractor of the manufacture and production), plus the reasonable cost of delivering such materials to the Site of the Work in the event that the price paid to the manufacturer, producer or dealer does not include delivery and in case of temporary materials, less their salvage value, if any.

The Manager shall have the authority to decide all questions in connection with the Extra Work. The exercise by the Manager of the powers and authorities vested in him/her by this section shall be binding and final upon the Port Authority and the Contractor.

The Contractor shall submit all reports, records and receipts as are requested by the Manager so as to enable him/her to ascertain the time expended in the performance of the Extra Work, the quantity of labor and materials used therein and the cost of said labor and materials to the Contractor.

The provisions of this Contract relating generally to Work and its performance shall apply without exception to any Extra Work required and to the performance thereof. Moreover, the provisions of the Specifications relating generally to the Work and its performance shall also apply to any Extra Work required and to the performance thereof, except to the extent that a written order in connection with any particular item of Extra Work may expressly provide otherwise.

If the Contractor deems work to be Extra Work, the Contractor shall give written notice to the Manager within twenty-four (24) hours of performing the work that it so considers as Extra Work, and failure of the Contractor to provide said notice shall be a waiver of any claim to an increase in compensation for such work and a conclusive and binding determination that it is not Extra Work.

The Contractor shall supply the amount of materials, supplies, equipment and personnel required by the Manager within five (5) business days following the receipt of written or verbal notice from the Manager, or in the case of an emergency as determined by the Manager, within twenty four (24) hours following the receipt by the Contractor of the Manager's written or oral notification. Where oral notification is provided hereunder, the Manager shall thereafter confirm the same in writing.

All Extra Work shall be billed to the Port Authority on a separate invoice on a monthly basis.

The Contractor is required to provide separate materials, supplies, equipment and personnel for Extra Work when such is deemed necessary by the Manager. "Extra Work" as used herein shall be defined as work which differs from that expressly or impliedly required by the Specifications in their present form. Total Extra Work performed by the Contractor shall not exceed six percent (6%) of the Total Estimated Contract Price of this Contract for the entire Term of this Contract including extensions thereof, or six percent (6%) of the Total Estimated Contract Price of each Section if this Contract is awarded by separate Sections.

An increase in area or frequency does not constitute Extra Work, but shall be compensated based on the prices in the Pricing Sheet(s) and the paragraph herein titled "Increase or Decrease in Areas or Frequencies."

If the Contractor performs Extra Work which was approved by the Port Authority, the Contractor shall submit a separate invoice to the Port Authority. The invoice package shall contain at minimum the following:

a) A description of the work performed
b) The title and employee name who performed the work
c) The unit price multiplied by the duration of time the work was performed
d) The total amount due
e) The date(s) the work was performed
f) Company name
g) Any supporting documentation (reports, records, receipts, etc.)

The Contractor is required to perform Extra Work pursuant to a written order of the Manager expressly recognizing such work as Extra Work. If Lump Sum or Unit Price compensation cannot be agreed upon by the parties in writing prior to the start of Work, the Contractor shall perform such Extra Work and the Contractor's compensation shall be increased by the sum of the following amounts and such amounts only: (1) the actual net cost, in money, of the Labor, and material, required for such Extra Work; (2) ten percent (10%) of the amount under (1) above; (3) such rental as the Manager deems reasonable for plant and equipment (other than small tools) required for such Extra Work at cost to the Contractor; (4) if the Extra Work is performed by a subcontractor, a five percent (5%) markup of the sum of the amounts under (1) through (3) above in lieu of the (10%) due the contractor if the work were performed itself.

The Manager shall have the authority to decide all questions in connection with the Extra Work. The exercise by the Manager of the powers and authorities vested in him/her by this section shall be binding and final upon the Port Authority and the Contractor.

The Contractor shall submit all reports, records and receipts as are requested by the Manager so as to enable him/her to ascertain the time expended in the performance of the Extra Work, the quantity of labor and materials used therein and the cost of said labor and materials to the Contractor.

The provisions of this Contract relating generally to Work and its performance shall apply without exception to any Extra Work required and to the performance thereof. Moreover, the provisions of the Specifications relating generally to the Work and its performance shall also apply to any Extra Work required and to the performance thereof, except to the extent that a written order in connection with any particular item of Extra Work may expressly provide otherwise.

If the Contractor deems work to be Extra Work, the Contractor shall give written notice to the Manager at least twenty-four (24) hours of performing the work that it so considers as Extra Work, and failure of the Contractor to provide said notice shall be a waiver of any claim to an increase in compensation for such work and a conclusive and binding determination that it is not Extra Work. The Contractor shall not commence any Extra Work or any work it considers Extra Work unless it receives written approval from the Port Authority Manager.

The Contractor shall supply the amount of materials, supplies, equipment and personnel required by the Manager within seven (7) days following the receipt of written or verbal notice from the Manager, or in the case of an emergency as determined by the Manager, within 24 hours following the receipt by the Contractor of the Manager's written or oral notification. Where oral notification is provided hereunder, the Manager shall thereafter confirm the same in writing.

Section 8. Insurance

The Contractor shall take out, maintain, and pay the premiums on Commercial General Liability Insurance, including but not limited to premises-operations, products-completed operations, and independent contractors coverage, with contractual liability covering the obligations assumed by the contractor under this contract, AND, if vehicles are to be used to carry out the performance of this Contract, then the Contractor shall also take out, maintain, and pay the premiums on Automobile Liability Insurance covering owned, non-owned, and hired autos in the following minimum limits:

Commercial General Liability Insurance - $ 5 million combined single limit per occurrence for bodily injury and property damage liability.

Automobile Liability Insurance - $ 5 million combined single limit per accident for bodily injury and property damage liability.

In addition, the liability policy(ies) shall name The Port Authority of New York and New Jersey as additional insured, including but not limited to premises- operations, products-completed operations on the Commercial General Liability Policy. Moreover, the Commercial General Liability Policy shall not contain any provision which would limit the scope of coverage from standard Commercial General Liability coverage. The liability policy (ies) shall contain a cross-liability or separation of insureds clause so that coverage will respond as if separate policies were in force for each insured. Furthermore, the Contractor's insurance shall be primary. These insurance requirements shall be in effect for the duration of the contract to include any warrantee/guarantee period.

The liability policy (ies) must contain the following endorsement for the above liability coverages and must appear in its entirety, on the certificate of insurance:

"The insurer(s) shall not, without obtaining the express advance written permission from the General Counsel of the Port Authority, raise any defense involving in any way the jurisdiction of the Tribunal over the person of the Port Authority, the immunity of the Port Authority, its Commissioners, officers, agents or employees, the governmental nature of the Port Authority, or the provisions of any statues respecting suits against the Port Authority."

The Contractor shall also take out, maintain, and pay premiums on Workers' Compensation Insurance in accordance with the requirements of law in the state(s) where work will take place, and Employer's Liability Insurance with limits of not less than $1 million each accident.

Each policy above shall contain a provision that the policy may not be canceled, terminated, or modified without thirty (30) days' prior written notice to the Port Authority of New York and New Jersey, **Att: Facility Contract Administrator,** at the location where the work will take place and to the **General Manager, Risk Management**, 225 Park Ave South, New York, NY 10003.

The Port Authority may at any time during the term of this Contract change or modify the limits and coverages of insurance. Should the modification or change results in an additional premium, The General Manager, Risk Management for the Port Authority may consider such cost as an out-of-pocket expense.

Within five (5) days after the award of this agreement or contract and prior to the start of work, the Contractor must submit an original certificate of insurance, to the Port Authority of New York and New Jersey, Facility Contract Administrator, at the location where the work will take place. This certificate of insurance MUST show evidence of the above insurance policy (ies) stating the agreement/contract number prior to the start of work. The General Manager, Risk Management must approve the certificate(s) of insurance before any work can begin. Upon request by the Port Authority, the Contractor shall furnish to the General Manager, Risk Management, a certified copy of each policy.

If at any time the above liability insurance should be canceled, terminated, or modified so that the insurance is not in effect as above required, then, if the Manager shall so direct, the Contractor shall suspend performance of the Contract at the Facility. If the Contract is so suspended, no extension of time shall be due on account thereof. If the Contract is not suspended (whether or not because of omission of the Manager to order suspension), then the Port Authority may, at its option, obtain insurance affording coverage equal to the above required, the cost of such insurance to be payable by the Contractor to the Port Authority.

Renewal certificates of insurance or policies shall be delivered to the Facility Contract Administrator, Port Authority at least fifteen (15) days prior to the expiration date of each expiring policy. The General Manager, Risk Management must approve the renewal certificate(s) of insurance before work can resume on the facility. If at any time any of the certificates or policies shall become unsatisfactory to the Port Authority, the Contractor shall promptly obtain a new and satisfactory certificate and policy.

The requirements for insurance procured by the Contractor shall not in any way be construed as a limitation on the nature or extent of the contractual obligations assumed by the Contractor under this contract. The insurance requirements are not a representation by the Port Authority as to the

adequacy of the insurance to protect the Contractor against the obligations imposed on them by law or by this or any other Contract. **[CITS#4003N]**

Section 9. <u>Holidays</u>

The following holidays will be observed at the Site of the Work:

New Year's Day	Columbus Day
Martin Luther King Day	Veteran's Day
President's Day	Thanksgiving Day
Memorial Day	Day after Thanksgiving
Independence Day	Christmas Day
Labor Day	

and such other days as may be declared holidays by the legislature of the state in which the work is to be performed. This list is subject to periodic revision and the Contractor shall be responsible for obtaining all updated lists from the Port Authority Manager.

No work shall be performed on a holiday without the Port Authority's Manager's approval. The Port Authority reserves the right to order work on a holiday.

Contractor employees who work directly under this Contract shall not receive additional compensation for services provided on a Holiday.

Project Managers may elect to not work on such Holidays, subject to Port Authority approval. Security Auditors are expected to work on Holidays.

Section 10. <u>Increase or Decrease in Areas or Frequencies</u>

The Manager shall have the right, at any time and from time to time in his/her sole discretion, to increase or decrease the frequencies of all or any part of the services required hereunder and/or to add areas not described herein in the Specifications or remove areas or parts of areas which are hereunder so described. In the event the Manager decides to change any frequencies or areas such change shall be no less than 24 hours prior oral notice (to be confirmed in writing) or by written notice not less than 30 days, said changes to be effective upon the date specified in said notice.

In the event of an increase or decrease in areas or frequencies, the Contractor's compensation will be adjusted to reflect such change in areas or frequencies utilizing the applicable Unit Price for such services (for the applicable Contract year) as set forth on the Pricing Sheet(s).

Where no specific Unit Price has been quoted for the type of services to be increased or decreased, the Manager shall have the right to negotiate the compensation to reflect such change, whether an increase or decrease in areas or frequencies, which, in the opinion of the Manager, are necessary to complete the work, by multiplying the increased or decreased amount by the negotiated rate.

In the event of a decrease, the Contractor shall not be entitled to compensation for Work not performed.

Any increases in frequencies or areas shall not constitute Extra Work and, as such, shall not be limited by the Extra Work provisions of this Contract.

Section 11. Liquidated Damages

The Contractor's obligations for the performance and completion of the work within the time or times provided for in this Contract are of the essence. In the event the Contractor fails to satisfactorily perform all or any part of the work required hereunder in accordance with the requirements set forth in the Specifications (as the same may be modified in accordance with provisions set forth elsewhere herein) then, inasmuch as the damage and loss to the Port Authority for such failure to perform includes items of loss whose amount will be incapable or very difficult of accurate estimation, the damages for such failure to perform shall be liquidated as follows: the Manager shall determine whether the Contractor has performed in a satisfactory manner and their determination shall be final, binding and conclusive upon the Contractor.

Failure of the Port Authority to impose liquidated damages shall not be deemed Port Authority acceptance of unsatisfactory performance or a failure to perform on the part of the Contractor or a waiver of its remedies hereunder.

a. Failure to Provide Required Titles or Perform Title Functions

In the event the Contractor fails to provide any of the required titles listed in this Contract or perform any of the applicable title functions listed in this Contract, then inasmuch as the damage and loss to the Port Authority, including disruption of the operation at the Facility and disruption of Security at the Facility, which will result from the non-performance of the portion of the Service not performed, cannot be easily calculated and may be incapable of determination, then in lieu of and in liquidation of damages for such breach, the amount payable by the Port Authority to the Contractor hereunder shall be reduced by an amount equal to the product obtained by multiplying two-hundred percent (200%) of the applicable hourly charge or charges set forth in the Contractors Pricing form, as the same may have been adjusted, by the number of hours or major fractions thereof that the Contractor fails to provide the Services (it being understood that in no event shall any amount be payable by the Port Authority for Service hours not actually provide by the Contractor), said amount or amounts to be deducted from any sums due to owing from the Port Authority to the Contractor as the Port Authority shall determine from time to-time, in its sole discretion.

b. Failure to Meet System Implementation Schedules

In the event that, for any reason, the Contractor fails to adhere to the system implementation schedule(s) and complete system implementation in its entirety by Contract completion dates, then inasmuch as the damage and loss to the Port Authority, including disruption of the operation at the Facility and disruption of Security at the Facility, which will result from the non-performance of the portion of the Service not performed, cannot be easily calculated and may be incapable of determination, then in lieu of and in liquidation of damages for such breach, the amount payable by the Port Authority to the Contractor hereunder shall be reduced by an amount equal to the product obtained by multiplying two-hundred percent (200%) of the applicable title hourly charge or charges set forth in the Contractors Pricing form, as the same may have been adjusted, by the number of hours or major fractions thereof the Contractor fails to meeting the implementation schedule or complete system implementation. Said amount or amounts to be deducted from any sums due to owing from the Port Authority to the Contractor as the Port Authority shall determine from time to-time, in its sole discretion.

c. Failure to Limit Employee Work Time

In the event the Contractor has its employees work more than twelve (12) hours per day as prohibited in this Contract, then inasmuch as the damage and loss to the Port Authority,

including disruption of the operation at the Facility and disruption of Security at the Facility, which will result from the non-performance of the portion of the Service not performed, cannot be easily calculated and may be incapable of determination, then in lieu of and in liquidation of damages for such breach, the amount payable by the Port Authority to the Contractor hereunder shall be reduced by an amount equal to the product obtained by multiplying two-hundred percent (200%) of the applicable hourly charge or charges set forth in the Contractors Pricing form, as the same may have been adjusted, by the number of hours or major fractions thereof for every hour the employee works more than twelve (12) hours. Said amount or amounts to be deducted from any sums due to owing from the Port Authority to the Contractor as the Port Authority shall determine from time to-time, in its sole discretion.

d. Failure to Meet Personnel Qualifications

In the event that, for any reason, the Contractor fails to have its employees meet or maintain the applicable personnel qualifications in this Contract, then, inasmuch as the damage and loss to the Port Authority, including disruption of the operation of the Facility and disruption of the security service at the Facility which will result from such non-performance cannot be easily calculated and will be incapable of determination, then in lieu of and in liquidation of damages for such breach, the amount payable by the Port Authority to the Contractor hereunder shall be reduced by an amount equal to One Hundred Dollars ($100) per day multiplied by the number of days or major fractions thereof the Contractor fails to have its employees meet or maintain the applicable personnel qualifications in this Contract. The said amount or amounts are to be deducted from any sums due and owing from the Port Authority to the Contractor hereunder as the Port Authority shall determine from time to time in its sole discretion.

e. Failure to Develop/Update and Submit Accurate Training Curricula

In the event that, for any reason, the Contractor fails to develop or update, complete and submit accurate training curricula by a mutually agreed upon date between the Contractor and the Port Authority, then, inasmuch as the damage and loss to the Port Authority, including disruption of the operation of the Facility and disruption of the security service at the Facility which will result from such non-performance cannot be easily calculated and will be incapable of determination, then in lieu of and in liquidation of damages for such breach, the amount payable by the Port Authority to the Contractor hereunder shall be reduced by an amount equal to One Hundred Dollars ($100) per day multiplied by the number of days or major fractions thereof the Contractor fails to develop or update, complete and submit accurate training curricula. The said amount or amounts are to be deducted from any sums due and owing from the Port Authority to the Contractor hereunder as the Port Authority shall determine from time to time in its sole discretion.

f. Failure to Provide Accurate Documentation, Reports, Records or Invoices

In the event that, for any reason, the Contractor fails to maintain or provide or have available when required or requested by the Port Authority or fails to submit and/or secure any accurate and correct documentation, reports, records or invoices as required, then, inasmuch as the damage and loss to the Port Authority, including disruption of the operation of the Facility and disruption of the security service at the Facility which will result from such non-performance cannot be easily calculated and will be incapable of determination, then in lieu of and in liquidation of damages for such breach, the amount payable by the Port Authority to the Contractor hereunder shall be reduced by an amount equal to One Hundred Dollars ($100) per day documentation, report or records not provided multiplied by the number of

days or major fractions thereof that the Contractor fails to maintain or provide any documentation, reports or records, said amount or amounts to be deducted from any sums due and owing from the Port Authority to the Contractor hereunder as the Port Authority shall determine from time to time in its sole discretion.

Nothing contained in this Section nor the exercise of any right by the Port Authority hereunder shall be deemed to be a waiver or relinquishment of any rights by the Port Authority or any other right it may have hereunder including any right to terminate this agreement based on the Contractor's breach or at Law or in equity.

Section 12. Specifications

The Contractor shall furnish personnel to performance on-site security audit services.
Under the terms and conditions of this Contract, the Contractor shall provide staff to perform on-site security audit services as described herein at John F. Kennedy International (JFK), Newark Liberty International (EWR), LaGuardia (LGA), Teterboro (TEB), Stewart International (SWF) Airports, and the World Trade Center Site (WTC) sometimes collectively or individually, as the context may require, referred to as "the Facility" or "Facilities."

Section 13. Job Classifications

a. Airport Security Auditors
b. Project Managers

Please note all Contractor staff are prohibited from carrying any firearms on the premise of any facilities.

Section 14. Specific Skill Personnel Requirements

The Contractor shall furnish competent and adequately trained personnel to perform the security audit services required hereunder.

Please note all Contractor staff are prohibited from carrying any firearms on the premise of any facilities.

All personnel assigned by the Contractor to provide services under this Contract must comply and successfully complete all background investigation, training and testing procedures to receive a Port Authority airport/WTC ID with appropriate privileges as required by 49 C.F.R. Part 1542 and Port Authority rules, policies and procedures pertaining to security. All personnel assigned by the Contractor to provide services under this Contract must comply with all WTC security requirements for unescorted access within the WTC site. The Port Authority may impose, increase, and/or upgrade security requirements for the Contractor, subcontractors and their staff during the term of this Contract to address changing security conditions and/or new governmental regulations.

All personnel assigned by the Contractor must have in their possession at all times while providing services under this Contract their company ID card and unexpired airport ID card or unexpired WTC ID card, as applicable.

Prior to the assignment of any personnel to the Contract as a Security Auditor or Project Manager, the Contractor shall furnish to the Port Authority resumes which detail their experience and qualifications. The Port Authority will at any time have the right to reject an employee or

prospective employee, of the Contractor, for work associated with this Contract. The Port Authority may require an interview prior to the assignment of any personnel to this Contract.

Personnel currently assigned to this Contract and who will be assigned to this Contract who do not:

a) meet the personnel qualifications listed in this section
b) successfully pass the drug and alcohol testing requirements
c) successfully pass the physical examination (if applicable)

may not work under this Contract without the express written permission of the Port Authority. It is the responsibility of the Contractor to inform the Port Authority of any person(s) who do not meet any personnel qualifications.

The Port Authority shall have the right to waive any of the below listed requirements if, in the sole opinion of the Port Authority, special circumstance warrant such action.

a) Security Auditors

Security Auditors shall meet the following minimum qualifications:

i. Have a minimum of ten (10) years of professional experience in the provision of security audit services or security non-guard services (e.g. police officer, federal agent/inspector, licensed private investigator, licensed private investigator, security supervisor, etc.)

ii. A four-year degree from an accredited USA college or university is preferred. However, a Port Authority approved equivalent will be considered if requested in writing by the Contractor

iii. Have demonstrated knowledge of TSA regulations, airport operations and similar types of security audits. Experience in construction environments is desirable

iv. Be eligible and legally permitted to perform the work contemplated herein, in the United States of America.

v. Be fluent (read, write and speak) in the English language

vi. Must be physically able to perform security audits. Physically fit is defined as being able to:
- Stand or walk for an entire shift
- Climb multiple sets of stairs, escalators and ladders
- Withstand exposure to extreme weather conditions for an entire shift
- Open heavy entry and/or exit doors (e.g. steel or fireproof doors)

vii. Security Auditors and Project Managers are subject to an annual physical examination. Security Auditors must be in general good health without physical defects or abnormalities which would interfere with the performance of security audits hereunder including, but not limited to, the following:
- Not less than 20-30 corrected vision in each eye
- No color and/or depth perception confusion or impairment
- Unimpaired hearing

b)Project Managers

The Airport/WTC Security Manager shall approve the Project Managers prior to commencement of the Contract. Project Managers shall meet the minimum qualifications:

i. Have a minimum of ten (10) years in management and supervisory experience in the provision of security audit services or non-guard security related services (e.g. police officer, federal agent/inspector, licensed private investigator, security inspector, etc.)

ii. A four-year degree from an accredited USA college or university is preferred. However, a Port Authority approved equivalent will be considered if requested in writing by the Contractor

iii. Demonstrated knowledge of TSA regulations, airport operations and similar types of security audits and construction environments is desirable

iv. Be eligible and legally permitted to perform the work contemplated herein, in the United States of America

v. Be fluent (read, write and speak) in the English language

vi. Have demonstrated experience in performing security audits

vii. Must be physically able to perform security audits. Physically fit is defined as:
   a. Stand or walk for an entire shift
   b. Climb multiple sets of stairs, escalators and ladders
   c. Withstand exposure to extreme weather conditions for an entire shift
   d. Open heavy entry and/or exit doors (e.g. steel or fireproof doors)

viii. Demonstrated experience conducting trainings is desirable

ix. Security Auditors and Project Managers are subject to an annual physical examination. Project Managers must be in general good health without physical defects or abnormalities which would interfere with the performance of security audits hereunder including, but not limited to, the following:
   a. Not less than 20-30 corrected vision in each eye
   b. No color and/or depth perception confusion or impairment
   c. Unimpaired hearing

x. Must possess the following computer/word processing/internet skills. Please note this listing is not all inclusive:
   - **Must possess basic computer skills, such as being able to:**
     - Use email (read, compose, delete, respond, forward)
     - Understand basic components of a computer (monitor, CPU, Storage)
     - Use of a keyboard (finding letters without looking)
     - Use of mouse to move cursor, click, double click, click and drag,
     - Use icons to open programs
     - Use start menu to open programs

- Use of Windows features (minimize, resize, maximize and exit buttons)
- Use menu bars (drop down boxes)
- Use of tool bars
- How to scroll
- Understand the basic types of computer storage (hard drive, flash drive, etc)
- Understand the how to save and open files from flash drives (USB)
- Find files using "My Computer" or " Windows Explorer"
- Create, rename, or delete folders
- Turn on/off monitor
- Turn on/off computer
- Log on/off computer
- Identify computer parts (keyboard, monitor, screen, mouse, volume control, USB ports, etc)
- Locate and retrieve documents in CD drives, shared drives, USB ports, etc

- **Must possess Word Processing skills, such as being able to:**
  - Locate and use Function Keys (capital, shift, spacebar, enter, backspace/delete, arrows, etc)
  - Change size/color/font/style of text
  - Use spell check correctly
  - Use edit/undo buttons
  - Move, copy and paste text within document and to other documents
  - Use bulleted and numbered lists

- **Must be Internet proficient, such as being able to:**
  - Use Internet Explorer on different various web browsers in Windows
  - Use web browser to search on specific sites
  - Use online search techniques to solve problems
  - Use web-based training programs
  - Use navigation bars on web sites
  - Use of links on web sites
  - Use Back/Forward buttons, Home button (house icons)

Section 15. <u>Duties of Staff</u>

The Port Authority shall have the right at any time and from time to time in its sole discretion to increase or decrease the anticipated hours to be provided by the Contractor hereunder. In the event the Port Authority decides to increase or decrease the number of scheduled Security Auditors and their hours, it shall give not less than twenty four (24) hours prior oral notice (to be confirmed in writing) to the Contractor to such effect; said changes to be effective upon the date specified in the said notice. In the event that such increase in hours requires that the Contractor train additional employees, the Contractor will be given up to two (2) weeks to arrange for employees to be hired, trained and on duty. Additional conditions shall apply to the increase or decrease the number of Contract employees and/or hours. Please refer to the Contract Specific Terms and Conditions, Increase and Decrease in Areas or Frequencies.

Training costs and expenses for new employees are to be paid for by the Contractor at no separate reimbursable charge to the Port Authority. Payment for such additional Security Auditor hours shall be at the same hourly rate then in effect.

The Contractor shall provide the security audit services at such times and places and in such a manner as the Port Authority shall direct or approve in accordance with the terms and provisions hereof. The Contractor shall immediately correct any aspect of the service which shall have been determined to be unsatisfactory hereunder or which, in the opinion of the Port Authority, is likely to result in unsatisfactory performance of services hereunder.

The Contractor and its employees working directly under this Contract are prohibited from actively working for an existing Aviation/Airline/Tenant, which is present at a Port Authority facility unless the Port Authority gives written approval.

a) WTC Security Auditors - Operating Procedures and Requirements

A thorough facility evaluation should be accomplished in a time period not to exceed two hours. The security audits will be conducted at various times within the 24 hr day, on weekends, and holidays, to ensure all time periods (peak and non-peak) are covered.

Procedures for security audits at the WTC shall be developed jointly by the Port Authority and the Contractor to address the current security procedures in effect at the WTC Site.

b) Airport Security Auditors - Operating Procedures and Requirements

A thorough terminal/cargo area/building/cargo facility audit should be accomplished in approximately three to four hours. The security audits will be conducted at various times throughout the year. All time periods are covered, twenty four (24) hours per day, seven (7) days per week, and weekends and holidays. This coverage will ensure that peak and non-peak performance are being addressed.

The Contractor shall furnish Security Auditors as directed by the Port Authority on a twenty four (24) hour a day availability, every day of the year. It is estimated but not guaranteed that the number of hours per month will total approximately 1,355 - 1,505 hours. Approximately twenty five percent (25%) of the 1,355 - 1,505 hours are anticipated, but not guaranteed, to be scheduled during late shifts (between 11:00 PM and 7:00 AM EST), on holidays, or weekends. The estimated hours will be broken down by facility as per the following estimates: JFK (six hundred and fifty (650) hours), EWR (three hundred and twenty five (325) hours), LGA (two hundred and twenty (220) hours), TEB (ten (10) hours) and SWF (fifty (50) hours).

Payment for time expended by Security Auditors will be based on actual hours worked and actual demonstrated hours worked on the sign-in sheet.

Security Auditors are prohibited from actively working in a law enforcement capacity.

Security Auditors shall comply with the below procedures while performing security audits:

i. The Port Authority shall allow from time to time the Security Auditor to review airport and/or airline/cargo facilities security plans prior to the commencement of a security audit. It is the Security Auditor's responsibility to review and understand these plans.

ii. Check TSR 1542, alarmed and access controlled doors/access points to ensure they are secured and functioning properly. These doors may lead to aircraft,

baggage make-up, ramp or other secured areas. While checking doors and/or access points, the terminal building should be checked for any obvious security risks (i.e., open and unattended boarding for loading of passengers, etc.).

iii. Random sampling of fire exit doors to:
- Determine if they are secured, alarmed, and operating correctly
- Observe Security Operations Console (SOC)
- Check security procedures and response time by security or airport staff to a breach of fire exit doors.

iv. Attempt to access ramp areas without using proper identification through:
- magnetic swipe card reader door
- fire exit door
- piggybacking
- offices, maintenance shops, etc.
- jetway and aircraft
- other (e.g. perimeter fencing, baggage doors, cargo doors, etc.)

v. Evaluate if Security Guards and Airport Personnel who have unescorted access to the SIDA/AOA comply with the airport security procedures within the SIDA/AOA by:
- Verifying airport personnel airport identification (airport ID card) is valid and properly displayed
- Checking if airport personnel challenge individuals on the SIDA/AOA who do not properly display their airport ID cards. For those individuals who do not challenge, the Security Auditor must issue a BOR.

vi. Observe guard posts and attempt to obtain ramp access without following TSA requirements.

vii. Observe RON (Remain Over Night) Aircraft to ensure airport personnel is following required TSA procedures.

viii. Test and assess other security policies, practices, and procedures as directed and propose new "best practices" to the Project Manager.
- Security Auditors shall be rotated amongst the airports to reduce recognition by airport personnel.

- Audits will be performed in accordance with the Contractor's schedule as approved by the Port Authority or at specific facilities identified by the Port Authority. The Contractor's schedule can be changed by the Port Authority due to the operational needs or to address specific problem areas.

- Security Auditors will be required to sign in at the beginning of a shift and out at the end of a shift, when they are on the airport, at a location designated by the Port Authority.

ix. Within twenty-four (24) hours after an audit, the Security Auditor must submit a written report concerning all major events encountered during his/her shift. This report, along with appropriate copies of any BOR's issued and Challenge (Bogus Bob/Babs) awards or Airport Community Watch awards issued or recommended, will be forwarded to the designated Port Authority representative. Any serious incidents or problems must immediately be bought to the attention of the designated facility representative.

If the Security Auditor discovers a violation of TSA regulations, he/she will notify Port Authority staff or designee of the situation and if applicable, make a recommendation.

Security Auditors will distribute Challenge award tickets (Bogus Bob/Babs tickets) to airport employees they believe have demonstrated exceptional vigilance while performing their duties. In addition, the Security Auditor may recommend airport employees for Airport Security and/or Crime Watch awards through the Airport Community Watch Program. All such recommendations must be made in the Security Auditor's daily report.

With the exception of Stewart International Airport (SWF), in cases where a Security Auditor discovers a violation of TSA regulations, the Security Auditor will issue a Breach of Rules (BOR) to the individual violating regulations, or if the individual cannot be located, a representative from the company that is responsible for the area, or if a representative cannot be located, to the company itself. The Security Auditor will follow pre-defined procedures to distribute copies of the BOR immediately.

In cases where a Security Auditor discovers a violation of TSA regulations at SWF airport, the Security Auditor will notify SWF Operations (845) 567-1562.

c) Project Managers - Operating Procedures and Requirements

The Contractor shall provide each Project Manager five (5) days per week, Monday through Friday, during the hours of 8:00 AM to 5:00 PM exclusive of Port Authority Holidays as hereinafter defined in the section entitled "Holidays." One Project Manager will be stationed at JFK and the other one will be stationed at EWR. The Project Managers may be required to rotate among the facilities. The Project Manager stationed at JFK will have the responsibility of covering JFK and LGA airports and the WTC Site. The Project Manager stationed at EWR airport will have the responsibility of handling EWR, SWF and TEB airports. The Port Authority reserves the right to change the number and/or location of where the Project Managers shall work.

Payment for time expended by Project Managers is covered under the Monthly Management Fee.

The Project Managers will be responsible for the following:

i. Ensuring the consistency and standardization of all operating procedures and management reports related to this Contract at all facilities.

ii. Monitor all activities performed under this Contract and will be the primary contact person who will carry out all directives provided by the Directors or their designees.

iii. Have a direct relationship with the Directors and/or their designees and will communicate all issues relating to each facility covered under the Contract to the relevant Director or his or her designees.

Compensation for the Project Manager shall be included in the Monthly Management Fee.

The Project Managers will perform duties which include, but are not limited to, the following:

i. On behalf of the Contractor, handle the administration of this Contract, carry out the directions of the Port Authority, and meet and communicate with Port Authority representatives from the facilities from time to time as required.

ii. Resolve any issues with the Port Authority related to this Contract.

iii. Ensure appropriate Contractor personnel are available for duty including the assignment of replacement personnel, as necessary.

iv. Represent the Contractor at meetings at the facilities, as may be directed by the Port Authority, which concern the operations of the Contractor under this Contract.

v. Be available on-call twenty-four (24) hours a day, to assist and advise the Port Authority on the operations of the Contractor hereunder. If called and requested by the Port Authority, the Project Manager must be on site within four (4) hours of notification. If the Project Manager is not available, the Contractor must appoint a designee which is approved by the Port Authority in place of the Project Manager. In addition, communications equipment that is compatible with the Port Authority system is required. Currently the airport staff uses Sprint/Nextel and the WTC personnel uses Nextel/Sprint and/or Verizon service.

vi. Oversee the preparation of all reports and materials as may be required by the Port Authority. He/she will also make a monthly presentation to Port Authority Management staff, facilities staff and/or airline management on improvements, adverse and positive developing trends, recommendations and other significant information. The Contractor must be able to statistically support his/her statements on adverse and positive developing trends, recommendations, etc.

For the WTC Site, he/she will make a quarterly presentation WTC and/or WTC stakeholder, tenant, Contractor, subcontractor community providing audit trends and offering recommendations for improvement.

vii. Attend and/or conduct training as determined by the Port Authority. Attending or conducting such training will be performed during the business hours specified in this Contract. Costs and expenses associated with attending or giving training will be covered under the Monthly Management Fee.

viii. Conduct security audits as required by the Port Authority if a Security Auditor is unavailable. Costs and expenses associated with attending will be covered under the Monthly Management Fee.

ix. For the Airports, be required to demonstrate working knowledge of Transportation Security Administration (TSA) regulations and general airport operating procedures so as to provide guidance to all Security Auditors. For the WTC, required to demonstrate working knowledge of WTC Site procedures, including current security and operating procedures.

x. Ensure all Security Auditors are properly qualified and trained, receive relevant information about this Contract and their duties in a timely and effective manner, and are given the necessary resources to complete their duties as described within this Contract.

xi. All services performed by the Project Managers and other management staff shall be included in the Monthly Management Fee. Other management staff includes any other titles except "Security Auditor" unless the Port Authority gives written pre-approval.

xii. The Contractor's Project Manager will ensure the detailed duty procedures detailed above are scheduled and performed on a weekly basis, or as otherwise directed by the Port Authority.

xiii. Notify the Airport/WTC Security Manager or any Airport Security or Crime Watch recommendations from his/her Security Auditors. If the Airport/WTC Security Manager agrees with the recommendation, the Project Manager can then notify the employee and provide the call number to the Port Authority Police Department to complete and submit an Airport Community Watch application for award consideration.

xiv. Any other unforeseen duties which the Project Manager must perform will be covered under the Monthly Management Fee.

Should the Project Manager delegate any of the duties listed above to another Contract employee who is not a Project Manager, the performance of those services will still be covered under the Monthly Management Fee.

Section 16. <u>Management Authority</u>

The Port Authority Manager shall, at all times, have the authority to request a Contractor employee be removed from the site or re-assigned to another position based upon job performance or violation of Airport Rules and Regulations, Contract requirements, or any other facility rules or regulations that may apply. In the event the Airport/WTC General Manager disapproves of any individual, the Contractor shall substitute said individual with an approved replacement. In the performance of the Contract, the Contractor shall conform to all orders, directions and requirements of the Airport/WTC General Manager and shall perform the Contract to the satisfaction of the Airport/WTC General Manager at such times and in such manner and sequence as she/he may require, and the Contractor's performance shall at all stages be subject to her/his inspection. The Airport/WTC General Manager shall determine the amount,

quality, acceptability and fitness of all parts of the Service and shall interpret the specifications and any orders for extra work. Upon request, the Airport/WTC General Manager shall confirm in writing any oral order, direction, requirements or determination.

Section 17. Attendance Records for Contractor Employees

The Contractor shall maintain accurate daily attendance records for all employees working directly under this Contract for actual hours worked performing security audit services. Contractor employees are required to sign in and out each time they work at a Facility or at any location designated by the Port Authority.

Section 18. Training Requirements

The Contractor agrees prior to Contract commencement and during the term of the Contract at all times, it shall have available a total base workforce sufficient to carry out the Contract requirements. The Contractor agrees prior to the commencement of the Contract, it shall recruit and present a sufficient number of candidates to participate in the Port Authority training program.

Except as otherwise expressly agreed to by the Port Authority, the Contractor may not assign an employee as a Security Auditor or Project Manager unless said employee has successfully completed the airport training program conducted by the Contractor and/or the Port Authority, from time to time, as hereinafter set forth.

The Contractor agrees to cooperate and assist the Port Authority as may be required from time to time and any time, to facilitate the training of the Contractor's personnel hereunder.

a) Initial and Refresher Training for Contractor staff

i. Initial Training for Contractor staff

Initial airport training is expected to take approximately two weeks and will include but not limited to the successful completion of the following courses taught by the Contractor and/or the Port Authority:

- Security Identification Display Area (SIDA) training
- Issuing Officer (IO)/Signatory Authority training
- Customer Care training
- Other Customer Service and/or Security related trainingInitial WTC training is expected to take approximately two days.

All costs and expenses associated with initial training for employees working directly under this Contract shall be borne by the Contractor at no separate reimbursable charge to the PA.

ii. Refresher Training for Contractor staff

The Port Authority may institute an in-service refresher training program as it deems necessary or desirable for any or all of the Contractor's employees hereunder. Refresher training should take no longer than one day to complete. Such training programs for the employees who work directly under this Contract will be provided at the sole cost and expense of the Contractor at no separate reimbursable charge to the PA.

b) Training Materials

The Contractor is required to develop or update Security Audit training manuals. These training manuals are used to help the contract staff perform their job functions out in the field (SIDA/AOA) as they provide detailed narrative information. The Contractor shall develop two (2) manuals for each facility (JFK, LGA, EWR, TEB and SWF airports)

These manuals are subject to Port Authority approval prior to distribution. The materials should at a minimum meet the requirements specified in TSR 1542 and Security Directives (SD) but are not inclusive to them.

These manuals are considered and treated as confidential and proprietary and shall not leave the applicable facility. The Contractor shall not duplicate or disclose any information to any person other than its own employees, agents, or representatives who must have such information unless such duplication, or disclosure is authorized by the Port Authority.

Any development or update to the training manuals must be performed by only one (1) Contract employee and submitted to the Port Authority electronically at least two (2) weeks in advance of implementation. The Contractor must receive written approval by the Port Authority before commencing the work.

Any costs associated with the development or update of the training manuals shall be covered under the Monthly Management Fee (MMF).

Section 19. <u>Materials, Supplies and Equipment</u>

The Contractor shall be responsible for any equipment or furniture issued by the Port Authority. If such issued equipment is unusable due to misuse or negligence on the part of the Contractor, then the Contractor may be required to reimburse the Port Authority. All issued equipment will be tagged and logged on forms specified by the Port Authority.

The Contractor shall provide, at its own expense, a means by which the Security Auditors may at any time, while performing their duties, contact the Port Authority, Project Manager or any other staff designated by the Port Authority.

The Contractor shall provide, at its own expense, a means by which the Port Authority, the Project Manager or any other staff designated by the Port Authority may contact the Security Auditors, while performing their duties.

The Contractor shall provide and utilize Port Authority approved forms to cover the reporting of security operations under this Contract at the facility subject to approval by the Port Authority. The Contractor shall provide all office supplies and equipment excluding a telephone(s). The Contractor will pay telephone service as it is necessary for the daily operation of this Contract.

Materials and equipment such as copies, pens, pencils, laptops and projectors that are used for the delivery of security auditing courses will be provided by the Port Authority.

The Contractor shall subscribe to an electronic mail service such that correspondence can be transmitted thereby. All security correspondence related to audits, audit results, security audit training, schedules of Security Auditors and Project Managers, locations of files, reports, monthly reports, etc., shall not be transmitted via electronic mail until the Port Authority has

approved of the transmission vehicle. The Contractor may have the option to be assigned Port Authority emails for Contract staff.

All technology equipment, hardware and software must meet the Port Authority's Technology Services Department's Standards and Guidelines attached hereto as Attachment G and System Administration Guide as Attachment J.

Section 20. Drug and Alcohol Testing and Physical Examination Requirements

The Contractor shall institute prior to commencement of this Contract, and administer continuously throughout the term of this Contract, a program for initial and recurrent random drug and alcohol testing for all employees assigned to this Contract. The recurrent drug and alcohol testing shall be unannounced and random and shall occur at least once a year. Such drug and alcohol testing shall be conducted by an independent third party with no personal or business relationship to the Contractor except for the provision of drug and alcohol testing. The independent third party Contractor shall conduct testing in accordance with guidelines established by 49 CFR Part 40 Procedures for Transportation Workplace Drug and Alcohol Testing Programs. Testing shall be of the following substances and not be limited to:

Amphetamines
Barbiturates
Benzodiazepenes
Cocaine
Marijuana
Methadone
Methaqualone
Opiates: Morphine (if indicated), Codeine (if indicated), 6MAM if (indicated)
Phencyclidine (PCP)
Propoxyphone

If a Contract employee tests positive for any of the above mentioned substances, he/she is prohibited from working directly on this Contract. It is the Contractor's responsibility to notify the Port Authority if an employee tests positive.

The details of the drug and alcohol testing program will be available to the Port Authority for review prior to the start of this Contract. Any changes to the drug and alcohol testing program will be discussed with the Port Authority prior to implementation.

All associated costs and expenses to perform the drug and alcohol testing shall be borne by the Contractor at no separate reimbursable charge to the Port Authority.

Physical Examination Requirements

The Contractor shall institute prior to the commencement of this Contract, and within each twelve (12) month period thereafter during the terms of this Contract, a program for annual physical examinations for Security Auditors and Project Managers. The Contractor shall arrange the physical examinations. All associated physical examination costs and expenses are borne by the Contractor at no separate reimbursable charge to the PA. Such physical examinations shall be conducted by an independent third party with no personal or business relationship to the Contractor except for the provision of physical examinations.

If a Contract employee cannot pass the physical examination, he/she is prohibited from working directly on this Contract unless Port Authority provides written approval.

Section 21. Identification Requirements

The Contractor shall require each employee working directly under this Contract, to obtain an applicable and valid facility issued ID(s). Security Auditors shall carry on his/her person at all times while performing security audit services in accordance with this Contract. If the Project Manager is performing security audits, he/she shall carry on his/her person at all times a valid facility issued ID(s). The airport ID/WTC ID shall be available for presentation to any Port Authority or other government, airport, airline, or service company personnel upon request.

Section 22. Ineligibility for Challenge (Bogus Bob/Babs) and Airport Community Crime and Security Watch Awards

The Contractor and its entire staff shall be ineligible for Challenge (Bogus Bob/Babs) awards, Airport Community Security and Crime Watch, and any other security-related awards made available from time to time by the Port Authority, the airlines, or the airport community.

Section 23. Security Audit Reporting System: Report Development, Procedures and Record Retention

Currently, the Port Authority requires a Contractor to have a web-based security audit reporting system. If the Port Authority chooses to select a new system, the Contractor is required to retrieve the security audit data in the current system and import them into the new system. It is the Contractor's responsibility to: 1) enter in future security audit results into the new system and 2) maintain the new system. In addition, the Contractor's system must interface with the Identity Management and Credential System (IMCS).

For the WTC Site, this summary report will be broken down by project, contractor, location, and type of activity, and comparisons will be made to prior periods for the same project, contractor, and type of activity. Additional information which may be required for the WTC reports will be determined by the WTC Site Manager.

Additional information which may be required for the WTC reports will be determined by the WTC Site Manager. Daily audit observations at the WTC shall be prepared in report format and submitted within 24 hours of the audit taking place. The audits shall be divided into specific categories as determined by the WTC Site Manager.

A. Record Retention

The Contractor is required to keep all electronic and paper records associated with all security audits (positive and negative results) on file for the entire contract duration. The Contractor agrees it shall develop any reports at the request of the Port Authority. The development of these reports shall be at the cost and expense of the Contractor under the Monthly Management Fee. The Contractor must submit the proposed changes and estimated time in writing to the Port Authority. The Port Authority must agree to these changes prior to the commencement of the report development.

B. Procedure

The Contractor shall present monthly to the Port Authority a summary security audit report on all airports for the previous month. This report should detail findings and indicate any and all developing security trends (positive and negative) at the facilities broken down by: (1) facility, (2) terminal, (3) building, (4) airline, (5) cargo facility and

(6) inspection/audit types (to be used interchangeably). This report must provide comparisons made to similar activities in prior periods.

C. Report Development

The Contractor shall make the required reports and other future report(s) available on this web-based system. The report listing shall be given to the Contractor once the Contract is awarded.

Section 24. Security of Information Plan

The Contractor shall make every effort to secure all documents and information relating to and throughout this Contract. The Contractor will submit electronically and hard copy to the Port Authority a plan which details how it will secure all Contract documentation and information no later than sixty (60) days after Contract commencement. The Port Authority must approve this plan. The Contractor shall refer and comply with the Port Authority Information Security Handbook requirements.

Section 25. Confidentiality – Proprietary Information

The Contractor shall consider information obtained and used for the composition of any reports, manuals, and other materials during the term of this Contract as confidential and proprietary, including such reports, manuals and other materials. The Contractor agrees that it will not, and that it shall take reasonable measures to ensure that its employees, agents and representative shall not, during or after the term of the Contract, permit the duplication, use or disclosure of any such information or materials to any person (other than its own employees, agents or representatives who must have such information) unless such duplication, use or disclosure is specifically authorized by the Port Authority. In addition, employees of the Contractor shall not leave the facility premises with such information. This includes but not limited to reports, analyses, data, and other information, whether written, printed, electronically or magnetically stored, or transmitted verbally.

Upon termination or expiration of the Contract, the Contractor shall surrender to the Port Authority any and all information and records pertaining to the services conducted for this Contract. This includes but not limited to reports, analyses, data, and other information, whether written, printed, electronically or magnetically stored, or transmitted verbally.

All personnel that directly or indirectly work on this Contract whether the Contractor staff is used for support, auditing, or management of the Contract are required to sign the Port Authority Non-Disclosure Agreements.

Section 26. Space Provided to the Contractor

The Port Authority may, at its sole discretion and subject to availability at the facility, furnish the Contractor without charge exclusive or non-exclusive space ("space") for administrative office purposes in connection with this Contract and for the storage of the Contractor's equipment, materials and supplies used on at a facility, which Space shall be taken by the Contractor in its "as is" condition.

The Port Authority shall have the right at any time and as often as it considers necessary, to inspect the Space and (without any obligation to do so) to enter thereon to make ordinary repairs and in the event of an emergency to take such action therein as may be required for the protection of persons and property. The Port Authority, its officers, employees and

representatives shall have the right at all times to enter upon the Space provided the Contractor for the purpose of inspecting the same, for observing the performance of the Contractor of its obligations under this Contract, and for the doing of any act or duty which the Port Authority may be obligated to have the right to do under this Contract or otherwise. The Port Authority shall have the right, from time to time, to re-designate the location of the Space and the Contractor shall, at its own expense, comply therewith.

The Contractor shall repair all damage to the space and all damage to fixtures, improvements and personal property of the Port Authority which may now or may hereafter be located thereon, which may be caused by the operations of the Contractor under this agreement or by acts or omissions of the Contractor, its officers, agents, employees or representatives whether the damage occurs during the course of their employment by the Contractor or otherwise.

Upon the expiration or earlier termination or revocation of this Contract or upon a change of Space or termination of the right to use the Space, the Contractor shall remove its equipment, materials, supplies, and other personal property from the Space. If the Contractor shall fail to remove its property on or before the expiration, termination or revocation of this Contract, or upon a change of Space or termination of the right to use Space, the Port Authority dispose of such property or waste, remove such property to a public warehouse for deposit or retain the same in its own possession, and sell the same at public auction, the proceeds of which shall be applied first to the expenses of removal, storage and sale, second to any sums owned by the Contractor; if the expenses of such removal, storage and sale exceed the proceeds of sale, the Contractor shall pay such excess to the Port Authority upon demand.

The Contractor shall not perform any maintenance (excluding cleaning) and repairs, nor erect any structures, make any improvements or do any other construction work on the Space provided to the Contractor hereunder or elsewhere at the Airport or alter, modify or make additions or repairs to or replacements of any existing structures or improvements, or install any fixtures (other than trade fixtures, removable without injury to the Space) without the prior written approval of the Port Authority and in the event any construction, improvements, alterations, modifications, additions, repairs or replacements are made without such approval, then upon notice so to do, the Contractor will remove the same, or at the option of the Port Authority, cause the same to be changed to the satisfaction of the Port Authority. In case of any failure on the part of the Contractor to comply with such notice, the Port Authority may effect the removal or change and the Contractor shall pay the cost thereof to the Port Authority on demand.

Nothing in the Agreement contained shall give the Contractor the right to sell, and the Contractor shall not sell, or permit to be sold, any merchandise at or on the Space. Nothing in this Agreement contained shall give any right to install, and the Contractor shall not install or permit to be installed, any vending machines or devices at or on the Space.

Upon the expiration or earlier revocation of this Agreement, or upon a change in location constituting the Space, the Contractor shall promptly vacate the area then constituting the Space and leave the same in the condition existing when it was made available to the Contractor, reasonable wear and tear excepted.

Section 27. <u>Contractor's Vehicles – Parking</u>

Contractor employees will use their own personal or company provided vehicle to drive to and from sites of work. Free parking at airports may be provided but it is not guaranteed. The Contractor will receive no additional compensation for the use of personal vehicles.

If there is a parking and/or transportation charge to the Contractor or its employees, the Port Authority will not reimburse the cost(s) or expense(s).

Contractor vehicles will not be Port of New York Authority (PONYA) plated as Contractor employees are prohibited to travel onto the secure areas of the airport with their vehicles. No parking is available at the WTC Site.

Section 28. Employee Uniforms and Appearance

The Contractor will ensure Security Auditors appear to match a cross section of the facility population. Dress Security Auditors should be appropriate for the area in which the work is being performed (i.e. denim for ramp work, business casual for terminal areas).

Dress code for the Project Managers shall be business attire.

Section 29. Transitioning Services at Start/Termination of the Contract

The Contractor shall support an orderly transition from the existing Contractor providing the services to the new Contract. The Contractor is expected to actively participate in discussions and agree to written plans, which clearly specify the transition period and responsibilities.

Section 30. Safety Provisions

For the safety of everyone in the facility environment, no staff assigned to this Contract shall work more than twelve (12) hours per day on any day, either on work associated with this Contract or on any other Contract or any combination thereof. The Contractor is required to adhere to WTC safety provisions, policies and procedures. Subsequent to Contract award, the Contractor is required to contact the WTC Manager for more information.

Section 31. Site Specific Recycling and Trash Removal

In addition to the trash removal requirements listed in the General Contract Provisions, the Contractor is required to properly dispose of any materials which are considered sensitive, confidential, etc. Please refer to the Port Authority Security Information Handbook as Attachment G for more detailed disposal procedures.

Section 32. Limitation on Future Contracting

The Contractor awarded this contract is precluded from being awarded any future Port Authority Contract for guard or security auditing services as a prime contractor or as a subcontractor for the duration of this contract, including any option years or periods, if exercised. The restriction shall apply to any and all affiliates, divisions and subsidiaries of the Contractor. This limitation shall not apply to an award for the replacement contract for the services described herein.

ATTACHMENT B

PART II - GENERAL CONTRACT PROVISIONS

ATTACHMENT B
PART II
GENERAL CONTRACT PROVISIONS

TABLE OF CONTENTS

1. GENERAL AGREEMENT 4

2. DEFINITIONS 4

3. GENERAL PROVISIONS 5

4. INTELLECTUAL PROPERTY 5

5. PROPRIETARY RIGHTS IN SUBJECT MATTER NOT WITHIN THE INTELLECTUAL PROPERTY CLAUSE 6

6. INDEMNITY IN REGARD TO INFRINGEMENT MATTER 7

7. CONTRACT RECORDS AND DOCUMENTS – PASSWORDS AND CODES 8

8. COMPLIANCE WITH WEB SITE TERMS OF USE AND PRIVACY POLICIES 8

9. TIME IS OF THE ESSENCE 8

10. FINAL PAYMENT 8

11. DEFAULT, REVOCATION OR SUSPENSION OF CONTRACT 9

12. WITHHOLDING OF PAYMENT 13

13. CONTRACTOR PERSONNEL STANDARDS OF PERFORMANCE 13

14. DESIGNATED SECURE AREAS 13

15. NOTIFICATION OF SECURITY REQUIREMENTS 14

16. INSURANCE PROCURED BY THE CONTRACTOR 16

17. ASSIGNMENTS AND SUBCONTRACTS 19

18. CERTAIN CONTRACTOR'S WARRANTIES 19

19. RIGHTS AND REMEDIES OF THE AUTHORITY 21

20. RIGHTS AND REMEDIES OF THE CONTRACTOR 22

21. TAX EXEMPTIONS 22

22. TITLE TO EQUIPMENT 22

23. NOTICE REQUIREMENTS 22

24. SERVICE OF NOTICES ON THE CONTRACTOR 23

25. NO THIRD PARTY RIGHTS 23

26. INDEMNIFICATION AND RISKS ASSUMED BY THE CONTRACTOR 23

27. Approval of Methods 25

28. PORT AUTHORITY TECHNOLOGY STANDARDS AND GUIDELINES AND SUPPLEMENTAL GUIDELINES FOR THE PORT AUTHORITY TECHNOLOGY SERVICES DEPARTMENT 25

29. SUBMISSION TO JURISDICTION 25

30. APPLICABLE LAW 25

31. AUTHORITY OF THE DIRECTOR 26

32. APPROVALS BY THE DIRECTOR 27

33. CONTRACT REVIEW AND COMPLIANCE AUDITS 27

34. AUTHORITY ACCESS TO RECORDS 27

35. HARMONY 28

36. CLAIMS OF THIRD PERSONS 29

37. NO DISCRIMINATION IN EMPLOYMENT, EQUAL EMPLOYMENT OPPORTUNITY 29

38. CONTRACTOR'S INTEGRITY PROVISIONS 29

39. CONFIDENTIAL INFORMATION/NON-PUBLICATION 34

40. PROVISIONS OF LAW DEEMED INSERTED 35

41. INVALID CLAUSES 35

42. NO ESTOPPEL OR WAIVER 35

43. NON-LIABILITY OF THE AUTHORITY REPRESENTATIVES 35

44. MODIFICATION OF CONTRACT 36

45. M/WBE GOOD FAITH PARTICIPATION 36

46. ENTIRE AGREEMENT 37

GENERAL CONTRACT PROVISIONS

1. GENERAL AGREEMENT

The undersigned (hereinafter referred to as the "Contractor" or "you") agrees to provide, and The Port Authority of New York and New Jersey (hereinafter referred to as the "Authority") agrees to accept to provide all the necessary supervision, personnel, equipment, materials and all other things necessary to perform the Services required by this Contract as more fully set forth in the Scope of Work attached hereto and made a part hereof. The Scope of Work requires the doing of all things necessary or proper for or incidental to the requirements as set forth in the Scope of Work. All things not expressly mentioned in the Scope of Work but involved in carrying out their intent are required by the Scope of Work and the Contractor shall perform the same as though they were specifically mentioned, described and delineated.

2. DEFINITIONS

As used herein, "Director" shall mean the a Port Authority employee of the Authority acting either personally or through her duly authorized representatives acting within the scope of the particular authority vested in them unless specifically stated to mean acting personally. For the purpose of administering this Agreement, the Director has designated the Project Manager ("PM") to act as his duly authorized representative.

For the purposes of this Agreement the Project Manager (or "Manager") shall be the individual with day-to-day responsibility for managing the project on behalf of the Port Authority. The Project Manager will be Courtney Fong.

As used herein, the term "days" or "calendar days" in reference to a period of time shall mean consecutive calendar days, Saturdays, Sundays, and holidays included.

"Facility" Port Authority Facilities within the Port District, as set forth in Attachment C: "Port Authority Facilities".

"Services" or "Work" - shall mean all services, equipment and materials (including materials and equipment, if any, furnished by the Authority) and other facilities and all other things necessary or proper for, or incidental to the services to be performed or goods to be furnished in connection with the service to be provided hereunder, as set forth in the Scope of Work.

As used herein, the term "Work Day" shall mean a day between Monday and Friday with Monday and Friday included.

As used herein the term "Specifications" shall mean all requirements of this RFP, technical and otherwise, for the performance of the Scope of Work and services hereunder.

Holidays: The following legal holidays will be observed at Port Authority offices and facilities:

New Year's Day	Columbus Day
Martin Luther King, Jr. Day	Veteran's Day
Presidents Day	Thanksgiving Day
Memorial Day	Day After Thanksgiving
Independence Day	Christmas Day
Labor Day	

Do not perform any Work unless authorized by the Authority on these days.

As used herein, the terms "Port Authority" or "Authority" shall mean the Port Authority of New York and New Jersey.

3. GENERAL PROVISIONS

A. Under no circumstances shall you or your subcontractors communicate in any way with any department, board, agency, commission, or other organization or any person whether governmental or private in connection with the services to be performed hereunder except upon prior written approval and instructions of the Director, provided, however, that data from manufacturers and suppliers of materials, devices and equipment shall be obtained by you when you find such data necessary unless otherwise instructed by the Authority.

B. Any services performed for the benefit of the Authority at any time by you or on your behalf, even if expressly and duly authorized by the Authority, shall be deemed to be rendered under and subject to this Agreement (unless referable to another expressly written, duly executed agreement by the same parties), whether such additional services are performed prior to, during or subsequent to the services described herein, and no rights or obligations shall arise out of such additional services except as provided under this Agreement.

C. The Contractor shall observe and obey (and compel its officers, employees, guests, invitees, and those doing business with it, to observe and obey) the rules and regulations of the Port Authority now in effect, and such further rules and regulations which may from time to time during the effective period of this Contract, be promulgated by the Port Authority for reasons of safety, health, preservation of property, or maintenance of a good and orderly appearance of the Facilities, or for the safe and efficient operation of the Facilities. The Port Authority agrees that, except in cases of emergency, it shall give notice to the Contractor of every rule and regulation hereafter adopted by it.

D. This Contract does not constitute the Contractor as an agent or representative of the Port Authority for any purpose whatsoever. The Contractor shall perform all services hereunder as an independent Contractor and the Contractor, its officers, and employees shall not be deemed to be agents, servants, or employees of the Port Authority.

4. INTELLECTUAL PROPERTY

A. Except as provided below: as between the Port Authority and the Contractor all process flows, codes including, but not limited to scripts, programs, routines, processes, procedures, documentation, estimates, reports, records, data, charts, documents, models, designs, renderings, drawings, specifications, photographs, computations, computer tapes or discs, and other documentation of any type whatsoever, whether electronic or in the

form of writing, figures or delineations, which are prepared or compiled in connection with this Agreement, shall become the exclusive property of the Authority, and the Authority shall have the exclusive right to use or permit the use of them and any ideas or methods represented by them for any purpose and at any time without other compensation than that specifically provided for herein. With regard to training manuals or any other knowledge transfer documentation, communication or presentation prepared under this Agreement the Authority shall expressly have the right to use, alter and reproduce including electronically, said manuals for its internal business purposes. The Contractor hereby warrants and represents that the Authority will have at all times the ownership and rights provided for in the immediately preceding sentence free and clear of all claims of third persons whether presently existing or arising in the future and whether presently known to either of the parties to this Agreement or not. Any information given to the Port Authority before, with or after submission of the Agreement on Terms of Discussion, either orally or in writing, is not given in confidence and may be used, or disclosed to others, for any purpose at any time without obligation or compensation and without liability of any kind whatsoever except as otherwise set forth in the Agreement On Terms Of Discussion.

The right to use all patented materials, appliances, processes of manufacture or types of construction, trade and service marks, copyrights and trade secrets, collectively hereinafter referred to as "Intellectual Property Rights", in the performance of the work, shall be obtained by the Contractor without separate or additional compensation. Where the services under this Agreement require the Contractor to provide materials, equipment or software for the use of the Port Authority or its employees or agents, the Port Authority shall be provided with the Intellectual Property Rights required for such use without further compensation than is provided for under this Agreement.

B. All preexisting information or documentation including computer programs or code including source code, of the Contractor, utilized by the Contractor hereunder in the performance of his services hereunder shall be deemed licensed to the Authority for the duration and purposes of this agreement, but shall remain the property of the Contractor.

C. When in the performance of the contract services the Contractor utilizes passwords or codes for any purpose, at any time during or after the performance of such services, upon written request by the Authority, the Contractor shall make available to the designated Authority representative all such passwords and codes.

D. Third party software not specially prepared for the purpose of this agreement but utilized by the Contractor hereunder in the performance of his services hereunder shall be licensed to the Contractor and the Authority for the duration and purposes of this agreement but shall remain the property of said third party.

E. The above-described software shall be furnished by the Contractor without additional compensation.

5. PROPRIETARY RIGHTS IN SUBJECT MATTER NOT WITHIN THE INTELLECTUAL PROPERTY CLAUSE

If in accordance with this Contract the Contractor furnishes research, development or consultative services in connection with the performance of the Work and if in the course of such research, development, or consultation patentable or copyrightable subject matter or trade secrets or other

proprietary matter is produced by the Contractor, its officers, agents, employees, subcontractors, or suppliers, not custom software, and not covered under clause 6 entitled Intellectual Property, the Authority shall have, without cost or expense to it, an irrevocable, non-exclusive, royalty-free license to make, have made, and use, either itself or by anyone on its behalf, such subject matter in connection with any activity now or hereafter engaged in or permitted by the Authority. Promptly upon request by the Authority, the Contractor shall furnish or obtain from the appropriate person a form of license satisfactory to the Authority, but it is expressly understood and agreed that as between the Contractor and the Authority the license herein provided for shall nevertheless arise for the benefit of the Authority immediately upon the production of said subject matter and shall not await formal exemplification in a written license agreement as provided for above. Such license may be transferred by the Authority to its successors, immediate or otherwise, in the operations of or ownership of any facility now or hereafter operated by the Authority or the Authority but such license shall not be otherwise transferable.

The right of the Authority as well as the Contractor to use all patented material, compositions of matter, manufactures, apparatus, appliances, processes of manufacture or types of construction as well as any copyrightable matter, trade secrets or other proprietary matters, shall be obtained by the Contractor without separate or additional compensation whether the same is patented or copyrighted before, during or after the performance of the Work.

6. INDEMNITY IN REGARD TO INFRINGEMENT MATTER

The Contractor shall indemnify the Authority against and save it harmless from all loss and expense incurred in the defense, settlement or satisfaction of any claims in the nature of patent, copyright, or other proprietary rights infringement arising out of or in connection with the Authority's use, in accordance with the preceding clause of such patentable subject matter or patented material, compositions of matter, manufactures, apparatus, appliances, processes of manufacture or types of construction, or copyrighted matter or other matter protected as intellectual property. If requested by the Authority and if notified promptly in writing of any such claims, the Contractor shall conduct all negotiations with respect to and defend such claim without expense to the Authority. If the Authority be enjoined from using any of the facilities which form the subject matter of this Contract, and as to which the Contractor is to indemnify the Authority against proprietary rights claims, the Authority may, at its option and without thereby limiting any other right it may have hereunder or at law or in equity, require the Contractor to supply, temporarily or permanently, facilities not subject to such injunction and not infringing any proprietary rights and if the Contractor shall fail to do so, the Contractor shall, at its expense, remove all such facilities and refund the cost thereof to the Authority and otherwise equitably adjust compensation and take such steps as may be necessary to ensure compliance by the Authority with such injunction, to the satisfaction of the Authority.

The Contractor shall promptly and fully inform the Director of any claims or disputes for infringement or otherwise, whether existing or potential, of which it has knowledge relating to any Intellectual Property used, developed or licensed in connection with the performance of the Work or otherwise in connection with this Contract.

7. CONTRACT RECORDS AND DOCUMENTS – PASSWORDS AND CODES

When the performance of the contract services requires the Contractor to produce, compile or maintain records, data, drawings, or documents of any kind, regardless of the media utilized, then all such records, drawings, data and documents which are produced, prepared or compiled in connection with this contract, shall become the property of the Port Authority, and the Port Authority shall have the right to use or permit the use of them and any ideas or methods represented by them for any purpose and at any time without other compensation than that specifically provided herein.

When in the performance of the contract services the Contractor utilizes passwords or codes for any purpose, at any time during or after the performance of such services, upon written request by the Authority, the Contractor shall make available to the designated Authority representative all such passwords and codes.

8. COMPLIANCE WITH WEB SITE TERMS OF USE AND PRIVACY POLICIES

Subject to all of the provisions of this Contract including, without limitation, the obligations of the Contractor under the section hereof entitled "Indemnification", the Contractor shall, and shall compel its employees, agents and subcontractors, to strictly abide by and comply with the policies established by the Authority governing the use of the Authority's web sites as set forth in the Authority web sites Terms of Use and Privacy Statement as the same may be supplemented or amended. The Contractor shall immediately implement all procedures in connection with such policies and in furtherance thereof as directed by the Authority.

9. TIME IS OF THE ESSENCE

The Contractor's obligations for the performance and completion of all work within the time or times provided for in this Contract are of the essence of this Contract.

10. FINAL PAYMENT

After satisfactory completion of all services required hereunder, and upon receipt from the Contractor of such information as may be required, the Director shall certify in writing to the Contractor the total compensation earned by the Contractor.

If so required, the Contractor shall thereupon furnish to the Authority a detailed sworn statement of all claims, just and unjust, of subcontractors, materialmen and other third persons then outstanding which he has reason to believe may thereafter be made on account of the services provided under this Agreement.

Within thirty days after issuance of such certificate of total compensation earned (or within thirty days after receipt of the documents provided for in the immediately preceding paragraph, if required and if such date is later), the Port Authority shall pay to the Contractor by check the amount stated in said certificate, less all other payments and advances whatsoever to or for the account of the Contractor. All prior estimates and payments shall be subject to correction in this payment, which is throughout this Agreement called the Final Payment.

The acceptance by the Contractor, or by anyone claiming by or through him, of the Final Payment shall be and shall operate as a release to the Authority of all claims and of all liability to the Contractor for all things done or furnished in connection with this contract and for every act and

neglect of the Authority and others relating to or arising out of the this contract, including claims arising out of breach of the contract and claims based on claims of third persons.
The Contractor's agreement as provided in the immediately preceding paragraph shall be deemed to be based upon the consideration forming part of this Contract as a whole and not to be gratuitous; but in any event even if deemed gratuitous and without consideration, such agreement as provided in the immediately preceding paragraph shall nevertheless be effective. Such release shall include all claims, whether or not in litigation and even though still under consideration by the Authority. Such release shall be effective notwithstanding any purported reservation of right by the Contractor to preserve such claim. The acceptance of any check designated as "Final Payment" or bearing any similar designation shall be conclusively presumed to demonstrate the intent of the Contractor that such payment was intended to be accepted as final, with the consequences provided in this numbered clause, notwithstanding any purported reservation of rights.

The Contractor agrees that he shall not be entitled to, and hereby waives any right he might otherwise have to, and shall not seek any judgment whether under this Contract or otherwise for any such Final Payment or for an amount equivalent thereto or based thereon, or for any part thereof, if such judgment would have the effect of varying, setting aside, disregarding or making inapplicable the terms of this numbered clause or have the effect in any way of entitling the Contractor to accept such Final Payment or an amount equivalent thereto or based thereon or any part thereof other than in the same fashion as a voluntary acceptance of a Final Payment subject to all the terms of this Contract including this numbered clause, unless and until the Contractor should obtain a judgment on any claim arising out of or in connection with this Contract (including a claim based on breach of contract) for an amount not included in said Final Payment.

11. DEFAULT, REVOCATION OR SUSPENSION OF CONTRACT

A. If one or more of the following events shall occur:

1. If fire or other event shall destroy all or a substantial part of the Facility, asset or infrastructure necessary to perform the Scope of Work.

2. If any governmental agency shall condemn or take a temporary or permanent interest in all or a substantial part of the Facility, or all of a part of the Port Authority's interest herein;

then upon the occurrence of such event or at any time thereafter during the continuance thereof, the Port Authority shall have the right on twenty-four (24) hours written notice to the Contractor to revoke this Contract, such revocation to be effective upon the date and time specified in such notice.

In such event this Contract shall cease and expire on the effective date of revocation as if said date were the date of the expiration of this Contract. Such revocation shall not, however, relieve the Contractor of any liabilities or obligations hereunder which shall have accrued on or prior to the effective date of revocation.

B. If one or more of the following events shall occur:

1. The Contractor shall become insolvent, or shall take the benefit of any present or future insolvency statute, or shall make a general assignment for the benefit of creditors, or file a voluntary petition in bankruptcy or a petition or answer seeking an arrangement or its reorganization or the readjustment of its indebtedness under the federal bankruptcy laws or under any other law or statute of the United States or of any State thereof, or consent to the appointment of a receiver, trustee, or

liquidator of all or substantially all its property; or

2. By order or decree of a court the Contractor shall be adjudged bankrupt or an order shall be made approving a petition filed by any of the creditors, or, if the Contractor is a corporation, by any of the stockholders of the Contractor, seeking its reorganization or the readjustment of its indebtedness under the federal bankruptcy laws or under any law or statute of the United States or of any State thereof; or

3. A petition under any part of the federal bankruptcy laws or an action under any present or future insolvency law or statute shall be filed against the Contractor and shall not be dismissed within thirty (30) days after the filing thereof; or

4. The interest of the Contractor under this Contract shall be transferred to, passed to or devolve upon, by operation of law or otherwise, any other person, firm or corporation, or

5. The Contractor, if a corporation, shall, without the prior written approval of the Port Authority, become a surviving or merged corporation in a merger, a constituent corporation in a consolidation, or a corporation in dissolution; or

6. If the Contractor is a partnership, and the said partnership shall be dissolved as the result of any act or omission of its copartners or any of them, or by operation of law or the order or decree of any court having jurisdiction, or for any other reason whatsoever; or

7. By or pursuant to, or under authority of any legislative act, resolution or rule, or any order or decree of any court or governmental board, agency or officer having jurisdiction, a receiver, trustee, or liquidator shall take possession or control of all or substantially all of the property of the Contractor and such possession or control of all or substantially all of the property of the Contractor and shall continue in effect for a period of fifteen (15) days;

then upon the occurrence of any such event or at any time thereafter during the continuance thereof, the Port Authority shall have the right upon five (5) days notice to the Contractor to terminate this Contract and the rights of the Contractor hereunder; termination to be effective upon the date and time specified in such notice as if said date were the date of the expiration of this Contract. Termination shall not relieve the Contractor of any liabilities or obligations hereunder which have accrued on or prior to the effective date of termination.

C. If any of the following shall occur:

1. The Contractor shall cease, abandon any part of the service, desert, stop or discontinue its services in the premises for any reason whatsoever and regardless of the fault of the Contractor; or

2. The Contractor shall fail to keep, perform and observe each and every other promise, covenant and agreement set forth in this Contract on its part to be kept, performed or observed, within five (5) days after receipt of notice of default thereunder from the Port Authority (except where fulfillment of its obligations

requires activity over a greater period of time, and the Contractor shall have commenced to perform whatever may be required for fulfillment within five (5) days after receipt of notice and continues such performance without interruption except for causes beyond its control);

then upon the occurrence of any such event or during the continuance thereof, the Port Authority shall have the right on twenty four (24) hours notice to the Contractor to terminate this Contract and the rights of the Contractor hereunder, termination to be effective upon the date and time specified in such notice. Termination shall not relieve the Contractor of any liabilities, which shall have accrued on or prior to the effective date of termination.

D. If any of the events enumerated in this Section shall occur prior to commencement date of this Contract the Port Authority upon the occurrence of any such event or any time thereafter during the continuance thereof by twenty-four (24) hours notice may terminate or suspend this Contract and the rights of the Contractor hereunder, such termination or suspension to be effective upon the date specified in such notice.

E. No payment by the Port Authority of any monies to the Contractor for any period or periods after default of any of the terms, covenants or conditions hereof to be performed, kept and observed by the Contractor and no act or thing done or omitted to be done by the Port Authority shall be deemed to be a waiver of the right of the Port Authority to terminate this Contract or of any other right or remedies to which the Port Authority may be entitled because of any breach thereof. No waiver by the Port Authority of any default on the part of the Contractor in the performance of any of the terms, covenants and conditions hereof to be performed, kept or observed by the Contractor shall be or be construed to be a waiver by the Port Authority of any other subsequent default in the performance of any of the said terms, covenants and conditions.

F. In addition to all other rights of revocation or termination hereunder and notwithstanding any other provision of this Contract the Port Authority may terminate this Contract and the rights of the Contractor hereunder without cause at any time upon five (5) days written notice to the Contractor and in such event this Contract shall cease and expire on the date set forth in the notice of termination as fully and completely as though such dates were the original expiration date hereof and if such effective date of termination is other than the last day of the month, the amount of the compensation due to the Contractor from the Port Authority shall be prorated when applicable on a daily basis. Such cancellation shall be without prejudice to the rights and obligations of the parties arising out of portions already performed but no allowance shall be made for anticipated profits.

G. Any right of termination contained in this paragraph, shall be in addition to and not in lieu of any and all rights and remedies that the Port Authority shall have at law or in equity consequent upon the Contractor's breach of this Contract and shall be without prejudice to any and all such other rights and remedies. It is hereby specifically agreed and understood that the exercise by the Port Authority of any right of termination set forth in this paragraph shall not be or be deemed to be an exercise by the Port Authority of an election of remedies so as to preclude the Port Authority from any right to money damages it may have for the period prior to the effective date of termination to the original expiration date of the Contract, and this provision shall be deemed to survive the termination of this Contract as aforesaid.

H. If (1) the Contractor fails to perform any of its obligations under this Contract or any other agreement between the Port Authority and the Contractor (including its obligation to the Port Authority to pay any claim lawfully made against it by any supplier, subcontractor or worker or other person which arises out of or in connection with the performance of this Contract or any other agreement with the Port Authority) or (2) any claim (just or unjust) which arises out of or in connection with this Contract or any other agreement between the Port Authority and the Contractor is made against the Port Authority or (3) any subcontractor under this Contract or any other agreement between the Port Authority and the Contractor fails to pay any claims lawfully made against it by any supplier, subcontractor, worker or other third person which arises out of or in connection with this Contract or any other agreement between the Port Authority and the Contractor or if in the opinion of the Port Authority any of the aforesaid contingencies is likely to arise, then the Port Authority shall have the right, in its discretion, to withhold out of any payment (final or otherwise) such sums as the Port Authority may deem ample to protect it against delay or loss or to assure the payment of just claims of third persons, and to apply such sums in such manner as the Port Authority may deem proper to secure such protection or satisfy such claims. All sums so applied shall be deducted from the Contractor's compensation. Omission by the Port Authority to withhold out of any payment, final or otherwise, a sum for any of the above contingencies, even though such contingency has occurred at the time of such payment, shall not be deemed to indicate that the Port Authority does not intend to exercise its right with respect to such contingency. Neither the above provisions for rights of the Port Authority to withhold and apply monies nor any exercise or attempted exercise of, or omission to exercise, such rights by the Port Authority shall create any obligation of any kind to such supplier, subcontractors, worker or other third persons. If, however, the payment of any amount due the Contractor shall be improperly delayed, the Port Authority shall pay the Contractor interest thereon at the rate of 6% per annum for the period of the delay, it being agreed that such interest shall be in lieu of and in liquidation of any damages to the Contractor because of such delay.

I. If the Port Authority has paid any sum or has incurred any obligation or expense which the Contractor has agreed to pay or reimburse the Port Authority, or if the Port Authority is required or elects to pay any sum or sums or incurs any obligations or expense by reason of the failure, neglect or refusal of the Contractor to perform or fulfill any one or more of the conditions, covenants, or agreements contained in this Contract, or as a result of an act of omission of the Contractor contrary to the said conditions, covenants and agreements, the Contractor shall pay to the Port Authority the sum or sums so paid or expense so incurred, including all interests, costs and damages, promptly upon the receipt of the Port Authority's statement therefore. The Port Authority may, however, in its discretion, elect to deduct said sum or sums from any payment payable by it to the Contractor.

J. If the Port Authority pays any installment to the Contractor without reducing said installment as provided in this Contract, it may reduce any succeeding installment by the proper amount, or it may bill the Contractor for the amount by which the installment paid should have been reduced and the Contractor shall pay to the Port Authority any such amount promptly upon receipt of the Port Authority's statement therefore.

K. The Port Authority shall also have the rights set forth above in the event the Contractor shall become insolvent or bankrupt or if his affairs are placed in the hands of a receiver, trustee or assignee for the benefit of creditors.

12. WITHHOLDING OF PAYMENT

If (1) the Contractor fails to perform any of its obligations under this Contract or any other agreement between the Authority and the Contractor (including his obligation to the Authority to pay any claim lawfully made against him by any materialman, subcontractor or workman or other person which arises out of or in connection with the performance of this Contract or any other agreement with the Authority) or (2) any claim (just or unjust) which arises out of or in connection with this Contract or any other agreement between the Authority and the Contractor is made against the Authority or (3) any subcontractor under this Contract or any other agreement between the Authority and the Contractor fails to pay any claims lawfully made against him by any materialman, subcontractor, workman or other third person which arises out of on in connection with this Contract or any other agreement between the Authority and the Contractor or if in the opinion of the Authority any of the aforesaid contingencies is likely to arise, then the Authority shall have the right, in its discretion, to withhold out of any payment (final or otherwise and even though such payment has already been certified as due) such sums as the Authority may deem ample to protect it against delay or loss or to assure the payment of just claims of third persons, and to apply such sums in such manner as the Port Authority may deem proper to protect it against delay or loss or to satisfy such claims. All sums so applied shall be deducted from the Contractor's compensation. Omission by the Authority to withhold out of any payment, final or otherwise, a sum for any of the above contingencies, even though such contingency has occurred at the time of such payment, shall not be deemed to indicate that the Authority does not intend to exercise its right with respect to such contingency. Neither the above provisions for rights of the Authority to withhold and apply monies nor any exercise or attempted exercise of, or omission to exercise, such rights by the Authority shall create any obligation of any kind to such materialman, subcontractors, workman or other third persons.

Until actual payment to the Contractor, its right to any amount to be paid under this Contract (even though such amount has already been certified as due) shall be subordinate to the rights of the Authority under this clause.

13. CONTRACTOR PERSONNEL STANDARDS OF PERFORMANCE

The Contractor shall furnish sufficiently trained management, supervisory, technical and operating personnel to perform the services required of the Contractor under this Contract. If, in the opinion of the Director, any of the Contractor's personnel are not satisfactory in the performance of services to be furnished hereunder, the Contractor shall remove such personnel and replace them with personnel satisfactory to the Director.

At the time the Contractor is carrying out its operations there may be other persons working physically in the vicinity or in the same logical or technical infrastructure. . The Contractor shall so conduct its operations as to work in harmony and not endanger, interfere with or delay the operations of others, all to the best interests of The Authority and others and as may be directed by the Director.

14. DESIGNATED SECURE AREAS

Services under the Contract may be required in designated secure areas, as the same may be designated by the Manager from time to time ("Secure Areas"). The Port Authority shall require the observance of certain security procedures with respect to Secure Areas, which may include the escort to, at, and/or from said high security areas by security personnel designated by the Contractor or any subcontractor's personnel required to work therein. All personnel that require access to designated secure areas who are not under positive escort by an authorized individual

will be required to undergo background screening and personal identity verification.

Forty-eight (48) hours prior to the proposed performance of any work in a Secure Area, the Contractor shall notify the Manager. The Contractor shall conform to the procedures as may be established by the Manager from time to time and at any time for access to Secure Areas and the escorting of personnel hereunder. Prior to the start of work, the Contractor shall request a description from the Manager of the Secure Areas which will be in effect on the commencement date. The description of Secure Areas may be changed from time to time and at any time by the Manager during the term of the Contract.

15. NOTIFICATION OF SECURITY REQUIREMENTS

The Authority has the responsibility of ensuring safe, reliable and secure transportation facilities, systems, and projects to maintain the well-being and economic competitiveness of the region. Therefore, the Authority reserves the right to deny access to certain documents, sensitive security construction sites and facilities (including rental spaces) to any person that declines to abide by Port Authority security procedures and protocols, any person with a criminal record with respect to certain crimes or who may otherwise poses a threat to the construction site or facility security. The Authority reserves the right to impose multiple layers of security requirements on the Contractor, its staff and subcontractors and their staffs depending upon the level of security required, or may make any amendments with respect to such requirements as determined by the Authority.

These security requirements may include but are not limited to the following:

- Contractor/ Subcontractor identity checks and background screening
  The Port Authority's designated background screening provider may require inspection of not less than two forms of valid/current government issued identification (at least one having an official photograph) to verify staff's name and residence; screening federal, state, and/or local criminal justice agency information databases and files; screening of any terrorist identification files; access identification to include some form of biometric security methodology such as fingerprint, facial or iris scanning, or the like.

  The Contractor may be required to have its staff, and any subcontractor's staff, material-men, visitors or others over whom the Contractor/subcontractor has control, authorize the Authority or its designee to perform background checks, and a personal identity verification check. Such authorization shall be in a form acceptable to the Authority. The Contractor and subcontractors may also be required to use an organization designated by the Authority to perform the background checks.

  As of January 29, 2007, the Secure Worker Access Consortium (S.W.A.C.) is the only Port Authority approved provider to be used to conduct background screening and personal identity verification, except as otherwise required by federal law and/or regulation (such as the Transportation Worker Identification Credential for personnel performing in secure areas at Maritime facilities). Information about S.W.A.C., instructions, corporate enrollment, online applications, and location of processing centers can be found at http://www.secureworker.com, or S.W.A.C. may be contacted directly at (877) 522-7922 for more information and the latest pricing. The cost for said background checks for staff that pass and are granted a credential shall be reimbursable to the Contractor (and its subcontractors) as an out-of-pocket expense as provided herein. Staff that are rejected for a credential for any reason are not reimbursable.

- Issuance of Photo Identification Credential

  No person will be permitted on or about the Authority construction site or facility (including rental spaces) without a facility-specific photo identification credential approved by the Authority. If the authority requires facility-specific identification credential for the Contractor's and the subcontractor's staff, the Authority will supply such identification at no cost to the Contractor or its subcontractors. Such facility-specific identification credential shall remain the property of the Authority and shall be returned to the Authority at the completion or upon request prior to completion of the individual's assignment at the specific facility. It is the responsibility of the appropriate Contractor or subcontractor to immediately report to the Authority the loss of any staff member's individual facility-specific identification credential. The Contractor or subcontractor shall be billed for the cost of the replacement identification credential. Contractor's and subcontractor's staff shall display Identification badges in a conspicuous and clearly visible manner, when entering, working or leaving an Authority construction site or facility.

  Employees may be required to produce not less than two forms of valid/current government issued identification having an official photograph and an original, unlaminated social security card for identify and SSN verification. Where applicable, for sensitive security construction sites or facilities, successful completion of the application, screening and identify verification for all employees of the Contractor and subcontractors shall be completed prior to being provided a S.W.A.C. ID Photo Identification credential.

- Access control, inspection, and monitoring by security guards

  The Authority may provide for Authority construction site or facility (including rental spaces) access control, inspection and monitoring by Port Authority Police or Authority retained contractor security guards. However, this provision shall not relieve the Contractor of its responsibility to secure its equipment and work and that of its subconsultant/subcontractor's and service suppliers at the Authority construction site or facility (including rental spaces). In addition, the Contractor, subcontractor or service provider is not permitted to take photographs, digital images, electronic copying and/or electronic transmission or video recordings or make sketches on any other medium at the Authority construction sites or facilities (including rental spaces), except when necessary to perform the Work under this Contract, without prior written permission from the Authority. Upon request, any photograph, digital images, video recording or sketches made of the Authority construction site or facility shall be submitted to the Authority to determine compliance with this paragraph, which submission shall be conclusive and binding on the submitting entity.

- Compliance with the Port Authority Information Security Handbook

  The Contract may require access to Port Authority information considered Confidential Information ("CI") as defined in the Port Authority Information Security Handbook ("Handbook"), dated October, 2008, corrected as of February, 2009, and as may be further amended. The Handbook and its requirements are hereby incorporated into this agreement and will govern the possession, distribution and use of CI if at any point during the lifecycle of the project or solicitation it becomes necessary for the Contractor to have access to CI. Protecting sensitive information requires the application of uniform safeguarding measures to prevent unauthorized disclosure and to control any authorized disclosure of this information within the Port Authority or when released by the Port Authority to outside entities. The following is an outline of some of the procedures, obligations and directives contained in the Handbook:

  (1) The Contractor and subcontractors, when appropriate, shall sign Non-Disclosure Agreements (NDAs), or an Acknowledgment of an existing NDA, provided by the

Authority as a condition of being granted access to Confidential Information categorized and protected as per *The Port Authority of New York & New Jersey Information Security Handbook (October 15, 2009, corrected as of February 9, 2009)*.

(2) require Contractors and commercial enterprises to attend training to ensure security awareness regarding Port Authority information;

(3) specific guidelines and requirements for the handling of CI to ensure that the storage and protection of CI;

(4) restrictions on the transfer, shipping, and mailing of CI information;

(5) prohibitions on the publication, posting, modifying, copying, reproducing, republishing, uploading, transmitting, or distributing CI on websites or web pages. This may also include restricting persons, who either have not passed a pre-screening background check, or who have not been granted access to CI, from viewing such information;

(6) require that CI be destroyed using certain methods, measures or technology pursuant to the requirements set forth in the Handbook;

(7) require the Contractor to mandate that each of its subcontractors maintain the same levels of security required of the Contractor under any Port Authority awarded contract.

(8) prohibit the publication, exchange or dissemination of CI developed from the project or contained in reports, except between Contractors and subcontractors, without prior approval of the Port Authority;

(9) require that CI only be reproduced or copied pursuant to the requirements set forth in the Handbook.

- Audits for Compliance with Security Requirements
  The Port Authority may conduct random or scheduled examinations of business practices under this section entitled "NOTIFICATION OF SECURITY REQUIREMENTS" and the Handbook in order to assess the extent of compliance with security requirements, Confidential Information procedures, protocols and practices, which may include, but not be limited to, verification of background check status, confirmation of completion of specified training, and/or a site visit to view material storage locations and protocols.

The Authority may impose, increase, and/or upgrade security requirements for the Contractor, subcontractors and their staffs during the term of this Contract to address changing security conditions and/or new governmental regulations.

16. INSURANCE PROCURED BY THE CONTRACTOR

LIABILITY INSURANCE AND WORKERS' COMPENSATION INSURANCE

A. Commercial Liability Insurance:

1) The Contractor shall take out and maintain at his own expense Commercial General Liability Insurance including but not limited to Premises-Operations, Completed Operations and Independent Contractor coverages in limits of not less than $2,000,000 combined single limit per occurrence for Bodily Injury Liability and Property Damage Liability. And if vehicles are to be used to carry out the performance of this Agreement, then the Contractor shall also take out, maintain and pay the premiums on Automobile Liability Insurance covering all owned, non-owned and hired autos in not less than $2,000,000 combined single limit per accident for bodily injury and property damage. In addition, the liability policies (other than Professional Liability) shall

include the Authority and its wholly owned entities as additional insureds and shall contain a provision that the policy may not be canceled, terminated or modified without thirty (30) days written advance notice to the Project Manager. Moreover, the Commercial General Liability policy shall not contain any provisions (other than a Professional Liability exclusion, if any) for exclusions from liability other than provisions or exclusions from liability forming part of the most up to date ISO form or its equivalent unendorsed Commercial General Liability Policy. The liability policy(ies) and certificate of insurance shall contain separation of insured condition (cross-liability) and severability of interests provisions so that coverage will respond as if separate policies were in force for each insured.

Further, the certificate of insurance and the liability policy(ies) shall be specifically endorsed that "*The insurance carrier(s) shall not, without obtaining the express advance permission from the General Counsel of the Port Authority, raise any defense involving in any way the jurisdiction of the tribunal over the person of the Port Authority, the immunity of the Port Authority, its Commissioners, officers, agents or employees, the governmental nature of the Port Authority, or the provisions of any statutes respecting suits against the Port Authority.*"

2) Additional Coverages: The Contractor shall have the policy endorsed when required by the Director for specific services hereunder and include the additional premium cost thereof as an out-of-pocket expense:

a) If the services of the Contractor require the performance of services airside, the Commercial General Liability and Automobile Liability coverage limits stipulated in subparagraph 1, above, shall be increased to an amount not less than $25,000,000 per occurrence as provided herein.
b) Endorsement to eliminate any exclusions applying to explosion, collapse and underground property damage.
c) Endorsement to eliminate any exclusions on account of ownership, maintenance, operation, use, loading or unloading of watercraft.
d) Coverage for work within 50 feet of railroad.

B. Workers' Compensation Insurance:
1) The Contractor shall take out and maintain Workers' Compensation Insurance in accordance with the requirements of law and Employer's Liability Insurance with limits of not less than $1,000,000 each accident.

2) Additional Coverages: The Contractor shall have the policy endorsed when required by the Engineer for specific services hereunder and include the additional premium cost thereof as an out-of-pocket expense:
a) United States Longshoremen's and Harbor Workers' Compensation Act Endorsement.
b) Coverage B Endorsement - Maritime (Masters or Members of the Crew of Vessels), in limits of not less than $1,000,000 per occurrence.
c) Amendments to Coverage B, Federal Employers' Liability Act in limits of not less than $1,000,000 per occurrence.

C. Professional Liability Insurance:
1) Not less than $2 million each occurrence, covering negligent acts, errors, mistakes, and omissions arising out of the work or services performed by Contractor, or any person

employed by Contractor. All endorsements and exclusions shall be evidenced on the certificate of insurance. The coverage shall be written on an occurrence form or may be written on a claims-made basis with a minimum of a three-year reporting/discovery period.

D. Compliance:
The Contractor shall not commence the performance of any work on Authority premises until the Contractor has received notice from the Authority that the insurance provided by him in accordance with the clause hereof entitled "Insurance to be Provided by the Contractor" is satisfactory, as evidenced by the certificate to be furnished under said clause. The time for completion shall not be extended on account of the time required to furnish the documents referred to above, but the Authority shall give notice to the Contractor within five (5) days after receipt of the certificate of insurance as to whether or not such insurance is satisfactory.

Prior to commencement of work at the site, the Contractor shall deliver a certificate from its insurer evidencing policies of the above insurance stating the title of this Agreement, the P. A. Agreement number and containing a separate express statement of compliance with each of the requirements above set forth to the Project Manager.

1) Upon request of the General Manager, Risk Management/Treasury, the Contractor shall furnish to the Authority a certified copy of each policy itself, including the provisions establishing premiums.

2) Renewal certificates of insurance or policies shall be delivered via e-mail to the Authority's Project Manager at least fifteen (15) days prior to the expiration date of each expiring policy. The General Manager, Risk Management must approve the renewal certificate(s) of insurance before work can resume. If at any time any of the certificates or policies shall become unsatisfactory to the Authority, the Contractor shall promptly obtain a new and satisfactory certificate and policy.

3) If at any time the above liability insurance should be canceled, terminated, or modified so that the insurance is not in effect as above required, then, if the General Manager shall so direct, the Contractor shall suspend performance of the Agreement at the premises. If the Agreement is so suspended, no extension of time shall be due on account thereof. If the Agreement is not suspended (whether or not because of omission of the General Manager to order suspension), then the Authority may, at its option, obtain insurance affording coverage equal to the above required, the cost of such insurance to be payable by the Contractor to the Authority.

The requirements for insurance procured by the Contractor shall not in any way be construed as a limitation on the nature or extent of the contractual obligations assumed by the Contractor under this Agreement. The insurance requirements are not a representation by the Authority as to the adequacy of the insurance to protect the Contractor against the obligations imposed on them by law or by this or any other Agreement.

17. ASSIGNMENTS AND SUBCONTRACTS

Any assignment or other transfer by the Contractor of this Contract or any part hereof or of any of his rights hereunder or of any monies due or to become due hereunder and any delegation of any of his duties hereunder without the express written consent of the Director shall be void and of no effect as to the Authority, provided, however, that the Contractor may subcontract portions of the Work to such persons as the Director, may, from time to time, expressly approve in writing. For each individual, partnership or corporation proposed by the Contractor as a subcontractor, the Contractor shall submit to the Authority a certification or, if a certification cannot be made, a statement by such person, partnership or corporation to the same effect as the certification or statement required from the Contractor pursuant to the clauses of the "Integrity" Section entitled "Certification of No Investigation Indictment, Conviction, Debarment Suspension, Disqualification and Disclosure of Other Information and "Non-Collusive Bidding and Code of Ethics Certification; Certification of No Solicitation Based on Commission, Percentage, Brokerage Contingent or Other Fee". All further subcontracting by any subcontractor shall also be subject to such approval of the Director

No consent to any assignment or other transfer, and no approval of any subcontractor, shall under any circumstances operate to relieve the Contractor of any of his obligations; no subcontract, no approval of any subcontractor and no act or omission of the Authority or the Director shall create any rights in favor of such subcontractor and against the Authority; and as between the Authority and the Contractor, all assignees, subcontractors, and other transferees shall for all purposes be deemed to be agents of the Contractor. Moreover, all subcontractors and all approvals of subcontractors, regardless of their form, shall be deemed to be conditioned upon performance by the subcontractor in accordance with this Contract; and if any subcontractor shall fail to perform the Contract to the satisfaction of the Director, the Director shall have the absolute right to rescind his approval forthwith and to require the performance of the Contract by the Contractor personally or through other approved subcontractors.

18. CERTAIN CONTRACTOR'S WARRANTIES

The Contractor represents and warrants:

A. That it is financially responsible and experienced in, and competent to perform this Contract; that no representation, promise or statement, oral or in writing, has induced it to submit its Proposal, saving only those contained in the papers expressly made part of this Contract; that the facts stated or shown in any papers submitted or referred to in connection with his Proposal are true; and, if the Contractor be a corporation, that it is authorized to perform this Contract;

B. That it has carefully examined and analyzed the provisions and requirements of this Contract, that from its own investigations it has satisfied itself as to the nature of all things needed for the performance of this Contract, the general and local conditions and all other matters which in any way affect this Contract or its performance, and that the time available to it for such examination, analysis, inspection and investigations was adequate;

C. That the Contract is feasible of performance in accordance with all its provisions and requirements and that it can and will perform it in strict accordance with such provisions and requirements;

D. That no Commissioner, officer, agent or employee of the Authority is personally interested directly or indirectly in this Contract or the compensation to be paid hereunder;

E. That, except only for those representations, statements or promises expressly contained in this Contract, no representation, statement or promise, oral or in writing, of any kind whatsoever by the Authority, its Commissioners, officers, agents, employees or consultants has induced the Contractor to enter into this Contract or has been relied upon by the Contractor, including any with reference to: (1) the meaning, correctness, suitability or completeness of any provisions or requirements of this Contract; (2) the nature, existence or location of materials, structures, obstructions, utilities or conditions, which may be encountered at the installation sites; (3) the nature, quantity, quality or size of the materials, equipment, labor and other facilities needed for the performance of this Contract; (4) the general or local conditions which may in any way affect this Contract or its performance; (5) the price of the Contract; or (6) any other matters, whether similar to or different from those referred to in (1) through (5) immediately above, affecting or having any connection with this Contract, the bidding thereon, any discussions thereof, the performance thereof or those employed therein or connected or concerned therewith.

F. That, notwithstanding any requirements of this Contract, any inspection or approval of the Contractor's services by the Authority, or the existence of any patent or trade name, the Contractor nevertheless warrants and represents that the services and any intellectual property supplied to the Authority hereunder shall be of the best quality and shall be fully fit for the purpose for which they are to be used. The Contractor unconditionally guarantees against defects or failures of any kind, including defects or failures in design, workmanship and materials, excepting solely defects or failures which the Contractor demonstrates to the satisfaction of the Authority have arisen solely from accident, abuse or fault of the Authority occurring after issuance of Final Payment hereunder and not due to fault on the Contractor's part. In the event of defects or failures in said services, or any part thereof, then upon receipt of notice thereof from the Authority, the Contractor shall correct such defects or failures as may be necessary or desirable, in the sole opinion of the Authority, to comply with the above guaranty.

Moreover, the Contractor accepts the conditions at the sites of work as they may eventually be found to exist and warrants and represents that it can and will perform the Contract under such conditions and that all materials, equipment, labor and other facilities required because of any unforeseen conditions (physical or otherwise) shall be wholly at its own cost and expense, anything in this Contract to the contrary notwithstanding.

Nothing in the Scope of Work or any other part of the Contract is intended as or shall constitute a representation by the Authority as to the feasibility of performance of this Contract or any part thereof. Moreover, the Authority does not warrant or represent either by issuance of the Scope of Work or by any provision of this Contract as to time for performance or completion or otherwise that the Contract may be performed or completed by the times required herein or by any other times.

The Contractor further represents and warrants that it was given ample opportunity and time and by means of this paragraph was requested by the Authority to review thoroughly all documents forming this Contract prior to execution of this Contract in order that it might request inclusion in this Contract of any statement, representation, promise or provision which it desired or on which it wished to place reliance; that it did so review said documents; that either every such statement, representation, promise or provision has been included in this

Contract or else, if omitted, that it expressly relinquishes the benefit of any such omitted statement, representation, promise or provision and is willing to perform this Contract without claiming reliance thereon or making any other claim on account of such omission.

The Contractor further recognizes that the provisions of this clause (though not only such provisions) are essential to the Authority's consent to enter into this Contract and that without such provisions; the Authority would not have entered into this Contract.

19. RIGHTS AND REMEDIES OF THE AUTHORITY

The Authority shall have the following rights in the event the Director shall deem the Contractor guilty of a breach of any term whatsoever of this contract:

a) The right to take over and complete the Work or any part thereof as agent for and at the expense of the Contractor, either directly or through other Contractors;
b) The right to cancel this Contract as to any or all of the Work yet to be performed;
c) The right to specific performance, an injunction or any other appropriate equitable remedy;
d) The right to money damages.

For the purpose of this Contract, breach shall include but not be limited to the following, whether or not the time has yet arrived for performance of an obligation under this Contract: a statement by the Contractor to any representative of The Authority indicating that he cannot or will not perform any one or more of his obligations under this Contract; any act or omission of the Contractor or any other occurrence which makes it improbable at the time that he will be able to perform any one or more of his obligations under this Contract; any suspension of or failure to proceed with any part of the Work by the Contractor which makes it improbable at the time that he will be able to perform any one or more of his obligations under this Contract; any false certification at any time by the Contractor as to any material item certified pursuant to the clauses hereof entitled "Certification of No Investigation (Criminal or Civil Anti-Trust), Indictment, Conviction, Debarment, Suspension, Disqualification and Disclosure of Other Required Information" and "Non-Collusive Bidding and Code of Ethics Certification; Certification of No Solicitation Based on Commission, Percentage, Brokerage, Contingent or Other Fee", or the willful or fraudulent submission of any signed statement pursuant to such clauses which is false in any material respect; or the Contractor's incomplete or inaccurate representation of its status with respect to the circumstances provided for in such clauses.

The enumeration in this numbered clause or elsewhere in this Contract of specific rights and remedies of The Authority shall not be deemed to limit any other rights or remedies which The Authority would have in the absence of such enumeration; and no exercise by The Authority of any right or remedy shall operate as a waiver of any other of its rights or remedies not inconsistent therewith or to stop it from exercising such other rights or remedies.

Neither the acceptance of the work or any part thereof, nor any payment therefor, nor any order or certificate issued under this Agreement or otherwise issued by the Authority, or any officer, agent or employee of the Authority, nor any permission or direction to continue with the performance or work, nor any performance by the authority of any of the Contractor's duties or obligations, nor any aid provided to the Contractor by the Authority in his performance of such duties or obligations, nor any other thing done or omitted to be done by the Authority, its Commissioners, officers, agents or employees shall be deemed to be a waiver of any provision of this agreement or of any rights or remedies to which the Authority may be entitled because of any breach hereof, excepting only a resolution of its Commissioners, providing expressly for such waiver. No

cancellation, rescission or annulment hereof, in whole or as to any part of the work, because of any breach hereof, shall be deemed a waiver of any money damages to which the Authority may be entitled because of such breach. Moreover, no waiver by the Authority of any breach of this Agreement shall be deemed to be a waiver of any other or any subsequent breach.

20. RIGHTS AND REMEDIES OF THE CONTRACTOR

Inasmuch as the Contractor can be adequately compensated by money damages for any breach of this Contract which may be committed by the Authority, the Contractor expressly agrees that no default, act or omission of the Authority shall constitute a material breach of this Contract, entitling him to cancel or rescind it or (unless the Director shall so direct) to suspend or abandon performance.

21. TAX EXEMPTIONS

Purchases of services and tangible personal property by the Port Authority are exempt from New York and New Jersey state and local sales and compensating use taxes. (Sales Taxes). Therefore, the Port Authority's purchase of the Contractor's services under this Contract is exempt from Sales Taxes. Accordingly, the Contractor must not include Sales Taxes in the price charged to the Port Authority for the contractor's services under this Contract.

22. TITLE TO EQUIPMENT

Title to all equipment to be furnished hereunder by the Contractor shall be transferred to the Authority upon its delivery to the installation site.

The Contractor shall furnish such bills of sale and affidavits of title as the Authority shall reasonably request.

23. NOTICE REQUIREMENTS

No claim against the Authority shall be made or asserted in any action or proceeding at law or in equity, and the Contractor shall not be entitled to allowance of such claim, unless the Contractor shall have complied with all requirements relating to the giving of written notice and of information with respect to such claim as provided in this clause. The failure of the Contractor to give such written notice and information as to any claim shall be conclusively deemed to be a waiver by the Contractor of such claim, such written notice and information being conditions precedent to such claim. As used herein "claim" shall include any claim arising out of this agreement (including claims in the nature of breach of contract or fraud or misrepresentation before or subsequent to execution of this Agreement and claims of a type which are barred by the provisions of this agreement) for damages, payment or compensation of any nature or for performance of any part of this Agreement.

The requirements as to the giving of written notice and information with respect to claims shall be as follows:

A. In the case of any claims for which requirements are set forth elsewhere in this Agreement as to notice and information, such requirements shall apply.

B. In the case of all other types of claims, notice shall have been given to the Director, as soon as practicable, and in any case within forty eight (48) hours after occurrence of the act, omission, or other circumstances upon which the claim is or will be based, stating as fully as practicable at the time all information relating thereto. Such information shall be supplemented with any further information as soon as practicable after it becomes or should become known to the

Contractor, including daily records showing all costs which the Contractor may be incurring or all other circumstances which will affect any claim to be made which records shall be submitted to the Authority.

The above requirements for notices and information are for the purpose of enabling the Authority to avoid waste of public funds by affording it promptly the opportunity to cancel or revise any order, change its plans, mitigate or remedy the effects of circumstances giving rise to a claim or take such other action as may seem desirable and to verify any claimed expense or circumstance as they occur and the requirements herein for such notice and information are essential to this Agreement and are in addition to any notice required by statue with respect to suits against the Authority.

The above referred to notices and information are required whether or not the Authority is aware of the existence of any circumstances which might constitute a basis for a claim and whether or not the Authority has indicated it will consider a claim.

No, act, omission or statement of any kind shall be regarded as a waiver of any of the provisions of this clause or may be relied upon as such waiver except only either a written statement signed by the Executive Director of the Authority or a resolution of the Commissioners of the Authority expressly stating that a waiver is intended as to any particular provision of this clause, and more particularly, no discussion, negotiation, consideration, correspondence or requests for information with respect to a claim by any Commissioner, officer, employees or agent of the Authority shall be construed as a waiver of any provision of this clause or as authority or apparent authority to effect such a waiver.

Since merely oral notice or information may cause disputes as to the existence or substance thereof, and since notice, even if written, to other than the Authority representative above designated to receive it may not be sufficient to come to the attention of the representative of the Authority with the knowledge and responsibility of dealing with the situation, only notice and information complying with the express provisions of this clause shall be deemed to fulfill the Contractor's obligation under this Agreement.

24. SERVICE OF NOTICES ON THE CONTRACTOR

Whenever provision is made in this Contract for the giving of any notice to the Contractor, its deposit in any post office box, enclosed in a postpaid wrapper addressed to the Contractor at his/her office, or its delivery to his/her office, shall be sufficient service thereof as of the date of such deposit or delivery, except to the extent, if any, otherwise provided in the clause entitled "Submission to Jurisdiction". Until further notice to the Authority the Contractor's office will be that stated in his/her Proposal. Notices may also be served personally upon the Contractor; or if a corporation, upon any officer, director or managing or general agent; or if a partnership upon any partner.

25. NO THIRD PARTY RIGHTS

Nothing contained in this Agreement is intended for the benefit of third persons, except to the extent that the Agreement specifically provides otherwise by use of the words "benefit" or "direct right of action".

26. INDEMNIFICATION AND RISKS ASSUMED BY THE CONTRACTOR

To the extent permitted by law, the Contractor shall indemnify and hold harmless the Port

Authority, its Commissioners, officers, representatives and employees from and against all claims and demands, just or unjust, of third persons (including Contractor's employees, employees, officers, and agents of the Port Authority) arising out of or in any way connected or alleged to arise out of or alleged to be in any way connected with the Contract and all other services and activities of the Contractor under this Contract and for all expenses incurred by it and by them in the defense, settlement or satisfaction thereof, including without limitation thereto, claims and demands for death, for personal injury or for property damage, direct or consequential, whether they arise from the acts or omissions of the Contractor, the Port Authority, third persons(including Contractor's employees, employees, officers, and agents of the Port Authority), or from the acts of God or the public enemy, or otherwise, including claims and demands of any local jurisdiction against the Port Authority in connection with this Contract.

The Contractor assumes the following risks, whether such risks arise from acts or omissions (negligent or not) of the Contractor, the Port Authority or third persons (including Contractor's employees, employees, officers, and agents of the Port Authority)or from any other cause, excepting only risks occasioned solely by affirmative willful acts of the Port Authority done subsequent to the opening of proposals on this Contract, and shall to the extent permitted by law indemnify the Port Authority for all loss or damage incurred in connection with such risks:

a. The risk of any and all loss or damage to Port Authority property, equipment (including but not limited to automotive and/or mobile equipment), materials and possessions, on or off the premises, the loss or damage of which shall arise out of the Contractor's operations hereunder. The Contractor shall if so directed by the Port Authority, repair, replace or rebuild to the satisfaction of the Port Authority, any and all parts of the premises or the Facility which may be damaged or destroyed by the acts or omissions of the Contractor, its officers, agents, or employees and if the Contractor shall fail so to repair, replace, or rebuild with due diligence the Port Authority may, at its option, perform any of the foregoing work and the Contractor shall pay to the Port Authority the cost thereof.

b. The risk of any and all loss or damage of the Contractor's property, equipment (including but not limited to automotive and/or mobile equipment) materials and possessions on the Facility.

c. The risk of claim, whether made against the Contractor or the Port Authority, for any and all loss or damages occurring to any property, equipment (including but not limited to automotive and/or mobile equipment), materials and possessions of the Contractor's agents, employees, materialmen and others performing work hereunder.

d. The risk of claims for injuries, damage or loss of any kind just or unjust of third persons arising or alleged to arise out of the performance of work hereunder, whether such claims are made against the Contractor or the Port Authority.

If so directed, the Contractor shall at its own expense defend any suit based upon any such claim or demand, even if such suit, claim or demand is groundless, false or fraudulent, and in handling such shall not, without obtaining express advance permission from the General Counsel of the Port Authority, raise any defense involving in any way the jurisdiction of the tribunal over the person

of the Port Authority, the immunity of the Port Authority, its Commissioners, officers, agents or employees, the governmental nature of the Port Authority or the provision of any statutes respecting suits against the Port Authority.
Neither the requirements of the Port Authority under this Contract, nor of the Port Authority of the methods of performance hereunder nor the failure of the Port Authority to call attention to improper or inadequate methods or to require a change in the method of performance hereunder nor the failure of the Port Authority to direct the Contractor to take any particular precaution or other action or to refrain from doing any particular thing shall relieve the Contractor of its liability for injuries to persons or damage to property or environmental impairment arising out of its operations.

27. APPROVAL OF METHODS

Neither the approval of the Port Authority of the methods of furnishing services hereunder nor the failure of the Port Authority to call attention to improper or inadequate methods or to require a change in the method of furnishing services hereunder, nor the failure of the Port Authority to direct the Contractor to take any particular precautions or to refrain from doing any particular thing shall relieve the Contractor of its liability for injuries to persons or damage to property or environmental impairment arising out of its operations.

28. PORT AUTHORITY TECHNOLOGY STANDARDS AND GUIDELINES AND SUPPLEMENTAL GUIDELINES FOR THE PORT AUTHORITY TECHNOLOGY SERVICES DEPARTMENT

The Contractor and any subcontractors shall follow the Port Authority Technology Standard and Guidelines and the Supplemental Guidelines for the Port Authority Technology Services Department attached hereto and made a part hereof, and shall comply with any updates to or changes in best practices related to such Standards and Guidelines.

29. SUBMISSION TO JURISDICTION

The Contractor hereby irrevocably submits itself to the jurisdiction of the Courts of the State of New York and New Jersey, in regard to any controversy arising out of, connected with, or in any way concerning this Contract.

The Contractor agrees that the service of process on the Contractor in relation to such jurisdiction may be made, at the option of the Port Authority, either by registered or certified mail addressed to it at the address of the Contractor indicated on the signature sheet, or by actual personal delivery to the Contractor, if the Contractor is an individual, to any partner if the Contractor be a partnership or to any officer, director or managing or general agent if the Contractor be a corporation.
Such service shall be deemed to be sufficient when jurisdiction would not lie because of the lack of basis to serve process in the manner otherwise provided by law. In any case, however, process may be served as stated above whether or not it might otherwise have been served in a different manner.

30. APPLICABLE LAW

This Contract shall be construed in accordance with the laws of the State of New York. The Contractor hereby consents to the exercise by the courts of the States of New York and New Jersey of jurisdiction in personam over it with respect to any matter arising out of or in connection with this Contract and waives any objection to such jurisdiction which it might otherwise have; and the Contractor agrees that mailing of process by registered mail addressed to it at the address

of the Contractor set forth in the Proposal, shall have the same effect as personal service within the States of New York or New Jersey upon a domestic corporation of said State.

31. AUTHORITY OF THE DIRECTOR

Inasmuch as the public interest requires that the Project to which this Contract relates shall be performed in the manner which the Authority, acting through the Director deems best, the Director shall have absolute authority to determine what is or is not necessary or proper for or incidental thereto and the Specifications shall be deemed merely the Director's present determination on this point. In the exercise of this authority, the Director shall have power to alter the Specifications, to require the performance of Work not required by them in their present form, even though of a totally different character from that not required, and to vary, increase and diminish the character, quantity and quality of, or to countermand any Work now or hereafter required. If at any time it shall be, from the viewpoint of the Authority, impracticable or undesirable in the judgment of the Director to proceed with or continue the performance of the Contract or any part thereof, whether or not for reasons beyond the control of the Authority, the Director shall have authority to suspend performance of any part or all of the Contract until such time as the Director may deem it practicable or desirable to proceed. Moreover, if at any time it shall be, from the viewpoint of the Authority impracticable or undesirable in the judgment of the Director to proceed with or continue the performance of the Contract or any part thereof for reasons within or beyond the control of the Authority, the Director shall have authority to cancel this Contract as to any or all portions not yet performed and as to any materials not yet installed even though delivered. Such cancellation shall be without prejudice to the rights and obligations of the parties arising out of portions already satisfactorily performed, but no allowance shall be made for anticipated profits. To resolve all disputes and to prevent litigation, the parties to this Contract authorize the Director to decide all questions of any nature whatsoever arising out of, under, or in connection with, or in any way related to or on account of, this Contract (including claims in the nature of breach of contract or fraud or misrepresentation before or subsequent to acceptance of the Contractor's Proposal and claims of a type which are barred by the provisions of this Contract) and such decision shall be conclusive, final and binding on the parties. The Director's decision may be based on such assistance as she may find desirable. The effect of the decision shall not be impaired or waived by any negotiation or settlement offers in connection with the question decided, whether or not she participated therein, or by any prior decision of her or others, which prior decisions shall be deemed subject to review, or by any termination or cancellation of this Contract.

All such questions shall be submitted in writing by the Contractor to the Director for a decision together with all evidence and other pertinent information in regard to such questions, in order that a fair and impartial decision may be made. In any action against the Authority relating to any such question the Contractor must allege in the complaint and prove such submission, which shall be a condition precedent to any such action. No evidence or information shall be introduced or relied upon in such an action that has not been so presented to the Director.

In the performance of the Contract, the Contractor shall conform to all orders, directions and requirements of the Director and shall perform the Contract to her satisfaction at such times and places, by such methods and such manner and sequence as she may require, and the Contract shall at all stages be subject to her inspection. The Contractor shall employ no equipment, materials, methods or men to which she objects, and shall remove no materials, equipment or other facilities from the Authority site without permission. Upon request, she shall confirm in writing any oral order, direction, requirements or determination.

The enumeration herein or elsewhere of particular instances in which the opinion, judgment, discretion or determination of the Director shall control or in which the Contract shall be

performed to her satisfaction or subject to her inspection, shall not imply that only the matters of a nature similar to those enumerated shall be so governed and performed, but without exception the entire Contract shall be so governed and performed.

This provision shall be construed in accordance with the laws of the State of New York excluding its conflict of law provisions.

32. APPROVALS BY THE DIRECTOR

The approval by the Director of any service required hereunder, shall be construed merely to mean that at that time the Director knows of no good reason for objecting thereto and no such approval shall release the Contractor from its full responsibility for the satisfactory performance of the services to be supplied. "Approved equal" shall mean approved by the Director.

33. CONTRACT REVIEW AND COMPLIANCE AUDITS

The Contractor, and any subcontractors, shall provide system access and reasonable assistance to the Authority's External and Internal Audit staff or its consultants in their performance of work under the contract, including producing specific requested information, extraction of data and reports. The Contractor, and any subcontractors, shall support requests related to audits of the agreement and administration tasks and functions covered by this Contract.

The Authority reserves the right to use and load security and system software to evaluate the level of security and vulnerabilities in all systems which control, collect, dispense, contain, manage, administer, or monitor revenue "owned" by the Port Authority.

The Authority reserves the right to use as required and load security and system software to evaluate the level of security and vulnerabilities in any applicable environment-covered under this Contract. If such right is exercised, then both parties shall work in good faith to ensure there is no access or potential access to third party proprietary data within the applicable environment or access to other systems not covered under this Contract.

34. AUTHORITY ACCESS TO RECORDS

The Authority shall have access during normal business hours to all records and documents of the Contractor relating to any service provided under this Agreement, amounts for which it has been compensated, or claims he should be compensated, by The Authority above those included in the lump sum compensation set forth elsewhere herein. All Contractor records shall be kept in the Port District. The Contractor shall obtain for The Authority similar access to similar records and documents of subcontractors. Such access shall be given or obtained both before and within a period of three (3) years after Final Payment to the Contractor, provided, however, that if within the aforesaid one year period The Authority has notified the Contractor in writing of a pending claim by The Authority under or in connection with this Contract to which any of the aforesaid records and documents of the Contractor or of his subcontractors relate either directly or indirectly, then the period of such right of access shall be extended to the expiration of six (6) years from the date of Final Payment with respect to the records and documents involved.

Upon request of the Port Authority, the Contractor shall furnish or provide access to the federal Form I-9 (Employment Eligibility Verification) for each individual performing work under this Contract. This includes citizens and noncitizens.

The Contractor shall provide, at no cost to the Authority, access for and reasonable assistance to such auditors from the Authority or the Authority's external auditors that may, from time to time,

be designated to audit detail records which support Contractor charges to the Authority. The Authority shall have access to the detail records that support Contractor charges to the Authority for up to three (3) years following the termination of the Contract.

No provision in this Contract giving The Authority a right of access to records and documents is intended to impair or affect any right of access to records and documents that The Authority would have in the absence of such provision.

35. HARMONY

a. The Contractor shall not employ any persons or use any labor, or use or have any equipment, or permit any condition to exist which shall or may cause or be conducive to any labor complaints, troubles, disputes or controversies at the Facility which interfere or are likely to interfere with the operation of the Port Authority or with the operations of lessees, licensees or other users of the Facility or with the operations of the Contractor under this Contract.

   The Contractor shall immediately give notice to the Port Authority (to be followed by written notices and reports) of any and all impending or existing labor complaints, troubles, disputes or controversies and the progress thereof. The Contractor shall use its best efforts to resolve any such complaint, trouble, dispute or controversy. If any type of strike, boycott, picketing, work stoppage, slowdown or other labor activity is directed against the Contractor at the Facility or against any operations of the Contractor under this Contract, whether or not caused by the employees of the Contractor, and if any of the foregoing, in the opinion of the Port Authority, results or is likely to result in any curtailment or diminution of the services to be performed hereunder or to interfere with or affect the operations of the Port Authority , or to interfere with or affect the operations of lessees, licensees, or other users of the Facility or in the event of any other cessation or stoppage of operations by the Contractor hereunder for any reason whatsoever, the Port Authority shall have the right at any time during the continuance thereof to suspend the operations of the Contractor under this Contract, and during the period of the suspension the Contractor shall not perform its services hereunder and the Port Authority shall have the right during said period to itself or by any third person or persons selected by it to perform said services of the Contractor using the equipment which is used by the Contractor in its operations hereunder as the Port Authority deems necessary and without cost to the Port Authority. During such time of suspension, the Contractor shall not be entitled to any compensation. Any flat fees, including management fees, shall be prorated. Prior to the exercise of such right by the Port Authority, it shall give the Contractor notice thereof, which notice may be oral. No exercise by the Port Authority of the rights granted to it in the above subparagraph shall be or be deemed to be a waiver of any rights of termination or revocation contained in this Contract or a waiver of any rights or remedies which may be available to the Port Authority under this Contract or otherwise.

b. During the time that the Contractor is performing the Contract, other persons may be engaged in other operations on or about the worksite including Facility operations, pedestrian, bus and vehicular traffic and other Contractors performing at the worksite, all of which shall remain uninterrupted.

   The Contractor shall so plan and conduct its operations as to work in harmony with others engaged at the site and not to delay, endanger or interfere with the operation of others (whether or not specifically mentioned above), all to the best interests of the Port Authority and the public as may be directed by the Port Authority.

36. CLAIMS OF THIRD PERSONS

The Contractor undertakes to pay all claims lawfully made against him by subcontractors, materialmen and workmen, and all claims lawfully made against him by other third persons arising out of or in connection with or because of the performance of this Contract and to cause all subcontractors to pay all such claims lawfully made against them.

37. NO DISCRIMINATION IN EMPLOYMENT, EQUAL EMPLOYMENT OPPORTUNITY

During the performance of this Contract, the Contractor agrees as follows:

A. The Contractor is advised to ascertain and comply with all applicable Federal, State and Local statutes, ordinances, rules and regulations and Federal Executive Orders pertaining to equal employment opportunity, affirmative action and non-discrimination in employment.

B Without limiting the generality of any other term or provision of this Contract, in the event of the Contractor's non-compliance with any such statutes, ordinances, rules, regulations or orders, this Contract may be canceled, terminated, or suspended in whole or in part.

38. CONTRACTOR'S INTEGRITY PROVISIONS

Certification of No Investigation (criminal or civil anti-trust), Indictment, Conviction, Debarment, Suspension, Disqualification and Disclosure of Other Information:

1. By bidding on this Contract, each Proposer and each person signing on behalf of any Proposer certifies, and in the case of a joint bid each party thereto certifies as to its own organization, that the Proposer and each parent and/or affiliate of the Proposer has not

a. been indicted or convicted in any jurisdiction;
b. been suspended, debarred, found not responsible or otherwise disqualified from entering into any contract with any governmental agency or been denied a government contract for failure to meet standards related to the integrity of the Proposer;
c. had a contract terminated by any governmental agency for breach of contract or for any cause based in whole or in part on an indictment or conviction;
d. ever used a name, trade name or abbreviated name, or an Employer Identification Number different from those inserted in the Bid;

e. had any business or professional license suspended or revoked or, within the five years prior to bid opening, had any sanction imposed in excess of $50,000 as a result of any judicial or administrative proceeding with respect to any license held or with respect to any violation of a federal, state or local environmental law, rule or regulation;
f. had any sanction imposed as a result of a judicial or administrative proceeding related to fraud, extortion, bribery, bid rigging, embezzlement, misrepresentation or anti-trust regardless of the dollar amount of the sanctions or the date of their imposition; and
g. been, and is not currently, the subject of a criminal investigation by any federal, state or local prosecuting or investigative agency and/or a civil anti-trust investigation by any federal, state or local prosecuting or investigative agency.

2. Non-Collusive Bidding, and Code of Ethics Certification, Certification of No Solicitation Based On Commission, Percentage, Brokerage, Contingent or Other Fees

By bidding on this Contract, each Proposer and each person signing on behalf of any Proposer certifies, and in the case of a joint bid, each party thereto certifies as to its own organization, that

a. the prices in its bid have been arrived at independently without collusion, consultation, communication or agreement for the purpose of restricting competition, as to any matter relating to such prices with any other Proposer or with any competitor;
b. the prices quoted in its bid have not been and will not be knowingly disclosed directly or indirectly by the Proposer prior to the official opening of such bid to any other Proposer or to any competitor;
c. no attempt has been made and none will be made by the Proposer to induce any other person, partnership or corporation to submit or not to submit a bid for the purpose of restricting competition;
d. this organization has not made any offers or agreements or taken any other action with respect to any Authority employee or former employee or immediate family member of either which would constitute a breach of ethical standards under the Code of Ethics dated April 11, 1996, (a copy of which is available upon request to the individual named in the clause hereof entitled "Proposer's Questions"), nor does this organization have any knowledge of any act on the part of an Authority employee or former Authority employee relating either directly or indirectly to this organization which constitutes a breach of the ethical standards set forth in said Code;
e. no person or selling agency other than a bona fide employee or bona fide established commercial or selling agency maintained by the Proposer for the purpose of securing business, has been employed or retained by the Proposer to solicit or secure this Contract on the understanding that a commission, percentage, brokerage, contingent, or other fee would be paid to such person or selling agency; and
f. the Proposer has not offered, promised or given, demanded or accepted, any undue advantage, directly or indirectly, to or from a public official or employee, political candidate, party or party official, or any private sector employee (including a person who directs or works for a private sector enterprise in any capacity), in order to obtain, retain, or direct business or to secure any other improper advantage in connection with this Contract.
g. no person or organization has been retained, employed or designated on behalf of the Proposer to impact any Port Authority determination with respect to (i) the solicitation, evaluation or award of this Contract; or (ii) the preparation of specifications or request for submissions in connection with this Contract.

The foregoing certifications shall be deemed to be made by the Proposer as follows:

* if the Proposer is a corporation, such certification shall be deemed to have been made not only with respect to the Proposer itself, but also with respect to each parent, affiliate, director, and officer of the Proposer, as well as, to the best of the certifier's knowledge and belief, each stockholder of the Proposer with an ownership interest in excess of 10%;
* if the Proposer is a partnership, such certification shall be deemed to have been made not only with respect to the Proposer itself, but also with respect to each partner.

Moreover, the foregoing certifications, if made by a corporate Proposer, shall be deemed to have been authorized by the Board of Directors of the Proposer, and such authorization shall be deemed to include the signing and submission of the bid and the inclusion therein of such certification as

the act and deed of the corporation.

In any case where the Proposer cannot make the foregoing certifications, the Proposer shall so state and shall furnish with the signed bid a signed statement that sets forth in detail the reasons therefor. If the Proposer is uncertain as to whether it can make the foregoing certifications, it shall so indicate in a signed statement furnished with its bid, setting forth in such statement the reasons for its uncertainty. With respect to the foregoing certification in paragraph "2g", if the Proposer cannot make the certification, it shall provide, in writing, with the signed bid: (i) a list of the name(s), address(es), telephone number(s), and place(s) of principal employment of each such individual or organization; and (ii) a statement as to whether such individual or organization has a "financial interest" in this Contract, as described in the Procurement Disclosure policy of the Authority (a copy of which is available upon request to the Director of the Procurement Department of the Authority). Such disclosure is to be updated, as necessary, up to the time of award of this Contract. As a result of such disclosure, The Port Authority shall take appropriate action up to and including a finding of non-responsibility.

Failure to make the required disclosures shall lead to administrative actions up to and including a finding of non-responsibility.

Notwithstanding that the Proposer may be able to make the foregoing certifications at the time the bid is submitted, the Proposer shall immediately notify the Authority in writing during the period of irrevocability of bids on this Contract of any change of circumstances which might under this clause make it unable to make the foregoing certifications or require disclosure. The foregoing certifications or signed statement shall be deemed to have been made by the Proposer with full knowledge that they would become a part of the records of the Authority and that the Authority will rely on their truth and accuracy in awarding this Contract. In the event that the Authority should determine at any time prior or subsequent to the award of this Contract that the Proposer has falsely certified as to any material item in the foregoing certifications or has willfully or fraudulently furnished a signed statement which is false in any material respect, or has not fully and accurately represented any circumstance with respect to any item in the foregoing certifications required to be disclosed, the Authority may determine that the Proposer is not a responsible Proposer with respect to its bid on the Contract or with respect to future bids on Authority contracts and may exercise such other remedies as are provided to it by the Contract with respect to these matters. In addition, Proposers are advised that knowingly providing a false certification or statement pursuant hereto may be the basis for prosecution for offering a false instrument for filing (see e.g. New York Penal Law, Section 175.30 et seq.). Proposers are also advised that the inability to make such certification will not in and of itself disqualify a Proposer, and that in each instance the Authority will evaluate the reasons therefor provided by the Proposer. Under certain circumstances the Proposer may be required as a condition of Contract award to enter into a Monitoring Agreement under which it will be required to take certain specified actions, including compensating an independent Monitor to be selected by the Port Authority, said Monitor to be charged with, among other things, auditing the actions of the Proposer to determine whether its business practices and relationships indicate a level of integrity sufficient to permit it to continue business with the Port Authority.

3. Proposer Eligibility for Award of Contracts - Determination by an Agency of the State of New York or New Jersey Concerning Eligibility to Receive Public Contracts

Proposers are advised that the Authority has adopted a policy to the effect that in awarding its contracts it will honor any determination by an agency of the State of New York or New Jersey that a Proposer is not eligible to bid on or be awarded public contracts because the Proposer has

been determined to have engaged in illegal or dishonest conduct or to have violated prevailing rate of wage legislation.

The policy permits a Proposer whose ineligibility has been so determined by an agency of the State of New York or New Jersey to submit a bid on a Port Authority contract and then to establish that it is eligible to be awarded a contract on which it has bid because (i) the state agency determination relied upon does not apply to the Proposer, or (ii) the state agency determination relied upon was made without affording the Proposer the notice and hearing to which the Proposer was entitled by the requirements of due process of law, or (iii) the state agency determination was clearly erroneous or (iv) the state determination relied upon was not based on a finding of conduct demonstrating a lack of integrity or violation of a prevailing rate of wage law.

The full text of the resolution adopting the policy may be found in the Minutes of the Authority's Board of Commissioners meeting of September 9, 1993.

4. No Gifts, Gratuities, Offers of Employment, Etc.

During the term of this Contract, the Contractor shall not offer, give or agree to give anything of value either to a Port Authority employee, agent, job shopper, consultant, construction manager or other person or firm representing the Port Authority, or to a member of the immediate family (i.e., a spouse, child, parent, brother or sister) of any of the foregoing, in connection with the performance by such employee, agent, job shopper, consultant, construction manager or other person or firm representing the Port Authority of duties involving transactions with the Contractor on behalf of the Port Authority, whether or not such duties are related to this Contract or any other Port Authority contract or matter. Any such conduct shall be deemed a material breach of this Contract.

As used herein "anything of value" shall include but not be limited to any (a) favors, such as meals, entertainment, transportation (other than that contemplated by the Contract or any other Port Authority contract), etc. which might tend to obligate the Port Authority employee to the Contractor, and (b) gift, gratuity, money, goods, equipment, services, lodging, discounts not available to the general public, offers or promises of employment, loans or the cancellation thereof, preferential treatment or business opportunity. Such term shall not include compensation contemplated by this Contract or any other Port Authority contract. Where used herein, the term "Port Authority" shall be deemed to include all subsidiaries of the Port Authority.

The Contractor shall insure that no gratuities of any kind or nature whatsoever shall be solicited or accepted by it and by its personnel for any reason whatsoever from the passengers, tenants, customers or other persons using the Facility and shall so instruct its personnel.

In addition, during the term of this Contract, the Contractor shall not make an offer of employment or use confidential information in a manner proscribed by the Code of Ethics and Financial Disclosure dated April 11, 1996, (a copy of which is available upon request to the Office of the Secretary of the Port Authority).

The Contractor shall include the provisions of this clause in each subcontract entered into under this Contract.

5. Conflict of Interest

During the term of this Contract, the Contractor shall not participate in any way in the preparation, negotiation or award of any contract (other than a contract for its own services to the Authority) to

which it is contemplated the Port Authority may become a party, or participate in any way in the review or resolution of a claim in connection with such a contract if the Contractor has a substantial financial interest in the contractor or potential contractor of the Port Authority or if the Contractor has an arrangement for future employment or for any other business relationship with said contractor or potential contractor, nor shall the Contractor at any time take any other action which might be viewed as or give the appearance of conflict of interest on its part. If the possibility of such an arrangement for future employment or for another business arrangement has been or is the subject of a previous or current discussion, or if the Contractor has reason to believe such an arrangement may be the subject of future discussion, or if the Contractor has any financial interest, substantial or not, in a contractor or potential contractor of the Authority, and the Contractor's participation in the preparation, negotiation or award of any contract with such a contractor or the review or resolution of a claim in connection with such a contract is contemplated or if the Contractor has reason to believe that any other situation exists which might be viewed as or give the appearance of a conflict of interest, the Contractor shall immediately inform the Director in writing of such situation giving the full details thereof. Unless the Contractor receives the specific written approval of the Director, the Contractor shall not take the contemplated action which might be viewed as or give the appearance of a conflict of interest. In the event the Director shall determine that the performance by the Contractor of a portion of its Services under this Agreement is precluded by the provisions of this numbered paragraph, or a portion of the Contractor's said Services is determined by the Director to be no longer appropriate because of such preclusion, then the Director shall have full authority on behalf of both parties to order that such portion of the Contractor's Services not be performed by the Contractor, reserving the right, however, to have the Services performed by others and any lump sum compensation payable hereunder which is applicable to the deleted work shall be equitably adjusted by the parties. The Contractor's execution of this document shall constitute a representation by the Contractor that at the time of such execution the Contractor knows of no circumstances, present or anticipated, which come within the provisions of this paragraph or which might otherwise be viewed as or give the appearance of a conflict of interest on the Contractor's part. The Contractor acknowledges that the Authority may preclude it from involvement in certain disposition/privatization initiatives or transactions that result from the findings of its evaluations hereunder or from participation in any contract which results, directly or indirectly, from the Services provided by the Contractor hereunder.

III. Definitions

As used in this section, the following terms shall mean:

Affiliate - Two or more firms are affiliates if a parent owns more than fifty percent of the voting stock of each of the firms, or a common shareholder or group of shareholders owns more than fifty percent of the voting stock of each of the firms, or if the firms have a common proprietor or general partner.

Agency or Governmental Agency - Any federal, state, city or other local agency, including departments, offices, public authorities and corporations, boards of education and higher education, public development corporations, local development corporations and others.

Investigation - Any inquiries made by any federal, state or local criminal prosecuting agency and any inquiries concerning civil anti-trust investigations made by any federal, state or local governmental agency. Except for inquiries concerning civil anti-trust investigations, the term does not include inquiries made by any civil government agency concerning compliance with any regulation, the nature of which does not carry criminal penalties, nor does it include any background investigations for employment, or Federal,

State, and local inquiries into tax returns.

Officer - Any individual who serves as chief executive officer, chief financial officer, or chief operating officer of the Proposer by whatever titles known.

Parent - An individual, partnership, joint venture or corporation which owns more than 50% of the voting stock of the Proposer.

If the solicitation is a Request for Proposal:

Bid - shall mean Proposal;
Proposer - shall mean Proposer;
Bidding - shall mean submitting a Proposal.

In a Contract resulting from the taking of bids:

Bid - shall mean bid;
Proposer - shall mean Proposer;
Bidding - shall mean executing this Contract.

In a Contract resulting from the taking of Proposals:

Bid - shall mean Proposal;
Proposer - shall mean Proposer;
Bidding - shall mean executing this Contract.

39. CONFIDENTIAL INFORMATION/NON-PUBLICATION

A. As used herein, confidential information shall mean all information disclosed to the Contractor or the personnel provided by the Contractor hereunder which relates to the Authority's and/or PATH's past, present, and future research, development and business activities including, but not limited to, software and documentation licensed to the Authority or proprietary to the Authority and/or PATH and all associated software, source code procedures and documentation. Confidential information shall also mean any other tangible or intangible information or materials including but not limited to computer identification numbers, access codes, passwords, and reports obtained and/or used during the performance of the Contractor's Services under this Contract.

B. Confidential information shall also mean and include collectively, as per *The Port Authority of New York & New Jersey Information Security Handbook (October 15, 2008, corrected as of February, 9 2009),* Confidential Proprietary Information, Confidential Privileged Information and information that is labeled, marked or otherwise identified by or on behalf of the Authority so as to reasonably connote that such information is confidential, privileged, sensitive or proprietary in nature. Confidential Information shall also include all work product that contains or is derived from any of the foregoing, whether in whole or in part, regardless of whether prepared by the Authority or a third-party or when the Authority receives such information from others and agrees to treat such information as Confidential.

C. The Contractor shall hold all such confidential information in trust and confidence for the Authority, and agrees that the Contractor and the personnel provided by the Contractor hereunder shall not, during or after the termination or expiration of this Contract, disclose to any person, firm or corporation, nor use for its own business or benefit, any information obtained by it under or in connection with the supplying of services contemplated by this Contract. The Contractor and the

personnel provided by the Contractor hereunder shall not violate in any manner any patent, copyright, trade secret or other proprietary right of the Authority or third persons in connection with their services hereunder, either before or-after termination or expiration of this Contract. The Contractor and the personnel provided by the Contractor hereunder shall not willfully or otherwise perform any dishonest or fraudulent acts, breach any security procedures, or damage or destroy any hardware, software or documentation, proprietary or otherwise, in connection with their services hereunder. The Contractor shall promptly and fully inform the Director/General Manager in writing of any patent, copyright, trade secret or other intellectual property rights or disputes, whether existing or potential, of which the Contractor has knowledge, relating to any idea, design, method, material, equipment or other matter related to this Contract or coming to the Contractor's attention in connection with this Contract."

D. The Contractor shall not issue nor permit to be issued any press release, advertisement, or literature of any kind, which refers to the Port Authority or to the fact that goods have been, are being or will be provided to it and/or that services have been, are being or will be performed for it in connection with this Agreement, unless the vendor first obtains the written approval of the Port Authority. Such approval may be withheld if for any reason the Port Authority believes that the publication of such information would be harmful to the public interest or is in any way undesirable.

40. PROVISIONS OF LAW DEEMED INSERTED

Each and every provision of law and clause required by law to be inserted in this Contract shall be deemed to be inserted herein and the Contract shall be read and enforced as though it were included therein, and if through mistake or otherwise any such provision is not inserted, or is not correctly inserted, then upon the application of either party, the Contract shall forthwith be physically amended to make such insertion.

41. INVALID CLAUSES

If any provision of this Contract shall be such as to destroy its mutuality or to render it invalid or illegal, then if it shall not appear to have been so material that without it the Contract would not have been made by the parties, it shall not be deemed to form part thereof but the balance of the Contract shall remain in full force and effect.

42. NO ESTOPPEL OR WAIVER

The Authority shall not be precluded or estopped by any acceptance, certificate or payment, final or otherwise, issued or made under this Contract or otherwise issued or made by it, the Director or any officer, agent or employee of The Authority, from showing at any time the true amount and character of Work performed, or from showing that any such acceptance, certificate or payment is incorrect or was improperly issued or made; and The Authority shall not be precluded or estopped, notwithstanding any such acceptance, certificate or payment, from recovering from the Contractor any damages which it may sustain by reason of any failure on his part to comply strictly with this Contract, and any monies which may be paid to him or for his account in excess of those to which he is lawfully entitled.

43. NON-LIABILITY OF THE AUTHORITY REPRESENTATIVES

Neither the Commissioners of the Authority, nor any officer, agent, or employee thereof shall be charged personally by the Contractor with any liability or held liable under any term or provision of this Contract, or because of its execution or attempted execution, or because of any breach hereof.

44. MODIFICATION OF CONTRACT

No change in or modification, termination or discharge of this Contract, in any form whatsoever, shall be valid or enforceable unless it is in writing and signed by the party to be charged therewith or his duly authorized representative, provided, however, that any change in or modification, termination or discharge of this Contract expressly provided for in this Contract shall be effective as so provided.

45. M/WBE GOOD FAITH PARTICIPATION

If specified as applicable to this Contract, the Contractor shall use every good-faith effort to provide for participation by certified Minority Business Enterprises (MBEs) and certified Women-owned Business Enterprises (WBEs) as herein defined, in all purchasing and subcontracting opportunities associated with this Contract, including purchase of equipment, supplies and labor services.

Good Faith efforts to include participation by MBEs/WBEs shall include the following:

a. Dividing the services and materials to be procured into small portions, where feasible.

b. Giving reasonable advance notice of specific contracting, subcontracting and purchasing opportunities to such MBEs/WBEs as may be appropriate.

c. Soliciting services and materials from a Port Authority certified MBE/WBE or seeking MBEs/WBEs from other sources. To access the Port Authority's Directory of MBE/WBE Certified Firms go to www.panynj.gov/supplierdiversty

d. Ensuring that provision is made to provide progress payments to MBEs/WBEs on a timely basis.

e. Observance of reasonable commercial standards of fair dealing in the respective trade or business.

Either prior or subsequent to Contract award, the Contractor may request a full or partial waiver of the M/WBE participation goals set forth in this Contract by providing documentation demonstrating to the Manager, for approval by the Port Authority's Office of Business Diversity and Civil Rights, that its good faith efforts did not result in compliance with the goals set forth above because participation by eligible M/WBEs could not be obtained at a reasonable price or that such M/WBEs were not available to adequately perform as subcontractors. The Contractor shall provide written documentation in support of its request to the Manager. The documentation shall include, but not be limited to, documentation demonstrating good faith efforts as described above, which may include, proof that the Authority's directory does not contain M/WBEs in this specific field of work, a list of organizations contacted to obtain M/WBEs, and/or a list of M/WBEs contacted and their price quotes. If approved by the Authority's Office of Business Diversity and Civil Rights, the Manager will provide written approval of the modified or waived M/WBE Participation Plan.

Subsequent to Contract award, all changes to the M/WBE Participation Plan must be submitted via a modified M/WBE Participation Plan to the Manager for review and approval by the Authority's Office of Business Diversity and Civil Rights. For submittal of modifications to the M/WBE Plan, Contractors are directed to use form PA3749C, which may be downloaded at http://www.panynj.gov/business-opportunities/become-vendor.html. The Contractor shall not make changes to its approved M/WBE Participation Plan or substitute M/WBE subcontractors or suppliers for those named in their approved plan without the Manager's prior written approval.

Unauthorized changes or substitutions, including performing the work designated for a subcontractor with the Contractor's own forces, shall be a violation of this section. Progress toward attainment of M/WBE participation goals set forth herein will be monitored throughout the duration of this Contract.
The Contractor shall also submit to the Manager, along with invoices, the Statement of Subcontractor Payments as the M/WBE Participation Report, which may be downloaded at http://www.panynj.gov/business-opportunities/become-vendor.html. The Statement must include the name and business address of each M/WBE subcontractor and supplier actually involved in the Contract, a description of the work performed and/or product or service supplied by each such subcontractor or supplier, the date and amount of each expenditure, and such other information that may assist the Manager in determining the Contractor's compliance with the foregoing provisions.

If, during the performance of this Contract, the Contractor fails to demonstrate good faith efforts in carrying out its M/WBE Participation Plan and the Contractor has not requested and been granted a full or partial waiver of the M/WBE participation goals set forth in this Contract, the Authority will take into consideration the Contractor's failure to carry out its M/WBE Participation Plan in its evaluation for award of future Authority contracts.

46. TRASH REMOVAL

The Contractor shall remove daily from the Facility by means provided by the Contractor all garbage, debris and other waste material (solid or liquid) arising out of or in connection with its operations hereunder, and any such garbage, debris and other waste material not immediately removed shall be temporarily stored in a clear and sanitary condition, approved by the Manager of the Facility, and shall be kept covered except when filling or emptying them. The Contractor shall exercise care in removing such garbage, debris and other waste materials from the Facility. The manner of such storage and removal shall always be subject in all respects to the continual approval of the Port Authority. No equipment or facilities of the Port Authority shall be used in such removal unless with its prior consent in writing. No such garbage, debris or other waste materials shall be or be permitted to be thrown, discharged or disposed into or upon the waters at or bounding the Facility.

47. ENTIRE AGREEMENT

This Contract including the Request for Proposals for #32792 (including its Scope of Works and other attachments, endorsements and exhibits, if any,) as well as the Proposal submitted by the Contractor contains the entire agreement between the parties. In the event of any inconsistency between this Contract and other attachments, endorsements and exhibits, if any, including the Proposal submitted by the Contractor, this Contract shall be controlling.

ATTACHMENT C

PART III - COST PROPOSAL FORM

ENTRY OF PRICES

a. The prices quoted shall be written in figures, in ink, preferably in black ink where required in the spaces provided on the Cost Proposal Form(s) attached hereto and made a part hereof.

b. All Proposers are asked to ensure that all charges quoted for similar operations in the Contract are consistent.

c. Prices must be submitted for each Item required on the Cost Proposal Form(s). Proposers are advised that the Items on the Cost Proposal Form(s) correspond to the required services set forth in the Contract hereunder.

d. Proposers are asked to ensure that all figures are inserted as required, and that all computations made have been verified for accuracy. The Proposer is advised that the Port Authority may verify only that RFP or those RFPs that it deems appropriate and may not check each and every RFP submitted for computational errors. In the event that errors in computation are made by the Proposer, the Port Authority reserves the right to correct any error and to recompute the Estimated Total Five (5) Year Contract Price, as required, based upon the applicable unit prices inserted by the Proposer, which amount shall govern in all cases

e. In the event that a Proposer quotes an amount in the Estimated annual column but omits to quote an Hourly Rate or Monthly Charge/Fee for that amount in the space provided, the Port Authority reserves the right to compute and insert the appropriate unit price.

f. The Total Costs for the five (5) Year Contract Price is solely for the purpose of facilitating the comparisons of RFPs. Compensation shall be in accordance with the section of this Contract entitled "Billing and Payment".

g. The Total Estimated Contract Price shall be obtained by adding the Estimated Total Contract Price for the first year of the Contract to the Estimated Annual Contract Price for each subsequent year.

DATE: March 19, 2013 | Cost Proposal Form | RFP #32792

Aviation and World Trade Center - Year 1 (August 29, 2013 - August 31, 2014)

	Estimated Annual Hours*		Hourly Rate		Total Estimated Annual Cost	
A) Security Auditors						
1) Aviation Auditors	14,500	x	$	=	$	(1)
2) WTC Auditors	2,150	x	$	=	$	(2)
Total	16,650	A	(1) + (2)	=	$	**(A)**

B) MANAGEMENT FEE	Monthly Charge*		*# of Months*		Total Annual Charge	
1) Avia Management Fee:	$	x	12	=	$	(1)
2) WTC Management Fee:	$	x	12	=	$	(2)
Total		B	(1) + (2)	=	$	**(B)**

Total Estimated Annual Contract Amount - Year 1

(A) + (B) = $

DATE: March 19, 2013

Cost Proposal Form

RFP #32792

Aviation and World Trade Center - Year 2 (September 1, 2014 - August 31, 2015)

	Estimated Annual Hours*		Hourly Rate		Total Estimated Annual Cost	
A) Security Auditors						
1) Aviation Auditors	14,500	x	$	=	$	(1)
2) WTC Auditors	2,150	x	$	=	$	(2)
Total	16,650	A	(1) + (2)	=	$	**(A)**

B) MANAGEMENT FEE	Monthly Charge*		*# of Months*		Total Annual Charge	
1) Avia Management Fee:	$	x	12	=	$	(1)
2) WTC Management Fee:	$	x	12	=	$	(2)
Total		B	(1) + (2)	=	$	**(B)**

Total Estimated Annual Contract Amount - Year 2

(A) + (B) = $

DATE: March 19, 2013

Cost Proposal Form

RFP #32792

Aviation and World Trade Center - Year 3 (September 1, 2015 - August 31, 2016)

	Estimated Annual Hours*		Hourly Rate		Total Estimated Annual Cost	
A) Security Auditors						
1) Aviation Auditors	14,500	x	$	=	$	(1)
2) WTC Auditors	2,150	x	$	=	$	(2)
Total	16,650	A	(1) + (2)	=	$	**(A)**

B) MANAGEMENT FEE	Monthly Charge*		*# of Months*		Total Annual Charge	
1) Avia Management Fee:	$	x	12	=	$	(1)
2) WTC Management Fee:	$	x	12	=	$	(2)
Total		B	(1) + (2)	=	$	**(B)**

Total Estimated Annual Contract Amount - Year 3

(A) + (B) = $

DATE: March 19, 2013

Cost Proposal Form

RFP #32792

Aviation and World Trade Center - Year 4 (September 1, 2016 - August 31, 2017)

	Estimated Annual Hours*		Hourly Rate		Total Estimated Annual Cost	
A) Security Auditors						
1) Aviation Auditors	14,500	x	$	=	$	(1)
2) WTC Auditors	2,150	x	$	=	$	(2)
Total	16,650	A	(1) + (2)	=	$	**(A)**

B) MANAGEMENT FEE	Monthly Charge*		*# of Months*		Total Annual Charge	
1) Avia Management Fee:	$	x	12	=	$	(1)
2) WTC Management Fee:	$	x	12	=	$	(2)
Total		B	(1) + (2)	=	$	**(B)**

Total Estimated Annual Contract Amount - Year 4
(A) + (B) = $

DATE: March 19, 2013

RFP #32792

Cost Proposal Form

Aviation and World Trade Center - Year 4 (September 1, 2017 - August 31, 2018)

	Estimated Annual Hours*		Hourly Rate		Total Estimated Annual Cost	
A) Security Auditors						
1) Aviation Auditors	14,500	x	$	=	$	(1)
2) WTC Auditors	2,150	x	$	=	$	(2)
Total	16,650	A	(1) + (2)	=	$	**(A)**

B) MANAGEMENT FEE	Monthly Charge*		*# of Months*		Total Annual Charge	
1) Avia Management Fee:	$	x	12	=	$	(1)
2) WTC Management Fee:	$	x	12	=	$	(2)
Total		B	(1) + (2)	=	$	**(B)**

Total Estimated Annual Contract Amount - Year 5

(A) + (B) = $

Aviation and World Trade Center (Years 1-5) Summary Sheet

Total Contract Cost

(A)Estimated Annual Contract Cost- First Year = _____

(B)Estimated Annual Contract Cost - Second Year = _____

(C)Estimated Annual Contract Cost - Third Year = _____

(D)Estimated Annual Contract Cost - Fourth Year = _____

(E)Estimated Annual Contract Cost - Fifth Year = _____

Total Estimate Contract Price for the 5 year based period (Years 1-5) [A+B+C+D+E] = _____

Security Audit Services RFP #32792

Monthly Management Fee Cost Proposal Sheet for JFK, EWR, LGA, TEB, SWF and WTC*

		Title	Description	Year 1 Total	Year 2 Total	Year 3 Total	Year 4 Total	Year 5 Total	Total
a		FACILITY (PAYROLL)	CONTRACTOR'S STAFF LOCATED ON PORT AUTHORITY SITES.						
	1	Project Management Staff	List quantity and titles: 1 Project Manager (JFK, LGA, and WTC), 1 Project Manager (EWR, TEB, and SWF). Please note: The Project Manager stationed at JFK will be covering JFK, LGA and WTC. The Project Manager stationed at EWR will be covering SWF and TEB.						
	2	Facility Support Staff	List quantity and titles: 1 Administrative Assistant (JFK, LGA, and WTC), 1 Administrative Assistant (EWR, TEB, and SWF)						
	3	Incentive Pay Plan							
	4	Payroll Taxes and Fringe Benefits							
	A	**Total Salaries and Wages, Payroll Taxes and Fringe (A=1+2+3+4)**							
b		**FACILITY (OTHERS)**							
	1	Memberships	List all types:						
	2	Conferences	List all types:						
	3	Communication Devices	List service provider, # of users, type of device, service plans:						
	B	**Total Personnel Expenses (B=1+2+3)**							
c		**CONTRACTOR'S OFF-SITE SUPPORT**	**NOT LOCATED ON PORT AUTHORITY SITES.**						
	1	Forms and Supplies	List all types:						
	2	Office Equipment	List all types:						
	3	Hardware & Software	List all types:						
	4	Telephone & System Communications	List all types and use:						
	5	Faxes and Copiers	List quantity:						
	6	Web & Network Support	List all:						
	C	**Total Headquarters Support (C=1+2+3+4+5+6)**							
d		**OTHERS**							
	1	Insurance (Required by law)	Cost to comply with PA requirements.						
	2	Taxes (Required by law)	List all types:						
	3	General & Administrative	List all and percent:						
	4	Overhead	List all and percent:						
	5	Profit	List all and percent:						
	6	Other	List all others:						
	D	**Total Others (D=1+2+3+4+5+6)**							
e		**ANNUAL TOTAL = A+B+C+D**	**AVIA (82%)**						
			WTC (18%)						
			TOTAL						
f		**MONTHLY TOTAL = e/12 months**	**AVIA (82%)**						
			WTC (18%)						
			TOTAL						

***Monthly Management Fee applies to listed services at the following facilities:**	
John F. Kennedy International (JFK)	Security audits
LaGuardia (LGA)	Security audits
Newark Liberty International (EWR)	Security audits
Stewart International (SWF)	Security audits
Teterboro (TEB)	Security audits
World Trade Center (WTC)	Security audits

ATTACHMENT C- PROPOSER REFERENCE FORM

Name of Proposer:_____

Please provide a list of references on the firm's performance of similar work within the last five years, including all current contracts. Use additional sheets as necessary.

Include the following information for each reference:

Customer Name:_____
Address:_____
Contact Name and Title:_____
Phone and Fax Numbers of Contact:_____
Contract date(s):_____
Contract cost:_____
Description of work:
_____
_____
_____

Customer Name:_____
Address:_____
Contact Name and Title:_____
Phone and Fax Numbers of Contact:_____
Contract date(s):_____
Contract cost:_____
Description of Work:
_____
_____
_____

Customer Name:_____
Address:_____
Contact Name and Title:_____
Phone and Fax Numbers of Contact:_____
Contract date (s):_____
Contract cost:_____
Description of work:_____

ATTACHMENT D- M/WBE PARTICIPATION PLAN

*(AN M/WBE PARTICIPATION PLAN SHALL BE SUBMITTED AND WILL BE EVALUATED AS PART OF THE MANAGEMENT APPROACH. PLEASE INCLUDE FORM **PA 3749B**, TO BE COMPLETED BY THE PROPOSER FOR THE M/WBE PARTICIPATION PLAN SUBMISSION REQUIREMENT. IN THE EVENT OF AN M/WBE PLAN MODIFICATION, PLEASE USE FORM **PA 3749C**.)*

ATTACHMENT E- STATEMENT OF SUBCONTRACTOR PAYMENTS

INSTRUCTIONS FOR STATEMENT OF SUBCONTRACTOR PAYMENT

Attached is the Statement of Subcontractor Payments form, which shall be submitted with every invoice to be used in conjunction with the M/WBE Participation Plan.

STATEMENT OF SUBCONTRACTOR PAYMENTS

PA3968 / 03-09

M/WBE Participation Report

Instructions for Statement of Subcontractor Payment: To be submitted with every invoice to be used in conjunction with the M/WBE Participation Plan.

Contract/PO No.: _____

Contract Title: _____

Prime Contractor Name: _____

Contract/PO Amount: _____

PA Project Manager: _____

Date of Invoice: _____

Committed M/WBE Goals: M _____ W _____

Award Date: _____

Completion Date: _____

M/WBE Participation to Date: M _____ W _____

Subcontractor's Name	Address & Phone #	Description of Work Performed or Materials Supplied	M/WBE Status	Total Contract Amount Awarded	Total Previous Requests	Amount Paid to Date	Amount of This Request

In connection with the above-captioned contract: I HEREBY DECLARE AND AFFIRM that I am a duly authorized representative of this company, and that the following Minority and Women Business Enterprises have been contracted with and have furnished, or are furnishing and preparing materials for, and have done or are doing labor on the above captioned contract; that there is due and to become due them, respectively, the amounts set opposite their names for materials or labor as stated; and that this is a full, true, and complete statement of all such MBEs/WBEs and of the amounts paid, due, and to become due to them.

Signature	Print Name	Title	Date

ATTACHMENT F - Certified Environmentally Preferable Products/Practices

Proposer Name: _____ **Date:** _____

In line with the Port Authority's efforts to promote products and practices which reduce our impact on the environment and human health, Proposers are encouraged to provide information regarding their environmentally preferable/sustainable business practices as they relate to this contract wherever possible. Proposers **must** complete this form and submit it with their response, if appropriate. Proposers **must** submit appropriate documentation to support the items for which the Proposer indicates a "Yes" and present this documentation in the proper sequence of this Attachment.

1. Packaging

Has the Proposer implemented any of the following environmental initiatives? **(A checkmark indicates "Yes")**

____ Use of corrugated materials that exceed the EPA recommended post-consumer recycled content

____ Use of other packaging materials that contain recycled content and are recyclable in most local programs

____ Promotes waste prevention and source reduction by reducing the extent of the packaging and/or offering packaging take-back services, or shipping carton return

____ Reduces or eliminates materials which have been bleached with chlorine or chlorine derivatives

____ Eliminates any packaging that may contain polyvinyl chloride (PVC), or polystyrene or heavy metals

If yes, a description of the practices being followed must be included with the submission.

2. Business Practices / Operations / Manufacturing

Does the Proposer engage in practices that serve to reduce or minimize an impact to the environment, including, but not necessarily limited to, the following items? **(A checkmark indicates "Yes")**

____ Recycles materials in the warehouse or other operations

____ Use of alternative fuel vehicles or vehicles equipped with diesel emission control devices for delivery or transportation purposes

____ Use of energy efficient office equipment or signage or the incorporation of green building design elements

____ Use of recycled paper (that meets federal specifications) in their marketing and/or resource materials

____ Other sustainable initiative

If yes, a description of the practices being followed must be included with the submission.

3. Training and Education

Does the Proposer conduct/offer a program to train or inform customers and employees of the environmental benefits of the products to be offered under this contract, and/or does the Proposer conduct environmental training of its own staff?

☐ Yes ☐ No If yes, Proposer must attach a description of the training offered and the specific criteria targeted by the training.

4. Certifications

Has the Proposer or any of its manufacturers and/or subcontractors obtained any of the following product / industry certifications? **(A checkmark indicates "Yes")**

____ ISO 14000 or adopted some other equivalent environmental management system

____ Other industry environmental standards (where applicable), such as the CERES principles, LEED Certification, C2C Protocol, Responsible Care Codes of Practice or other similar standards

____ Third Party product certifications such as Green Seal, Scientific Certification Systems, Smartwood, etc.

If yes, Proposers must attach copies of the certificates obtained.

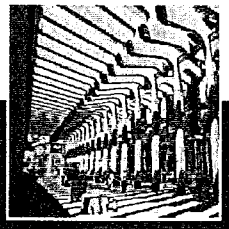
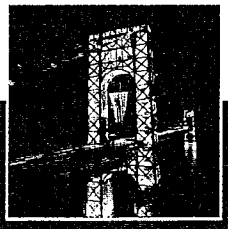
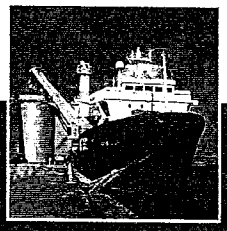
5. Other Environmental Criteria

Proposers are encouraged to respond to criteria specifically indicated in this RFP as "Management Approach" (and attach the appropriate documentation) to receive consideration in the evaluation.

I hereby certify, under penalty of the law that the above statements are true and correct.

_____ _____**Name** _____**Date**

ATTACHMENT G – PORT AUTHORITY INFORMATION SECURITY HANDBOOK

The Port Authority of New York & New Jersey

Information Security Handbook

October 15, 2008, corrected as of February 9, 2009

The Port Authority of New York and New Jersey

Information Security Handbook

Copyright © 2008 The Port Authority of New York and New Jersey

No copyright is claimed in the text of U.S. regulations or statutes quoted within.

3.6 UNAUTHORIZED DISCLOSURE OF INFORMATION 11

3.7 SECURITY CLEARANCE AND ACCESS PROHIBITIONS 11

3.8 BACKGROUND SCREENING 12

3.9 AUTHORIZED PERSONNEL CLEARANCE LIST 12

3.10 DEVELOPMENT OF CONFIDENTIAL INFORMATION PRACTICES AND PROCEDURES (CIPP) 12

3.11 PROCUREMENT STRATEGIES 13

CHAPTER 4

MARKING, HANDLING, STORAGE, TRANSMITTAL AND DESTRUCTION REQUIREMENTS 16

4.1 MARKING OF CONFIDENTIAL INFORMATION 16

4.2 HANDLING CONFIDENTIAL INFORMATION 18

4.3 TRANSMITTAL OF CONFIDENTIAL INFORMATION 18

4.4 STORAGE OF CONFIDENTIAL INFORMATION 21

4.5 DOCUMENT ACCOUNTABILITY LOG 21

4.6 REPRODUCTION 22

4.7 DESTRUCTION OF CONFIDENTIAL INFORMATION 22

CHAPTER 5

AUDITING AND MONITORING 23

5.1 PURPOSE 23

5.2 AUDITS AND INVESTIGATIONS 23

5.3 SELF-ASSESSMENT 24

CHAPTER 6

POLICY VIOLATIONS AND CONSEQUENCES 25

6.1 RESPONSIBILITIES 25

6.2 VIOLATIONS, INFRACTIONS, OR BREACH OF INFORMATION SECURITY PROTOCOLS 25

TABLE OF CONTENTS

Page

INTRODUCTION 1

CHAPTER 1

PORT AUTHORITY INFORMATION SECURITY ORGANIZATIONAL STRUCTURE 2

CHAPTER 2

CATEGORIZATION OF INFORMATION 4

2.1 DEFINITIONS 4

2.2 GENERAL PROCESS FOR CATEGORIZATION 5

2.3 TRAINING AND INFORMATION REVIEW 6

2.4 REMOVAL OF CATEGORY DESIGNATION 7

CHAPTER 3

INFORMATION ACCESS 8

3.1 APPLICABILITY 8

3.2 GENERAL CRITERIA 8

3.3 INFORMATION ACCESS CONTROLS 9

3.4 ACCESS DISQUALIFICATION 10

3.5 NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENTS (NDAs) 11

6.3 VIOLATION REPORTING, INVESTIGATION AND FACT FINDING 25

6.4 DISCIPLINARY ACTION 25

CHAPTER 7

INFORMATION SECURITY EDUCATION AND AWARENESS TRAINING 28

7.1 PURPOSE 28

7.2 OVERVIEW 28

7.3 TRAINING PROGRAM ELEMENTS 28

APPENDICES OF HANDBOOK

A – NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENTS

A-1: Non-Disclosure And Confidentiality Agreements with reference to Handbook

A-2: Non-Disclosure And Confidentiality Agreements without reference to Handbook

A-3: PA/PATH Employee Non-Disclosure And Confidentiality Agreement

B – INSTRUCTIONS ON NON-DISCLOSURE AND MAINTENANCE OF CONFIDENTIALITY OF PORT AUTHORITY CONFIDENTIAL INFORMATION

C – BACKGROUND SCREENING SPECIFICATIONS

D – THE SECURE WORKER ACCESS CONSORTIUM

E – COVERSHEET FOR CONFIDENTIAL PRIVILEGED INFORMATION

F – TRANSMITTAL RECEIPT

G –GUIDELINES FOR THE STORAGE OF CONFIDENTIAL INFORMATION

H – GUIDELINES FOR THE DISPOSAL AND DESTRUCTION OF CONFIDENTIAL INFORMATION

I - AUDIT PROCEDURES

INTRODUCTION

This *Port Authority of N.Y. & N.J. Information Security Handbook* ("Handbook") establishes guidelines and uniform processes and procedures for the identification, handling, receipt, tracking, care, storage and destruction of Confidential Information (as hereinafter defined) pursuant to The Port Authority of New York and New Jersey Information Security Policy (the "Policy"). This Handbook is intended to be the implementation guideline for that policy. It is also intended to complement the Port Authority Freedom Information Policy (FOI), inasmuch as it further defines certain information that may be exempt from release under FOI. The guidelines contained in this Handbook are not intended to, in any way, be in derogation of the FOI policy, which was adopted by the Committee of Operations in a Resolution, dated August 13, 1992.

This Handbook prescribes requirements and other safeguards that are needed in order to prevent unauthorized disclosure of Confidential Information and to control authorized disclosure and distribution of designated sensitive information, when it is released by The Port Authority of New York and New Jersey (the "Port Authority") either internally or externally. A major underlying principle, on which the Handbook is premised, is that there is a limited universe of sensitive information to which it applies. There is the expectation that prudent, informed and circumscribed judgments will be made by those staff members charged with the responsibility of identifying and properly designating sensitive information, as is provided for in this Handbook. In this regard, adherence to the Handbook's requirements will help ensure that the necessary care will be constantly and consistently undertaken in order to ensure that mis-designation, or "over marking", of information will be avoided. Another important principle of the Handbook is that access to properly designated sensitive information is premised on a strict "need to know" basis. It is the establishment of this "need to know" that is the essential prerequisite for being granted access privileges. It must be emphasized that possession of a federal security clearance or other access rights and/or privileges to sensitive information does not *per se* establish a "need to know" for purposes of obtaining access to discrete sensitive Port Authority information. This principle is equally applicable to the Port Authority and its internal staff as it is to third party individuals and entities, which are given access privileges to sensitive Port Authority information.

The procedures and processes described in this Handbook are intended to apply prospectively to all sensitive materials presently in use within the agency. Any retrospective application of the procedures and processes contained in this Handbook should be undertaken on a case-by-case basis under the direction of the Corporate Information Security Officer in consultation with the Law Department and with the concurrence of the Corporate Security Officer.

This Handbook will be amended and updated from time to time as may be appropriate. When appropriate, each Port Authority department, office and/or business unit, as well as contractors/consultants, should create a "Confidential Information Practices and Procedures" ("CIPP") document with additional guidelines for their respective businesses. This will assist staff, and third parties working with the Port Authority, in carrying out the requirements of this Handbook. A CIPP should augment, but may not deviate from, the requirements of this Handbook. The procedures, safeguards and requirements of this Handbook fully apply to all subsidiaries of the Port Authority that deal with, or create, Confidential Information. Whenever the term Port Authority is referenced in this Handbook, it should be understood to include and/or cover its subsidiary entities.

The Port Authority expressly reserves the right to reject any information designation and/or to remove/add any and all markings on information that is not consistent with this Handbook.

CHAPTER 1 - PORT AUTHORITY INFORMATION SECURITY ORGANIZATIONAL STRUCTURE

The Port Authority organizational structure for information security is as follows:

Corporate Security Officer (CSO) – is responsible for the implementation of Port Authority policy on security matters, both physical and informational, and for the coordination of security initiatives throughout the agency in order to assure consistency in practices, procedures and processes. In particular, the CSO works in close collaboration with the Chief Technology Officer and the Corporate Information Security Officer with regard to their respective areas of security responsibilities. The CSO acts as the Port Authority's principal liaison on security related matters with governmental, public and private entities. The CSO works closely with the Law Department, Public Safety Department and the Office of Inspector General on security initiatives, on compliance with governmental requirements on security matters, and on issues relating to compliance with the Port Authority's security policy. The CSO reports to the Chief Operating Officer of the Port Authority.

Corporate Information Security Officer (CISO) – the Office of the Secretary of the Port Authority will be designated to undertake the role and functions of the CISO and consults with the CSO in order to assure agency wide consistency on policy implementation. The CISO is responsible for the management, oversight and guidance of the Policy. The CISO works in conjunction with all appropriate Port Authority departments and subsidiaries to: (i) formulate practices and procedures concerning information security management issues affecting the Port Authority, its operations and facilities; (ii) review, categorize and manage all Port Authority information consistent with the Port Authority's policy and procedures under its Freedom of Information Policy; and (iii) establish procedures and handling requirements for Port Authority information based upon its sensitivity designation in order to ensure that the information is used solely for authorized purposes. The CISO will report to the Secretary who in turn reports to the Executive Director.

Departmental Information Security Officer (DISO) - each department head, and, where appropriate, office head, will designate a staff member to act as DISO in order to ensure compliance with the Policy. The DISO is responsible for management and oversight of information security issues for departmental operations and reports to the CISO on information security practices and procedures, or issues relating thereto. Additionally, the DISO may perform the Security Information Manager (SIM) functions, if a SIM has not been designated for a department, division, office, unit or project. Each DISO is also responsible for compiling an inventory of all Confidential Privileged Information and Confidential Information in their department's possession and/or providing updated listings to the CISO on a monthly basis, or on such other periodic basis as may be established by the CISO. Additionally, the DISO is responsible for approving the departmental Confidential Information Practices and Procedures ("CIPP") document and, before authorizing its use, for submitting the CIPP to the CISO for final approval and providing periodic reports to the CISO, as the CISO may require.

Security Information Manager (SIM) – Port Authority departments, offices or other business units, as well as contractors, vendors, and consultants, individuals and/or entities, where appropriate, who are involved with, or who could have exposure to, Confidential Information shall designate a SIM who is responsible for coordinating the implementation and daily oversight of the Policy for the particular Port Authority department, office, business unit, or third-

party contractor, vendor, or other party. The SIM reports to the DISO and/or the Security Project Manager (SPM) for a project, where applicable. If a Port Authority department determines that the SIM function may be carried out by the DISO, then the SIM designation may not be required, unless or until the DISO, in consultation with the CISO, determines otherwise. The functions of the SIM are further described throughout this Handbook.

Security Project Manager (SPM) – where applicable, a DISO may designate an individual overseeing a project for a department as the SPM, who will be responsible for securing information and ensuring compliance with the Policy on the particular project.

Chief Technology Officer (CTO) – is the head of the Technology Services Department. The CTO, or the CTO's designee, works with the CSO and the CISO to coordinate the Policy efforts and to provide the Port Authority with the most current resources needed to comply with legislative and regulatory requirements, to adhere to industry standards and best business practices and procedures, and to identify and address technology issues that may affect the current and future policy. The CTO is also responsible for providing technical support and training to assist staff and to meet information security management goals.

Office of Inspector General (OIG) – The OIG's responsibilities include: conducting criminal and administrative investigations of possible misconduct by Port Authority officers and employees, as well as third parties doing business with the Port Authority; reviewing agency internal controls and management practices for weaknesses that could allow losses from corruption, incompetence and/or bad decision making; making recommendations for cost effective improvements; serving as the confidential investigative arm for the Port Authority's Ethics Board; conducting educational awareness programs for all Port Authority employees pertaining to integrity and ethics; and, where appropriate, conducting background investigations of certain contractors proposing to do business with the Port Authority.

Information Security Subcommittee (ISSC), chaired by the CISO, includes departmental representatives from line departments (who might also be functioning as a DISO), the Law and Public Safety Departments, the Office of Inspector General and the CTO. The ISSC assesses the Policy needs and the effectiveness of the policy's implementation, as well as evaluating initiatives for its further development and refinement.

CHAPTER 2 - CATEGORIZATION OF INFORMATION

2.1 Definitions

For purposes of this Handbook the following definitions shall apply:

(a) "**Confidential Information**" means and includes collectively, Confidential Proprietary Information, Confidential Privileged Information, and Information that is labeled, marked or otherwise identified by or on behalf of the Port Authority so as to reasonably connote that such information is confidential, privileged, sensitive or proprietary in nature. The term Confidential Information shall also include all work product that contains or is derived from any of the foregoing, whether in whole or in part, regardless of whether prepared by the Port Authority or a third-party, or when the Port Authority receives such information from others and agrees to treat such information as Confidential.

(b) "**Confidential Privileged Information**" means and includes collectively, (i) any and all Information, documents and materials entitled to protection as a public interest privilege under New York State law and as may be deemed to be afforded or entitled to the protection of any other privilege recognized under New York and/or New Jersey state laws or Federal laws, (ii) Critical Infrastructure Information, (iii) Sensitive Security Information, and (iv) Limited Access Safety and Security Information.

(c) "**Confidential Proprietary Information**" means and includes information that contains sensitive financial, commercial or other proprietary business information concerning or relating to the Port Authority, its projects, operations or facilities that would be exempt from release under the Port Authority Freedom of Information Policy. It also includes sensitive financial, commercial and other business information received from third parties under Non-Disclosure and Confidential Agreements.

(d) "**Critical Infrastructure Information**" (CII) has the meaning set forth in the Homeland Security Act of 2002, under the subtitle Critical Infrastructure Information Act of 2002 (6 U.S.C. §131-134), and any rules or regulations enacted pursuant thereto, including, without limitation, the Office of the Secretary, Department of Homeland Security Rules and Regulations, 6 C.F.R. Part 29 and any amendments thereto. CII may also be referred to as "Protected Critical Infrastructure Information" or "PCII," as provided for in the referenced rules and regulations and any amendments thereto.

(e) "**Information**" means, collectively, all information, documents, data, reports, notes, studies, projections, records, manuals, graphs, electronic files, computer generated data or information, drawings, charts, tables, diagrams, photographs, and other media or renderings containing or otherwise incorporating information that may be provided or made accessible at any time, whether in writing, orally, visually, photographically, electronically or in any other form or medium, including, without limitation, any and all copies, duplicates or extracts of the foregoing.

(f) **"Limited Access Safety and Security Information"** means and includes sensitive information, the disclosure of which would be detrimental to the public interest and might compromise public safety and/or security as it relates to Port Authority property, facilities, systems and operations, and which has not otherwise been submitted for classification or designation under any Federal laws or regulations.

(g) **"Non-Disclosure and Confidentiality Agreement"** (NDA) refers to the Agreements attached hereto as Appendix "A" (which include Appendices A-1 through A-3). When approved by the Law Department, other forms of a NDA may be used for special situations or specific projects, however, a general NDA may be used in retaining consultants and contractors where the retainer involves work on various projects.

(h) **"Non-Disclosure Instructions"** (NDI) refers to the instructions attached hereto as Appendix "B." A NDI is used when represented staff are given or have responsibilities, which involve working on sensitive and/or security related matters, and/or when such staff is being given access to Confidential Information. The NDI is given to each individual before starting such work or on being given such access. The CISO, in consultation with the Law Department, may allow the use of NDI's in other circumstances, as may be appropriate.

(i) **"Sensitive Security Information"** (SSI) has the definition and requirements set forth in the Transportation Security Administrative Rules & Regulations, 49 CFR 1520, (49 U.S.C. §114) and in the Office of the Secretary of Transportation Rules & Regulations, 49 CFR 15, (49 U.S.C. §40119) and any amendments thereto.

2.2 General Process for Categorization

As defined hereinabove, the term Confidential Information includes all Port Authority Information protected pursuant to this Handbook. Although Confidential Privileged Information is a sub-category of Confidential Information, it is considered a separate category for Port Authority categorization, marking, and handling purposes due to its heightened level of sensitivity. Any sensitive Information not specifically deemed Confidential Privileged Information should be categorized as Confidential Information. In addition, certain other types of Confidential Information, such as SSI and CII, are treated separately and distinctly because they are governed by specific federal designations and must be marked and handled in accordance with federal regulations or requirements. The requirements in this Handbook apply to all Confidential Information, unless otherwise specified. Where a different or additional requirement applies to a specific sub-category of Confidential Information, it will be noted. Although the requirements of this Handbook shall apply prospectively upon its implementation, each Port Authority department, division or unit shall conduct an initial review and designation of all documents currently in use.

For purposes of this Handbook, Confidential Information shall be designated as one of two categories: (i) Confidential Information, or (ii) Confidential Privileged Information.

Each DISO, in consultation with the CISO, shall create a list of examples of Confidential Information and Confidential Privileged Information to be used as a guide by the departmental staff. This list may be included in the department's CIPP. Any employee, consultant, third-party contractor or other agency personnel may nominate Information for categorization in either of the two categories. The DISO, SPM, SIM, supervisors, managers or the CISO, as may be appropriate, should take the action needed to process the Confidential Information under their control and to review it as soon as possible. It is important to understand that not every piece of material currently held should be reviewed. The review should only be of Information that is

considered potential Confidential Information. If management, employees, consultants, third-party contractors, or other agency personnel determine that Information under review contains Confidential Information, the Confidential Information should be designated with the appropriate categorization.

In order to categorize Information as Confidential Privileged Information or Confidential Information the following steps must take place:

1. Inform the SPM or SIM, where applicable, and the unit supervisor of the group/entity proposing the categorization.
2. Obtain DISO concurrence and approval.
3. Obtain CISO final approval.
4. If approved, mark and label the information, and, if appropriate, apply a cover sheet (See Appendix E).

If Information has been nominated for categorization, a final decision on the nomination shall be made within one week of its submission. During the time period between the submission and a determination regarding the categorization, the nominated Information should not be reviewed, released or distributed to any individuals, other than those individuals who possess a need to know and are currently familiar with the Information, or were previously provided access to other Confidential Information for the same project or task.

2.3 Training and Information Review

Initially, Port Authority managers, including, but not limited to, the DISO, SPM and the SIM will complete training. This will enable them to conduct an initial review of Confidential Information under their control in order to identify and categorize it as Confidential Information or Confidential Privileged Information. Thereafter, employees, consultants, third-party contractors or other agency personnel will participate in and complete the training, which will enable them to continue the process of review, identification, and categorization of Confidential Information.

This phased approach provides an initial review of Confidential Information by management and a continuing review of Confidential Information thereafter. More specifically, this approach consists of four phases as set forth below:

- Phase 1 - Conduct department manager, DISO, SPM, and SIM, training.
- Phase 2 - Direct department managers, DISO, SPM, SIM to review and categorize the Confidential Information under their control into the designated information security categories.
- Phase 3 - Conduct employee, consultant, third-party contractor, and other agency personnel training.
- Phase 4 - Direct employees, consultants, third-party contractors, or others to commence/continue the process.

The basis for this phased approach is the orderly and timely completion of the Information Security Education and Awareness Training program for the appropriate individuals (See

Chapter 7). Each Department Director will determine which staff members in the respective department require training and will do so on an ongoing basis. When access to Confidential Information is given to third parties, a training requirement may also be a condition for granting access privileges.

2.4 Removal of Category Designation

At some point, Confidential Information may no longer be considered Confidential and should therefore have its designation removed or eliminated. This may occur as a result of any number of circumstances, including changes within the Policy, the changing nature of information security, a better understanding of particular material, and/or changes in public policy or law, among others. In order to determine whether category designations should be removed from particular materials, the CISO may establish criteria for the periodic review of all sensitive material. In any case, the category designation of any particular Confidential Information may not be removed without the approval of the CISO. A record of any removal of categorization for particular information must be kept by the DISO, with a copy provided to the CISO.

CHAPTER 3 – INFORMATION ACCESS

3.1 Applicability

Each employee, consultant, third-party contractor, tenant, individual and/or entity requiring, or requesting, access to Port Authority Confidential Information must adhere to the requirements set forth in this Handbook.[1] Confidential Information is intended for official business use only. Failure to abide by the procedures set forth in the Handbook can lead to a denial of access privileges to Confidential Information and/or other contractual, civil, administrative or criminal action.

All employees, consultants, third-party contractors, individuals and/or entities given access privileges to Confidential Information are responsible for overseeing the safeguarding and protection of Confidential Information in their possession or under their control as per this Handbook's requirements. Questions concerning the safeguarding, protection, release, and/or access to Confidential Information should immediately be brought to the attention of the CISO, DISO, SPM, or SIM, as may be appropriate, in the particular circumstance.

3.2 General Criteria

In order for access to Confidential Information to be considered for approval, all individuals including PA staff, must meet and complete the following criteria:

- Be a citizen of the United States of America, or be an alien who has been lawfully admitted for permanent residency or employment (indicated by immigration status), as evidenced by Immigration and Naturalization Service documentation, or be a national of the United States as defined by the Immigration and Nationality Act. This requirement may be waived by the CISO with the concurrence of the Director of Public Safety and/or the CSO where and when circumstances so require.
- Obtain sponsorship for a request to be given access to Confidential Information through the individual's assigned chief, director, manager, or supervisor. The written request must include justification for access, level of access required, and indicate the duration for which access privileges are required.
- Forward the request through the individual's supervisory chain to the CISO, via the appropriate DISO, SPM, or SIM, requesting that a specific background check be undertaken, where appropriate and/or required.
- Complete the Port Authority Information Security Education and Awareness Training.
- Execute a Port Authority NDA (See Appendix A), or an Acknowledgement of an existing executed NDA, or, if the individual is Port Authority represented staff, have been provided with the NDI. This requirement may be waived if approved by the CISO.

---

[1] The CISO in consultation with the Law Department may modify and/or waive the condition of complying with the requirements of the Handbook where such compliance is impractical, such as in the case of a governmental entity having its own information security procedures and/or protocols governing the handling and protection of sensitive information. In addition, certain sensitive information is required to be submitted to other governmental entities under applicable laws, rules or regulations, or the Port Authority may elect to submit Confidential Information to a governmental entity, such as in the case of the CII process, wherein it may elect to submit Confidential Information to the Department of Homeland Security in order to secure the protection of the CII regulatory scheme.

- Be granted final approval of the security clearance level, in writing, by the CISO who verifies that all requirements have been met.

The individual's name must be entered on the appropriate department, project, or company Authorized Personnel Clearance List. See Sec. 3.9 for more information regarding this List (Note: If an individual's name does not appear on the appropriate Authorized Personnel Clearance List, access must be denied).

Individuals who meet and complete the criteria listed above are neither guaranteed, nor automatically granted, access to Confidential Information, since access is conditioned on need to know criteria. The OIG may access, without approval of the CISO, DISO, SPM or SIM, all Confidential Information when it is needed in connection with an OIG investigation, audit or inspection work, or any other Port Authority related work, subject to the handling requirements set forth in this Handbook.

3.3 Information Access Controls

Access to all Confidential Information falling within any of the Port Authority Information categories shall be undertaken in a manner that complies with and maintains all applicable state, federal and common law protections. Access to particular Information must be conditioned upon a strict need to know basis with regard to the particular, discrete Information, regardless of any federal security clearance, or other Port Authority or other organizational information access authorization. An individual's need to know is not established simply by reason of the individual possessing a recognized federal security clearance, including one that allows for access to a higher level of classified information than is otherwise required for the discrete Port Authority Information to which access is sought. All requests for access to SSI by anyone who does not possess the requisite "need to know" under SSI regulations must be reported to the Transportation Security Administration ("TSA") or, if applicable, the United States Coast Guard ("USCG") and, in certain instances, the Department of Transportation ("DOT").

(a) Confidential Information

Access to Confidential Information shall be on a need to know basis only, as determined by the DISO. In certain instances access privileges may be conditioned on the satisfactory completion of a background investigation(s). The background investigation should utilize the least stringent criminal history access disqualification criteria that is appropriate for granting access to the particular information for both Port Authority and non-Port Authority employees. Where a background investigation is a condition to granting access, a DISO may determine that periodic updates of such investigations are required as a condition to maintaining continued access privileges. Access by third parties to Confidential Information may require that the parties execution a NDA or an Acknowledgment of an existing NDA if the CISO determines that a NDA and/or Acknowledgment is required.

(b) <u>Confidential Privileged Information</u>

Individuals requiring access to Confidential Privileged Information must have a need to know consistent with the creation and preservation of the privilege attaching to the particular Information. An individual will be given access privileges to the Information only to the extent

that it is necessary and/or is required by the individual in order to fulfill and/or carry out his/her duties, obligations and responsibilities to the Port Authority. Access to Confidential Privileged information may be subject to the satisfactory completion of periodic background investigations for both Port Authority and non-Port Authority employees. A list of disqualifying crimes for the different levels of background screening is attached as Appendix "C." A more stringent background investigation may be required of the individual for access to certain Confidential Privileged Information if determined by the CISO. All access to such Information must be granted and received in a manner that does not compromise or abrogate the particular privilege attaching to the Information.

Confidential Privileged Information may not be disclosed to any individual without appropriate prior approvals. Approval for disclosure of Confidential Privileged Information to third parties must be obtained from the CISO. A Port Authority employee or other individual may not waive any privilege attaching to Port Authority Information without the Port Authority's express permission as granted by the CISO, unless the Information to which the Port Authority asserts a privilege is personal to a particular employee or individual and the privilege is directly derived by reason of that circumstance. Access by third parties to Confidential Privileged Information will be conditioned on the parties' execution of a NDA or an Acknowledgment of an existing executed NDA, as may be appropriate and determined by the CISO. In certain circumstances, a Memorandum of Understanding or Memorandum of Agreement containing approved non-disclosure and confidentiality requirements may be utilized, in which cases approvals are required from the CISO and the General Counsel, or their respective designees. In the case of certain represented employees/individuals, NDIs may be utilized in lieu of NDAs.

3.4 Access Disqualification

Any employee, consultant, third-party contractor, or other individual and/or entity, who has been granted access to Confidential Information, may be temporarily denied access while an investigation is conducted regarding any report to the CISO, OIG and the DISO that such individual misused, mishandled, or lost Confidential Information, or disclosed, disseminated, or released Confidential Information to an unauthorized individual or entity. Further, access to Confidential Information can be denied when improper or incomplete verification checks of employees, entities, or individuals are discovered. Where it is determined that an individual has misused, mishandled or otherwise improperly disclosed, released or disseminated Confidential Information without authorization, that individual may be subject to disqualification of access privileges and may also be subject to sanctions, including formal disciplinary actions where the individual is a PA employee, with possible penalties up to and including termination of employment. The foregoing action shall be documented and provided to the individual's employer, SPM, DISO, or departmental manager and the CISO, as may be appropriate. In the case of third parties, remedial action may include, but is not limited to, imposition of a monitor to oversee compliance with information security and general security requirements, or possible disqualification, and/or termination of present and/or future business relationships. Individuals and entities may also be subject to criminal or civil legal action, as may be appropriate. Additionally, see Chapter 6 regarding the possible consequences of violations of this Policy.

3.5 Non-Disclosure and Confidentiality Agreements (NDAs)

Employees, consultants, third-party contractors, tenants, or other individual or entities, including governmental agencies where appropriate, will be required to sign NDAs or an Acknowledgment of an existing NDA, or be subject to an NDI, as a condition of being granted access to Confidential Privileged Information and, where appropriate, Confidential Information. Employees, consultants, third-party contractors, or other agency personnel who refuse to sign a NDA, in situations where it is required, will be denied access to Confidential Information, except in the case of certain employees and third parties where a NDI may be utilized in instructing and advising the employee and/or third party of the obligations and the requirements for handling Confidential Information. The DISO is responsible for determining whether a NDA/NDI is required as a condition to being granted access privileges to Confidential Information, other than Confidential Privileged Information. If an individual refuses to execute an individual Acknowledgment, or to receive the NDI, access to the Confidential Information is to be denied. The SIM is also responsible for keeping proper documentation for employees and individuals subject to NDIs, including the date when the individual was given the NDI and by whom. A copy of all executed agreements and acknowledgements are to be provided to the SIM. Original executed NDAs shall be forwarded to the CISO for filing in the official Port Authority records repository.

3.6 Unauthorized Disclosure of Information

If employees, consultants, third-party contractors, or other individuals and/or entities with authorized access to Confidential Information become aware that Confidential Information has been released to unauthorized persons, they are required to immediately notify the CISO, the Office of Inspector General, and any other appropriate information security officer and report the discovery. In the case of SSI, the CISO must inform the TSA, DOT, or USCG and, in the case of CII, the Department of Homeland Security ("DHS"), of the breach of security. DOT, DHS, TSA and USCG rules govern the reporting of any unauthorized disclosure.

3.7 Security Clearance and Access Prohibitions

Access to Confidential Information is not a right, privilege, or benefit of employment by the Port Authority, rather it is based on pre-established guidance. Confidential Information should not be divulged, released, turned over, or provided to any individual in any organization who does not meet the established criteria or conditions set forth herein, or who has not been approved for a security clearance issued by the Port Authority CISO. The following security clearance and access guidelines and/or prohibitions are in effect to protect Confidential Information:

- Confidential Information shall only be used in the performance of required job responsibilities, or in order to complete assigned tasks as determined by the SIM and DISO, with the concurrence of the CISO. No other disclosure or use of Confidential Information is authorized.
- Individual access to Confidential Information will be rescinded when an employee, consultant, third-party contractor, individual or entity, who had been granted access to Confidential Information, is no longer employed by the Port Authority, or is no longer under contract with, or no longer has a relationship with the Port Authority, or is no longer in a position that requires access to Confidential Information in order for the individual or entity to perform duties or complete tasks/projects.

- Employees may not unilaterally sponsor themselves for background verification or enter their name on an Authorized Personnel Clearance List.
- Group access of organizations to Confidential Information should be prohibited. Each individual in a group must have security clearance to access Confidential Information.
- Persons who rarely, if ever, require access to Confidential Information, (i.e., maintenance, food service, cleaning personnel, vendors and other commercial sales, or service personnel, who perform non-sensitive duties), should not be approved for a security clearance.

3.8 Background Screening

All background checks for third parties required under the Policy should normally be conducted through the "Secure Worker Access Consortium" (S.W.A.C.), which is presently the only Port Authority approved service provider of a background screening checks, except as otherwise required by federal law and or regulation. The Office of Emergency Management administers this provider. S.W.A.C. is accessed by an online application (http://www.secureworker.com) that enables the secure collection, processing, maintenance and real-time positive identity verification (PIV) of individuals. The S.W.A.C. background check is not a replacement for any federal agency (DHS, TSA, etc.) required background screening. S.W.A.C. membership is valid for one year, at the end of which the member must renew his online application. In addition, certain employees, such as those in the Public Safety Department, will have their criminal history background checked through the electronic databases maintained by federal and/or state law enforcement agencies when required as a condition of employment, or when required by federal or state laws, rules, and/or regulations, or, in certain cases, where it is legally permitted and is deemed appropriate by the CSO.

The SIM/SPM has authority to obtain the background check information from S.W.A.C. Additional information about S.W.A.C., corporate enrollment and online applications can be found at http://www.secureworker.com, or it may be contacted at (877) 522-7922. The S.W.A.C. application process is described in Appendix "D."

3.9 Authorized Personnel Clearance List

The CISO will maintain a master list database containing the names of all employees, consultants, third-party contractors, and other individuals and/or entities that have been granted a Port Authority security clearance and the specific category for which the security clearance was received, including, but limited to, for a particular project, or for specific Confidential Information. The DISO, SPM, and SIM are responsible for compiling, maintaining, and updating their respective list databases on an ongoing basis and forwarding the information to the CISO for compilation into a master listing. Each DISO shall periodically review its department's/business unit's list with its SPM and/or SIM to ensure that the list is current and that each individual's access to Confidential Information is still required.

3.10 Development of a Confidential Information Practices and Procedures (CIPP)

Departments, offices and/or business units may adopt an individualized, discrete CIPP tailored to their respective particular business practices for handling Confidential Information. The CIPP is meant to augment the Handbook and must be consistent with it. Each CIPP must be approved by the CISO before being implemented.

3.11 Procurement Strategies

(a) General

As a public agency, the Port Authority has an established procurement process based on openness, integrity, and fairness to the vendor community. The security of Confidential Information must be incorporated at the beginning of the procurement process in order to establish a security benchmark that may be applied throughout the procurement process, as well as during the term of the award/contract.

(b) Lifecycle Phases and Procurements

A project may contain Confidential Information in one or more of its lifecycle phases (pre-award, award, design, construction, close-out, or maintenance/service operation contracts, etc.).

Procurement and lifecycle information should be thoroughly reviewed by the originator before being submitted to the Procurement Department for processing. If Confidential Information is discovered thereafter by Procurement, or any reviewing department, the originator's department manager or designee should be contacted immediately to retrieve the Confidential Information and process it in accordance with the Policy and this Handbook.

(c) Risk Exposure and Business Risk Strategy

Procurement shall develop and retain, by project, a current listing of pre-screened persons or pre-qualified firms to bid on sensitive projects who agree to abide by the Policy requirements. Requirements must be included in procurement documents in order to help reduce potential disclosure of Confidential Information and to provide bidders with certain security requirements in advance. They must also be included in contract awards to ensure information protection practices, procedures, and protocols are included in each project's lifecycle phase. The typical requirements are:

(i) Non-Disclosure and Confidentiality Agreements (NDA). Require prospective consultants, prime vendors, or commercial enterprises to enter into a NDA with the Port Authority before obtaining a copy of a RFP. NDAs should be project and procurement specific and should be completed in a timely manner for specific types of procurements or projects. A broad or generic NDA should not normally be utilized to cover all procurements and projects under contract to a particular vendor over a long period of time, however, it may be appropriate in certain situations to utilize such a NDA, if approved by the DISO with the concurrence of the CISO. Vendors should contact the Port Authority to request authority to release the information prior to releasing RFP information to a sub-contractor. The sub-contractor may have to execute an Acknowledgement that it will comply with the terms of any NDA that the successful bidder has executed.

(ii) Background Screening. Require potential users seeking access to Confidential Information to undergo background pre-screening. The pre-screening may parallel the screening requirement used by the Port Authority to grant access to Confidential Information under Section 3.3. S.W.A.C.'s background screening is usually finalized within five to ten business days.

(iii) Designation of a Security Information Manager (SIM). Require companies involved in Confidential Information procurements or projects to designate a SIM to ensure information security and Confidential Information requirements are followed. A second employee may be designated as an alternate SIM.

(iv) Information Security Education and Awareness Training. Require consultants, vendors, contractors and commercial enterprises to attend training to ensure security awareness regarding Port Authority information.

(v) Physical Security. Outline the specific guidelines and requirements for the handling of Confidential Information to ensure that the storage and protection of Confidential Information is consistent with the requirements of Chapter 4 of this Handbook.

(vi) Transfer or Shipping Sensitive Information. Prohibit or place restrictions on the transfer, shipping, and mailing of Confidential Information consistent with the handling procedures set forth in Chapter 4 of this Handbook.

(vii) Website Restrictions. Prohibit posting, modifying, copying, reproducing, republishing, uploading, transmitting, or distributing Confidential Information on websites or web pages. This may also include restricting persons, who either have not passed a pre-screening background check, or who have not been granted access to Confidential Information, from viewing such information.

(viii) Destruction of Documents. Require Confidential Information to be destroyed using certain methods, measures or technology consistent with the requirements set forth in Chapter 4 of this Handbook.

(ix) Use of Similar Agreements Between Prime Vendor and Subcontractors. Require the prime vendor or general contractor to mandate that each of its subcontractors maintain the same levels of security required of the prime vendor or general contractor under any Port Authority awarded contract.

(x) Publication Exchanges. Prohibit the publication, exchange or dissemination of Confidential Information developed from the project or contained in reports, except between vendors and subcontractors, without prior approval of the Port Authority. Requests for approval should be routed to and reviewed by the CISO in conjunction with the Law Department and, where appropriate, Public Affairs.

(xi) Information Technology. Matters involving information technology policy, or use of particular hardware or software, should require the application of specific protocols and/or software tools to support Port Authority projects. Coordination of information technology and consultation with the CTO and the CISO may be required for the success of particular projects.

(xii) Audit. Include provisions to allow the Port Authority to conduct audits for compliance with Confidential Information procedures, protocols and practices, which may include, but not be limited to, verification of background check status, confirmation of completion of specified training, and/or a site visit to view material storage locations and protocols.

(xiii) Notification of Security Requirements. Advise all consultants, third-party contractors, and other individuals and/or entities, as may be appropriate, that Port Authority security procedure requirements may be imposed throughout the duration of the project.

(xiv) Reproduction/Copies. Reproductions of Confidential Information shall be consistent with the requirements of Chapter 4 of this Handbook.

CHAPTER 4 – MARKING, HANDLING, STORAGE, TRANSMITTAL AND DESTRUCTION REQUIREMENTS

4.1 Marking of Confidential Information

(a) Confidential Privileged Information and Confidential Information

All documents, drawings, and all other Information that contain Confidential Privileged Information or Confidential Information must be marked with the appropriate respective protective marking: "CONFIDENTIAL PRIVILEGED" (alternatively "CONFIDENTIAL AND PRIVILEGED") or "CONFIDENTIAL" (alternatively, where appropriate, Confidential Proprietary Information). The markings must be conspicuous and in bolded Arial with a 16 point font size. All copies of Confidential Information, Confidential Privileged Information, Sensitive Security Information, and Critical Infrastructure Information documents shall also bear the required markings and warnings.

The front page (or front and back cover, if appropriate) shall be marked at the top and bottom of the page. In addition, all interior pages within the document must also be marked at the top and the bottom of the page. Sets of documents large enough to be folded or rolled must be marked or stamped so that the marking is visible on the outside of the set when it is rolled or folded. The marking must be visible from the exterior container of the material, e.g., the spine of a binder, or compact disc container or cover.

All Confidential Privileged Information and Confidential Information must bear the following warning sign on its front cover, back cover, and title sheet or first page. For compact discs, DVDs or other smaller materials, the warning sign may be printed on an adhesive label and affixed to the material. It should be in 8-point font size and state:

> "WARNING": The attached is the property of The Port Authority of New York and New Jersey (PANYNJ). It contains information requiring protection against unauthorized disclosure. The information contained in the attached document cannot be released to the public or other personnel who do not have a valid need to know without prior written approval of an authorized PANYNJ official. The attached document must be controlled, stored, handled, transmitted, distributed and disposed of according to PANYNJ Information Security Policy. Further reproduction and/or distribution outside of the PANYNJ are prohibited without the express written approval of the PANYNJ.
>
> At a minimum, the attached will be disseminated only on a need to know basis and, when unattended, will be stored in a locked cabinet or area offering sufficient protection against theft, compromise, inadvertent access and unauthorized disclosure.

(b) Sensitive Security Information Requirements

Pursuant to the federal regulations governing SSI, Port Authority Confidential Privileged Information that has been designated SSI by the Federal government must be conspicuously marked with its respective protective marking "SENSITIVE SECURITY INFORMATION" on the top and the distribution limitation statement on the bottom of each page of the document

including, if applicable, the front and back covers, the title page, and on any binder cover or folder. The protective marking must be in bolded Arial 16-point font size and the distribution limitation statement must be in an 8-point font size. All copies of SSI documents must also bear the required markings.

The distribution limitation statement is:

> WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the TSA or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

(c) Critical Infrastructure Information

Pursuant to the federal regulations governing CII, Port Authority Confidential Privileged Information that has been marked PCII by the Department of Homeland Security PCII Program Manager or the manager's designee will be marked as follows:

> This document contains PCII. In accordance with the provisions of 6 CFR Part 29, this document is exempt from release under the Freedom of Information Act (5 U.S.C. 552 (b)(3)) and similar laws requiring public disclosure. Unauthorized release may result in criminal and administrative penalties. This document is to be safeguarded and disseminated in accordance with the CII Act and the PCII Program requirements.

(d) Document Control Number for Confidential Privileged Information

Documents that have been identified as Confidential Privileged Information will be given a control number, which shall consist of the category of information followed by an acronym for the transmitting department, followed by the last 2 digits of the year, followed by a number that is sequential and, finally, followed by the copy number.

Examples:

C&P – LAW – 05 – 1 – 1

C&P – PMD – 07 – 10 – 2

The front page (or front and back cover, if appropriate) and all pages of Confidential Privileged Information shall be marked with the control number. The control number must also be visible from the exterior container of the material, e.g., the spine of a binder, or compact disc container or cover.

4.2 Handling Confidential Information

Handling refers to the physical possession of, and includes working on or with, Confidential Information to perform job duties or complete tasks or projects. This includes, but is not limited to, reading, copying, editing, creating, or correcting the material. Confidential Information in any form, including physical or electronic, must be under constant surveillance by an authorized individual to prevent it from being viewed by, or being obtained by, unauthorized persons. Confidential Information is considered to be in use when it is not stored in an approved security container.

The following is a chart of the minimum-security requirements for handling Confidential Information, and certain requirements that apply only to Confidential Privileged Information:

Minimum Security Requirements for Handling	**Confidential Privileged Information**	**Confidential Information**
Must never be left unattended outside of storage location.	X	
Must be under the direct and constant supervision of an authorized person who is responsible for protecting the information from unauthorized disclosure.	X	
Must be turned face down or covered when an unauthorized person is in the vicinity. Be cognizant of others in area that can view your computer screen.	X	X
When leaving a computer unattended ensure that the screen is locked.	X	
Attach an information cover sheet when removing materials from their place of storage.	X	
Use all means to prevent unauthorized public disclosure of information.	X	X

4.3 Transmittal of Confidential Information

Transmission refers to the sharing among individuals and/or entities, and/or the transfer or movement of Confidential Information from one location to another using either physical or electronic means. The following chart sets forth the methods by which Confidential Information should be transmitted. In all instances, Confidential Information must at all times be safeguarded and transmitted in a manner and method designed to insure that it is not disclosed, or otherwise compromised, and it should be appropriately marked with the proper identifying marking.

In general, all Confidential Privileged Information must be signed in and out, and, in certain situations as determined by the SIM or SPM, Confidential Information may be signed in and out as well. A cover sheet must be attached to the Confidential Privileged or, in certain situations as determined by the SIM, to Confidential Information and it should be marked appropriately. With respect to Confidential Privileged Information, the coversheet attached as Appendix "E" is to be utilized to draw emphasis to the fact that a document contains Confidential Privileged Information and to limit visual exposure to unauthorized individuals in near proximity. Confidential Privileged Information and, where appropriate, Confidential Information, must be wrapped and sealed. The exterior of the wrapping should not indicate that it is sensitive material, or its category, or level. Confidential Information transmitted by email must state at the top of the email in bold uppercase letters "CONFIDENTIAL INFORMATION."

Confidential Privileged Information may be transported using public modes of transportation, and a courier service may also be utilized; provided, however, that the sign in and sign out procedures will apply, as well as wrapping and sealing procedures. All packages must be sealed in a manner that easily identifies whether the package has been opened prior to delivery to the intended recipient. The use of a double wrapped/enveloped package or a tamper resistant envelope must be used to fulfill this requirement. Protective markings are not to be placed on the outer visible envelope. If using a double wrapped package or two envelopes, the inner wrapping or envelope should be marked in accordance with appropriate category designation. The package must be addressed to an individual who is authorized to receive it or, preferably, to the SIM. All packages must contain a specific individual's name on the shipping label. Where appropriate any of the foregoing requirements may also be required in handling Confidential Information and can be provided for generally in the department's CIPP, or as required by the DISO and/or SIM with respect to handling such information in specific instances.

Minimum Security Requirements for Transmission	**Confidential Privileged Information**	**Confidential Information**
Verbally at a meeting, conference or briefing where all attendees have the appropriate security clearance	X	X
Electronic Systems: restrict to the Livelink[2] network or a similar secure repository	X	
Electronic Mail: restricted from using e-mail accounts to transmit unless expressly permitted by the SIM in writing	X	
Hand Carried or delivered in the personal custody of Port Authority employee: (a) request return receipt (b) place in sealed envelope, and (c) name of recipient, department, address and phone number must be written on face of envelope	X	
Approved Commercial Delivery Service (e.g., DHL, FedEx, UPS): (a) request return receipt, (b) verify recipient name and mailing address, (c) place in a sealed envelope, and (d) the exterior of a		

[2] Livelink is a secure repository for the records of a project.

mailing document shall not indicate the security category of the material contained therein	X	X
Use of USPS Certified Mail: (a) request return receipt, (b) verify recipient name and mailing address, and (c) the exterior of a mailing document shall not indicate the security category of the material contained therein	X	X
Intra-agency Mail System (a) request return receipt (b) place in sealed envelope, (c) name of recipient, department, address and phone number must be written on face of envelope, and (d) the exterior of a mailing document shall not indicate the security category of the material contained therein	X	X (b, c, d only)
Telephone: restricted from using a telephone to transmit, unless expressly permitted by SIM in writing. If approved: (a) use all means to prevent unauthorized public disclosure, and (b) may not use cell phone	X	
Fax Machine: restricted from using fax machine to transmit unless expressly permitted by the SIM in writing. If approved: (a) prior coordination with recipient required, (b) verify recipient fax number, (c) receipt of successful transmission, and (d) follow-up contact required	X	X(a,b,c only)

Steps for transmittal of a "hard copy" of all Confidential Privileged Information and, when required, for Confidential Information:

Step 1. Make certain that documents are properly marked: "CONFIDENTIAL PRIVILEGED" or "CONFIDENTIAL," according to its designated category.

Step 2. Prepare Transmittal Receipt (Appendix "F").

Step 3. Place document in envelope with the Transmittal Receipt, seal envelope, mark the inner envelope CONFIDENTIAL PRIVILEGED or CONFIDENTIAL, place envelope in second envelope (outer), this envelope shall not contain any protective markings.

Step 4. Address envelope to an individual who is authorized to receive it.

Step 5. Mail document.

Step 6. The Transmittal Receipt shall be returned to the party who initially sent the item.

When hard copies of 8 1/2 " X 11" multi-page documents include threat scenarios, asset criticality information, identification of security vulnerability details, risk assessments, design

basis threats and concepts of operations are distributed, this information is to be bound using heat sensitive binding to prevent individual sheets from being removed from a set.

4.4 Storage of Confidential Information

Steps should be taken to prevent unauthorized access to Confidential Information. Confidential Information should be kept in a locked storage room or a locked security container, such as a drawer, cabinet or safe-type file that has a locking mechanism, and must be vandalism resistant. The DISO will periodically review the departmental storage vehicles and mechanisms and determine their appropriateness for the information being stored. Confidential Information should be gathered and stored in a minimum number of office locations and Confidential Privileged Information must never be left unattended outside its storage location. A storage space or security container/receptacle may not be left open and unattended at any time. At no time should Confidential Information be stored, even for short periods, in unauthorized desk drawers, file cabinets, or other unsecured locations. The CISO may require that certain information be kept in a safe in a designated central location(s).

Combinations or locks for each security container must be changed or replaced when a person having knowledge of the combination or possession of a lock key no longer requires it, or there is reason to suspect that the combination has been tampered with, or that an unauthorized person may have acquired knowledge of the combination, or that a lock key is in the possession of an unauthorized person. Keys and combination locks protecting Confidential Information must be protected at the same level of protection as paper documents. The "Guidelines for the Storage of Confidential Information" attached as Appendix "G" provides further detailed information and instructions.

Confidential Privileged Information and, where appropriate Confidential Information, may not be stored at any individual's home overnight for a meeting the following day without prior authorization of the SIM or DISO.

Downloading of any Confidential Privileged Information and Confidential Information carries with it the responsibility to protecting that information in accordance with the procedures identified in this Handbook. The possessor of the electronic file assumes full responsibility for the proper handling, storage and transmittal of this Confidential Privileged Information and Confidential Information.

4.5 Document Accountability Log

All entities, Port Authority Departments and third-parties having Confidential Information in their possession will have a system in place that will account for the material in such a manner that retrieval is easily accomplished for inspection. The accountability log shall be maintained by the DISO, or the SPM, or SIM, where applicable, and include:

- The date that a document was received or created
- The identity of the sender or creator
- A brief description of the document
- The Control Number, if Confidential Privileged Information
- Number of copies

- Transmission history (sent to whom, when)
- If applicable at the time of the inspection, a Port Authority Records Destruction Certification (PA Form #283) stating that the document has been destroyed (including, when, by whom and the method), or a Certification that the document has been returned to the Port Authority.

4.6 Reproduction

Confidential Information should only be reproduced to the minimum extent necessary to carry out an individual or entity's responsibilities. However, the reproduced material must be marked and protected in the same manner and to the same extent as the original material. Authorized individuals must perform all reproduction work. Print and reproduction locations are limited to Port Authority sites, or, when appropriate, to authorized consultant and/or third-party contractor work site equipment. The CISO may require that the work site should limit reproduction of Confidential Information to a particular copying machine with technological capabilities limited to copying (not scanning or storing etc.). Service providers, authorized by the responsible SIM or DISO where appropriate, may be used for this task if the information remains safeguarded throughout the process. Each reproduction of Confidential Information shall contain all security markings, instructions, etc., as set forth in Section 4.1. All scraps, over-runs, and waste products resulting from reproduction shall be collected and processed for proper disposal.

4.7 Destruction of Confidential Information

All Confidential Information that is no longer needed shall be disposed of as soon as possible, consistent with the Port Authority's Record Retention Policy, by any method that prevents its unauthorized retrieval or reconstruction. The individuals who had been granted access to Confidential Information must perform the actual destruction. Authorized service providers may be used for this task provided that the information remains safeguarded until the destruction is completed. Paper products must be destroyed using a cross cut shredder located in the office. As previously noted in Section 4.5, a Port Authority Records Destruction Certificate (PA Form #283) must be provided to the DISO, SPM or SIM for any document being destroyed, including original or copies thereof, and provided to the CISO for final approval by the Secretary or her/his designee. In addition to the requirements in this Handbook, all Departments shall continue to comply with the Port Authority Records Program (A.P. 15-2.02). Where Confidential Information is no longer needed, but the Port Authority Records Program requires retention of the original, the original Confidential document shall be retained by the CISO and all copies are to be destroyed in accordance with this section. The "Guidelines for the Disposal and Destruction of Confidential Privileged Information" attached as Appendix "H" provides further detailed information and instruction.

Since deleted electronic files can be recoverable by utilizing software tools, Confidential Information stored in electronic form needs to be erased and destroyed with methods that comply with the US Department of Defense standards for file secure erasure (DoD 5220.22). Therefore, CyberScrub or a similar software shall be used to prevent discovery by a computer technician or other unauthorized person. With respect to Port Authority staff, individual staff shall contact the Technology Services Department ("TSD") to make a request that Confidential Information be permanently removed from a computer. This request shall be made by providing relevant information on a TSD form through the Internet or by email.

CHAPTER 5 – AUDITING AND MONITORING

5.1 Purpose

The ISSC, Audit and/or OIG may conduct random or scheduled examinations of business practices under the Policy in order to assess the extent of compliance with the Policy. The Policy's self-assessment and audit processes enable management to evaluate the Policy's uniformity throughout the Port Authority and of third parties' practices, in order to identify its strengths and potential exposures, and to help guide evolving policy objectives.

5.2 Audits and Investigations

Audits conducted by the ISSC and/or Audit may be scheduled in advance. The chief, department director, project manager, company liaison or contract representative of the organization being assessed should receive prior notice of the date of the assessment and also be advised as to what the assessment will consist of. A copy of the current version of the Audit Procedures guidelines, attached as Appendix "H", should be provided to the particular entity(ies) in order to allow adequate time to undertake appropriate pre-review and preparation action. The Audit Procedures guidelines should guide the ISSC and/or Audit through the assessment process. This Guideline is not all-inclusive and may be amended, as necessary. Organizations, departments, units, or third parties, preparing for an ISSC and/or Audit visit are encouraged to contact the CISO prior to the scheduled visit date in order to inquire and obtain additional information about the process.

The ISSC and/or Audit may also conduct information security assessments without prior notice and/or unannounced investigations coordinated through the Office of the General Counsel and the Office of Inspector General, as it may deem necessary and appropriate. Where appropriate, the CISO should be advised of the existence of such an investigation and, if appropriate, its nature.

The ISSC and/or Audit approach to conducting an assessment should consist of three phases (i) personnel interviews, (ii) site assistance visits, and (iii) corrective action follow-up.

(i) Personnel Interviews

The interview(s) should focus on the department, business unit, organization or third party's compliance with the Policy, how engaged the interviewee is with the Policy, and the level of education and awareness the interviewee has about the Policy. Employees, consultants, third-party contractors, and other individuals and/or entities should be included as potential interviewees. Personnel interviews should encompass a wide range of individuals who are regularly engaged with the Policy, as well as those having less involvement in it. This allows the ISSC to develop a balanced understanding regarding Policy compliance and effectiveness, as well as its impact on the organization and enable it both to identify concerns and issues regarding the Policy, and to solicit recommendations for possible improvements to the Policy.

(ii) Site Assistance Visits

The ISSC and/or Audit site visit should focus on a hands-on review of the following processes and procedures: document safeguards, handling protocols, transmission practices, control number usage, document marking, receipt and copying practices, and disposal of Confidential Information procedures. The visit should also include compliance reviews of the security clearance access criteria, document accountability audits, conditions regarding information access, background check processes, Authorized Personnel Clearance Lists updates, Confidential Information material sign out and sign in records, and the information security education awareness training program.

(iii) Follow-up

Policy compliance deficiencies noted during the assessments should be provided by the ISSC and/or Audit through the CISO to the department head, chief, project manager, consultant, third-party contractor liaison/representative, other agency staff, and the respective DISO, SPM, or SIM for corrective action. The ISSC, through the CISO, may also follow-up on investigation results to determine corrective actions and Policy compliance. The ISSC may also recommend the imposition of any penalties or disciplinary action that are described in Chapter 6.

With the assistance of the respective DISO, SPM, or SIM, a plan with milestones should be developed with the intention of correcting any identified deficiencies. A return site assistance visit may be scheduled in order to re-assess earlier identified deficiencies. The respective DISO, SPM, or SIM should forward a periodic corrective action progress report to the CISO as part of the milestone monitoring.

5.3 Self-Assessment

Department heads, chiefs, managers, supervisors, DISOs, SPMs or SIMs should conduct an annual self-assessment of their unit's Policy compliance using the Audit Procedures Guidelines. The results will not be forwarded to the CISO, Audit or ISSC, but should be used as a tool to gauge compliance before regular assessments are conducted. The results should be available for inspection and any serious findings should be forwarded to the CISO.

CHAPTER 6 – POLICY VIOLATIONS AND CONSEQUENCES

6.1 Responsibilities

Anyone having knowledge of any infraction, violation or breach of the Policy is required to report it to the OIG and to their supervisor, who shall in turn report the same to the DISO. The CISO shall have the final decision with respect to the violation determinations and/or the recommended course of action to be taken, consistent with Port Authority policy, practices and legal requirements referenced in this section.

All individuals who have been reported as having violated the Policy may be temporarily denied access to Confidential Information and/or have their security clearance suspended until an investigation is completed.

6.2 Violations, Infractions, or Breach of Information Security Protocols

Due to any number of unintended circumstances or, other conditions beyond the control of an individual, Confidential Information could be subject to compromise or loss. For example, an individual may unintentionally discard Confidential Information, mislabel Confidential Information, sent through the internal mail routing system, or drop or inadvertently leave Confidential Information in a public place. Intentional disclosure of Confidential Information to unauthorized individuals for personal gain, or to otherwise make available for unauthorized public release, may also occur. Violations, infractions and breaches of the Policy will be reviewed on a case-by-case basis to determine the facts and circumstances surrounding each incident.

6.3 Violation Reporting, Investigation and Fact Finding

Individuals must report alleged or suspected violations, infractions or breaches of the Policy to the OIG and to their supervisor or manager. The supervisor or manager must refer the issue and/or the individual to the DISO. The DISO, in consultation with the CISO and OIG, will determine whether an investigation into the allegations or other appropriate action is warranted. The CISO will consult with the OIG on these matters and the OIG will determine whether to undertake its own separate investigation into the matter. Individuals and/or entities must cooperate with all authorized investigations of any act, omission or occurrence relating to Port Authority property, information, materials, and, in the case of Port Authority employees, and if applicable, must comply with the Agency General Rules and Regulations. (See *"General Rules and Regulations for all Port Authority Employees."* Port Authority of New York and New Jersey. April 1990.)

6.4 Disciplinary Action

The following is a list of Policy violations and the respective disciplinary actions that may be taken against any individual and/or entity, having authorized access to Confidential Information, who violates their responsibilities in handling such information:

a) Non-deliberate violations involving negligence and/or carelessness, such as leaving Confidential Information unattended.

First Offense: Verbal reprimand and security briefing.

Second Offense: Written reprimand and/or a security briefing and possible suspension or termination of access privileges, depending on the circumstances.

Third Offense - Termination of access and possible imposition of civil penalties. Where the offense involves a Port Authority employee, disciplinary action may also be taken.

b) Non-deliberate violation involving negligence and/or carelessness such as misplacing or losing a document.

First Offense - Written reprimand and/or a security briefing, and possible suspension or termination of access privileges, depending on the circumstances, and possible imposition of a civil penalty. Where the offense involves a Port Authority employee, disciplinary action may also be taken.

Second Offense - Dismissal or termination of access privileges, and, depending on the circumstances, the imposition of a civil penalty, and possible legal action against the violator. Where the offense involves a Port Authority employee, disciplinary action may also be taken including suspension with forfeiture of up to one year's personal and vacation time allocation.

c) For cases of deliberate disregard of security procedures or gross negligence in handling Confidential Information.

First Offense – Suspension or termination of access privileges, termination of an agreement or contract, written reprimand, imposition of a civil penalty depending on the circumstances, and possible legal civil and/or criminal action against the violator. Where the offense involves a Port Authority employee, disciplinary action may be taken up to and including termination of employment. Termination of access privileges will be for a period of one year at minimum and may be permanent, subject to review by the CISO.

The Port Authority may also impose investigation costs and/or a monitor to oversee future compliance with its security policies and practices at the violator's expense, when the violation is by a consultant, vendor contractor or other third party. Nothing herein is construed to limit the Port Authority's right to exercise or take other legal rights and remedies including terminating agreements with a third party violator and/or refusing to enter into future business relationships with the violator and/or seeking such legal action, as it may deem appropriate, including injunctive, civil actions for monetary damages and/or seeking criminal prosecution of the violator(s).

In addition, any violation relating to SSI or CII will be reported to the TSA, the OIG, and/or, if applicable, DOT, USCG or DHS. Penalties and other enforcement or corrective action may be taken as set forth in relevant statutes, rules and regulations, including, without limitation, the issuance of orders requiring retrieval of Sensitive Security Information and Critical Infrastructure Information to remedy unauthorized disclosure and directions to cease future unauthorized disclosure. Applicable Federal Regulations, including, without limitation, 49 C.F.R. § 15.17 and 1520.17 and 6 CFR Part 29, provide that any such violation thereof or mishandling of information therein defined may constitute grounds for a civil penalty and other enforcement or corrective action being taken by the DOT, TSA and/or DHS.

CHAPTER 7 – INFORMATION SECURITY EDUCATION AND AWARENESS TRAINING

7.1 Purpose

Information security education and awareness training ensures that all personnel requiring access to Confidential Information, regardless of position or grade level, have an appropriate understanding of the need to adhere to security procedures in order to protect Confidential Information. The goal of the training program is basically to provide that all such employees, consultants, third-party contractors, other individuals, entities and/or, where appropriate, third parties develop essential security habits and thereby ensure that all personnel handling Confidential Information understand and carry out the proper handling protocols for those materials.

7.2 Overview

The CISO is responsible for implementing the Information Security Education and Awareness Training Program (the "Training Program"). The Training Program, with assistance from the Office of Inspector General, DISO, SPM and SIM, should be provided to all employees, consultants, third-party contractors, and other agency personnel requiring access to Confidential Information. These individuals, regardless of rank or position in a particular organization, must complete initial indoctrination and annual refresher training. The CISO, with the concurrence of the Law Department, may waive this requirement for certain individuals. A current list containing the names of all persons who completed training will be developed and retained by the CISO. The CISO shall ensure that all employees have complied with the requisite Training Program.

7.3 Training Program Elements

The Training Program consists of three interconnected elements: (a) indoctrination training, (b) orientation training, and (c) annual refresher training. Each element provides employees, consultants, third-party contractors, and other agency personnel with a baseline of knowledge, as well as periodic updates, about the existing and current Policy. Each element of the Training Program contributes another level of information to the individual. At a minimum, all individuals must receive the indoctrination training and the annual refresher training.

(a) Indoctrination Training

Indoctrination Training provides personnel with the fundamentals of the Training Program. It should be completed when beginning employment or assignment to a project for the Port Authority, but no later than sixty (60) days after initial hire, or after commencing work on a project. It may be combined with other types of new employee indoctrination programs. Individuals completing this level of training should understand the basic organization of the Policy, the Policy definitions, what materials are defined as Confidential Information under the Policy, how to identify Confidential Information (security category levels and markings), the general criteria and conditions required in order to be granted a security clearance, procedures for categorizing documents, the obligation to report suspected and alleged policy violations, and the penalties for non-compliance with the policy and for unauthorized disclosure of Confidential Information.

(b) Orientation Training

Orientation Training focuses on the more specific protocols, practices and procedures for individuals whose roles and responsibilities involve reading, using, safeguarding, handling, and disposing of Confidential Information. Individuals assigned such responsibilities should complete this level of training. Orientation training should be conducted prior to assignment to a department, project, task, or other special assignment, where the individual is expected to become involved with receiving and handling Confidential Information. Individuals completing this level of training should be introduced to the DISO, SPM, or SIM, understand the organizational elements of the Policy, know how to process Confidential Information, know the different security categories under their control or within their assigned work environment, know how to identify proper safeguarding protocols, including hardware needs, and understand the differences between general access privileges and the need to know requirement for access to particular information. Individuals should also read and acknowledge their understanding of the requirements.

(c) Annual Refresher Training

Once a year, during the anniversary month of the individual's start date on a project, or initial access to Confidential Information, all employees, consultants, third-party contractors, and other individuals and/or entities, who continue to have access to sensitive materials, should receive an information security education and awareness training refresher briefing to enhance their information security awareness. At a minimum, the annual refresher training should include indoctrination and orientation topic training, as well as key training on recent Policy changes or other appropriate information. Also, this milestone may be used to reaffirm the individual's need for a security clearance or to determine whether the individual requires a periodic update of their background check.

(d) Other Circumstances and Special Briefings

If a Port Authority employee, consultant, third-party contractor, or other individual and/or entity transfers to another department, is promoted within his or her department, or changes employers on the same project without a break in service, and can provide a record of completion of indoctrination training within the previous twelve months, only annual refresher training may be required. All other situations demand that an individual requiring access to Confidential Information fulfill the conditions for information security education and awareness training under this Policy.

In addition to reading and signing a NDA or an Acknowledgment of an existing NDA, or, alternatively, being subject to a NDI, temporary or one-time access individuals should be fully briefed on the limitations on access to Confidential Information and the penalties associated with the unauthorized disclosure, before being granted access to such information.

Special briefings may be provided on a case-by-case basis, as circumstances may require.

APPENDIX A-1

NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT BETWEEN

(INSERT NAME OF COMPANY)

AND

THE PORT AUTHORITY OF NEW YORK AND NEW JERSEY

THIS NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT (this "**Agreement**") is made as of this ____ day of _____, 20__, by and between THE PORT AUTHORITY OF NEW YORK AND NEW JERSEY (the "**Port Authority**") a body corporate and politic created by Compact between the States of New York and New Jersey, with the consent of the Congress of the United States, and having an office and place of business at 225 Park Avenue South, New York, New York, 10003, and _____ having an office and place of business at _____(address) ("**Recipient**").

WHEREAS, the Port Authority desires, subject to the terms and conditions set forth below, to disclose to Recipient Confidential Information (as defined below) in connection with _____-_____(insert description of project/work) (collectively, the "Project(s)", or "Proposed Project(s)"); and

WHEREAS, the Recipient acknowledges that the Port Authority, in furtherance of its performance of essential and critical governmental functions relating to the Project, has existing and significant interests and obligations in establishing, maintaining and protecting the security and safety of the Project site and surrounding areas and related public welfare matters; and

WHEREAS, in furtherance of critical governmental interests regarding public welfare, safety and security at the Project site, the Port Authority has collected information and undertaken the development of certain plans and recommendations regarding the security, safety and protection of the Project site, including the physical construction and current and future operations; and

WHEREAS, the Port Authority and Recipient (collectively, the "**Parties**") acknowledge that in order for Recipient to undertake its duties and/or obligations with regard to its involvement in the Project, the Port Authority may provide Recipient or certain of its Related Parties (as defined below) certain information in the possession of the Port Authority, which may contain or include confidential, privileged, classified, commercial, proprietary or sensitive information, documents and plans, relating to the Project or its occupants or other matters, the unauthorized disclosure of which could

result in significant public safety, financial and other damage to the Port Authority, the Project, its occupants, and the surrounding communities; and

WHEREAS, Recipient recognizes and acknowledges that providing unauthorized access to, or disclosing such information to third parties in violation of the terms of this Agreement could compromise or undermine the existing or future guidelines, techniques and procedures implemented for the protection against terrorist acts or for law enforcement, investigation and prosecutorial purposes, and accordingly could result in significant irreparable harm and injury; and

WHEREAS, in order to protect and preserve the privilege attaching to and the confidentiality of the aforementioned information as well as to limit access to such information to a strict need to know basis, the Port Authority requires, as a condition of its sharing or providing access to such confidential, privileged, classified, commercial, proprietary or sensitive information, documents and plans, that the Recipient enter into this Agreement and that its Related Parties thereafter acknowledge and agree that they will be required to treat as strictly confidential and/or privileged any of such information so provided, as well as the work product and conclusions of any assessments and evaluations or any recommendations relating thereto, and to also fully comply with applicable federal rules and regulations with respect thereto; and

WHEREAS, as a condition to the provision of such information to Recipient and certain Related Parties, the Recipient has agreed to enter into this Agreement with respect to the handling and use of such information and to cause Related Parties to join in and be bound by the terms and conditions of this Agreement.

NOW, THEREFORE, in consideration of the provision by Port Authority of Information for Project Purposes (as each such term is defined below) and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged by the Recipient and each Related Party that receives such Information, the Recipient and each such Related Party agrees, as follows:

1. Defined Terms. In addition to the terms defined in the Recitals above, the following terms shall have the meanings set forth below:

"**Authorized Disclosure**" means the disclosure of Confidential Information strictly in accordance with the Confidentiality Control Procedures applicable thereto: (i) as to all Confidential Information, only to a Related Party that has a need to know such Confidential Information strictly for Project Purposes and that has agreed in writing to be bound by the terms of this Agreement by executing a form of Acknowledgment as set forth in Exhibit A; and (ii) as to Confidential Privileged Information, only to the extent expressly approved in writing and in advance by the Port Authority, and then only the particular Confidential Privileged Information that is required to accomplish an essential element of the Project.

"**Confidential Information**" means and includes collectively, Confidential Proprietary Information, Confidential Privileged Information, and Information that

is labeled, marked or otherwise identified by or on behalf of the Port Authority so as to reasonably connote that such Information is confidential, privileged, sensitive or proprietary in nature. The term Confidential Information shall also include all work product that contains or is derived from any of the forgoing, whether in whole or in part, regardless of whether prepared by the Recipient, the Port Authority or others. The following Information shall not constitute Confidential Information for the purpose of this Agreement:

Particular Information, other than Confidential Privileged Information, that is provided to the Recipient by a source other than the Port Authority, provided that such source is not subject to a confidentiality agreement, or similar obligation, or understanding with or for the benefit of the Port Authority, with respect to such Information and that the identity of such source is not itself part of such Confidential Information.

Information that is or becomes generally available to the public other than as a result of a disclosure by the Recipient or a Related Party in violation of this Agreement.

"**Confidential Privileged Information**" means and includes collectively, (i) any and all Information, documents and materials entitled to protection as a public interest privilege under New York State law and as may be deemed to be afforded or entitled to the protection of any other privilege recognized under New York, and/or New Jersey state laws or Federal laws, (ii) Critical Infrastructure Information, (iii) Sensitive Security Information, and (iv) Limited Access Safety and Security Information.

"**Confidential Proprietary Information**" means and includes Information that contains financial, commercial or other proprietary, business information concerning the Project, the Port Authority, or its facilities.

"**Confidentiality Control Procedures**" means procedures, safeguards and requirements for the identification, processing, protection, handling, care, tracking and storage of Confidential Information that are required under applicable federal or state law, the Port Authority Handbook, or by the terms of this Agreement.

"**Critical Infrastructure Information**" (CII) has the meaning set forth in the Homeland Security Act of 2002, under the subtitle Critical Infrastructure Information Act of 2002 (6 U.S.C. §131-134), and any rules or regulations enacted pursuant thereto, including, without limitation, the Office of the Secretary, Department of Homeland Security Rules and Regulations, 6 C.F.R. Part 29 and any amendments thereto. CII may also be referred to as "Protected Critical Infrastructure Information" or "PCII," as provided for in the referenced rules and regulations and any amendments thereto.

"**Information**" means, collectively, all information, documents, data, reports, notes, studies, projections, records, manuals, graphs, electronic files, computer generated data or information, drawings, charts, tables, diagrams, photographs, and other media or renderings containing or otherwise incorporating information that may be provided or made accessible at any time, whether in writing, orally, visually, photographically, electronically or in any other form or medium, including, without limitation, any and all copies, duplicates or extracts of the foregoing.

"**Limited Access Safety and Security Information**" means and includes sensitive Information, the disclosure of which would be detrimental to the public interest and might compromise public safety and/or security as it relates to Port Authority property, facilities, systems and operations, and which has not otherwise been submitted for classification or designation under any Federal laws or regulations.

"**Port Authority Handbook**" means the Port Authority of N.Y. & N.J. Information Security Handbook, a copy of which is attached hereto as Exhibit B, as may be amended by the Port Authority, from time to time.

"**Project Purposes**" means the use of Confidential Information strictly and only for purposes related to Recipient's and its Related Parties' participation and involvement in the Project, and only for such period of time during which Recipient and its Related Parties are involved in Project related activities.

"**Related Party**" and "**Related Parties**" means the directors, employees, officers, partners or members of the Recipient, as applicable, and the Recipient's outside consultants, advisors, accountants, architects, engineers or subcontractors or subconsultants (and their respective directors, employees, officers, partners or members) to whom any Confidential Information is disclosed or made available.

"**Sensitive Security Information**" has the definition and requirements set forth in the Transportation Security Administrative Rules & Regulations, 49 CFR 1520, (49 U.S.C. §114) and in the Office of the Secretary of Transportation Rules & Regulations, 49 CFR 15, (49 U.S.C. §40119) and any amendments thereto.

2. Use of Confidential Information. All Confidential Information shall be used by the Recipient in accordance with the following requirements:

All Confidential Information shall be held in confidence and shall be processed, treated, disclosed and used by the Recipient and its Related Parties only for Project Purposes and in accordance with the Confidentiality Control Procedures established pursuant to Paragraph 2(c), below, including, without limitation, the Port Authority Handbook, receipt of which is acknowledged by Recipient and shall be acknowledged in writing by each Related Party by signing the Acknowledgment attached hereto as Exhibit A, and applicable legal requirements. Confidential Information may be disclosed, only if and to the extent that such disclosure is an Authorized Disclosure.

Recipient and each Related Party acknowledges and agrees that (i) any violation by the Recipient or any of its Related Parties of the terms, conditions or restrictions of this Agreement relating to Confidential Information may result in penalties and other enforcement or corrective action as set forth in such statutes and regulations, including, without limitation, the issuance of orders requiring retrieval of Sensitive Security Information and Critical Infrastructure Information to remedy unauthorized disclosure and to cease future unauthorized disclosure and (ii) pursuant to the aforementioned Federal Regulations, including, without limitation, 49 C.F.R. §§ 15.17 and 1520.17, any such violation thereof or mishandling of information therein defined may constitute grounds for a civil penalty and other enforcement or corrective action by the United States Department of Transportation and the United States Department of Homeland Security, and appropriate personnel actions for Federal employees.

Recipient and each Related Party covenants to the Port Authority that it has established, promulgated and implemented Confidentiality Control Procedures for identification, handling, receipt, care, and storage of Confidential Information to control and safeguard against any violation of the requirements of this Agreement and against any unauthorized access, disclosure, modification, loss or misuse of Confidential Information. Recipient and each Related Party shall undertake reasonable steps consistent with such Confidentiality Control Procedures to assure that disclosure of Confidential Information is compartmentalized, such that all Confidential Information shall be disclosed only to those persons and entities authorized to receive such Information as an Authorized Disclosure under this Agreement and applicable Confidentiality Control Procedures. The Confidentiality Control Procedures shall, at a minimum, adhere to, and shall not be inconsistent with, the procedures and practices established in the Port Authority Handbook.

The Port Authority may request in writing that the Recipient or any Related Parties apply different or more stringent controls on the handling, care, storage and disclosure of particular items of Confidential Information as a precondition for its disclosure. The Port Authority may decline any request by the Recipient or any of its Related Parties to provide such item of Confidential Information if the Recipient or any of the Related Parties do not agree in writing to apply such controls.

Nothing in this Agreement shall require the Port Authority to tender or provide access to or possession of any Confidential Information to the Recipient or its Related Parties, whether or not the requirements of this Agreement are otherwise satisfied. However, if such Confidential Information is provided and accepted, the Recipient and its Related Parties shall abide by the terms, conditions and requirements of this Agreement.

The Recipient and each Related Party agrees to be responsible for enforcing the provisions of this Agreement with respect to its Related Parties, in accordance with the Confidentiality Control Procedures. Except as required by law pursuant

to written advice of competent legal counsel, or with the Port Authority's prior written consent, neither the Recipient, nor any of the Related Parties shall disclose to any third party, person or entity: (i) any Confidential Information under circumstances where the Recipient is not fully satisfied that the person or entity to whom such disclosure is about to be made shall act in accordance with the Confidentiality Control Procedures whether or not such person or entity has agreed in writing to be bound by the terms of this Agreement or any "Acknowledgement" of its terms or (ii) the fact that Confidential Information has been made available to the Recipient or such Related Parties, or the content or import of such Confidential Information. The Recipient is responsible for collecting and managing the Acknowledgments signed by Related Parties pursuant to this Agreement. Recipient shall, at the Port Authority's request, provide the Port Authority a list of all Related Parties who have signed an Acknowledgment, and copies of such Acknowledgments.

As to all Confidential Information provided by or on behalf of the Port Authority, nothing in this Agreement shall constitute or be construed as a waiver of any public interest privilege or other protections established under applicable state or federal law.

3. **Disclosures and Discovery Requests**. If a subpoena, discovery request, Court Order, Freedom of Information Request, or any other request or demand authorized by law seeking disclosure of the Confidential Information is received by the Recipient or any Related Party, Recipient shall notify the Port Authority thereof with sufficient promptness so as to enable the Port Authority to investigate the circumstances, prepare any appropriate documentation and seek to quash the subpoena, to seek a protective order, or to take such other action regarding the request as it deems appropriate. In the absence of a protective order, disclosure shall be made, in consultation with the Port Authority, of only that part of the Confidential Information as is legally required to be disclosed. If at any time Confidential Information is disclosed in violation of this Agreement, the Recipient shall immediately give the Port Authority written notice of that fact and a detailed account of the circumstances regarding such disclosure to the Port Authority.

4. **Retention Limitations; Return of Confidential Information**. Upon the earlier occurrence of either the Port Authority's written request or completion of Recipient's need for any or all Confidential Information, such Confidential Information, all writings and material describing, analyzing or containing any part of such Confidential Information, including any and all portions of Confidential Information that may be stored, depicted or contained in electronic or other media and all copies of the foregoing shall be promptly delivered to the Port Authority at Recipient's expense. In addition, as to Confidential Information that may be stored in electronic or other form, such Confidential Information shall be completely removed so as to make such Confidential Information incapable of being recovered from all computer databases of the Recipient and all Related Parties. The Recipient may request in writing that the Port Authority

consent to destruction of Confidential Information, writings and materials in lieu of delivery thereof to the Port Authority. The Port Authority shall not unreasonably withhold its consent to such request. If the Port Authority consents to such destruction, the Recipient and each Related Party shall deliver to the Port Authority a written certification by Recipient and such Related Party that such Confidential Information, writings and materials have been so destroyed within such period as may be imposed by the Port Authority. Notwithstanding the foregoing, to the extent required for legal or compliance purposes, the Recipient may retain a copy of Confidential Information, provided that (a) the Port Authority is notified in writing of such retention, and (b) Recipient continues to abide by the requirements of this Agreement with respect to the protection of such Confidential Information.

5. **Duration and Survival of Confidentiality Obligations**. The obligations under this Agreement shall be perpetual (unless otherwise provided in this Agreement) or until such time as the Confidential Information is no longer considered confidential and/or privileged by the Port Authority.

6. **Severability**. Each provision of this Agreement is severable and if a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

7. **Injunctive and Other Relief**. Recipient and each Related Party acknowledges that the unauthorized disclosure and handling of Confidential Information is likely to have a material adverse and detrimental impact on public safety and security and could significantly endanger the Port Authority, its facilities (including, without limitation, the Project site), its patrons and the general public and that damages at law are an inadequate remedy for any breach, or threatened breach, of this Agreement by Recipient or its Related Parties. The Port Authority shall be entitled, in addition to all other rights or remedies, to seek such restraining orders and injunctions as it may deem appropriate for any breach of this Agreement, without being required to show any actual damage or to post any bond or other security.

8. **Governing Law**. This Agreement shall be governed by and construed in accordance with the laws of the State of New York, without regard to conflict of laws principles. The Port Authority (subject to the terms of the Port Authority Legislation (as defined below)) and the Recipient specifically and irrevocably consent to the exclusive jurisdiction of any federal or state court in the County of New York and State of New York with respect to all matters concerning this Agreement and its enforcement. The Port Authority (subject to the terms of the Port Authority Legislation (as defined below)) and the Recipient agree that the execution and performance of this Agreement shall have a New York situs and, accordingly, they each consent (and solely with respect to the Port Authority, subject to the terms of the Port Authority Legislation (as defined below)) to personal jurisdiction in the State of New York for all purposes and proceedings arising from this Agreement. "**Port Authority Legislation**" shall mean the concurrent legislation of the State of New York and State of New Jersey set forth at Chapter 301 of the Laws of New York of 1950, as amended by Chapter 938 of the Laws

of New York of 1974 (McKinney's Unconsolidated Laws §§7101-7112) and Chapter 204 of the Laws of New Jersey of 1951 (N.J.S.A. 32:1-157 to 32:1-168).

9. Notices. Any notice, demand or other communication (each, a "**notice**") that is given or rendered pursuant to this Agreement by either party to the other party, shall be: (i) given or rendered, in writing, (ii) addressed to the other party at its required address(es) for notices delivered to it as set forth below, and (iii) delivered by either (x) hand delivery, or (y) nationally recognized courier service (e.g., Federal Express, Express Mail). Any such notice shall be deemed given or rendered, and effective for purposes of this Agreement, as of the date actually delivered to the other party at such address(es) (whether or not the same is then received by other party due to a change of address of which no notice was given, or any rejection or refusal to accept delivery). Notices from either party (to the other) may be given by its counsel.

The required address(es) of each party for notices delivered to it is (are) as set forth below. Each party, however, may, from time to time, designate an additional or substitute required address(es) for notices delivered to it, provided that such designation must be made by notice given in accordance with this Paragraph 0.

If to the Port Authority: _____

_____

The Port Authority of New York and New Jersey

225 Park Avenue South, __th Floor

New York, NY 10003

with a copy to: The Port Authority of New York and New Jersey

225 Park Avenue South - 15th Floor

New York, NY 10003

Attn: General Counsel

If to the Recipient: _____
_____
_____

with a copy to: _____
_____
_____

10. Entire Agreement. This Agreement contains the complete statement of all the agreements among the parties hereto with respect to the subject matter thereof, and all prior agreements among the parties hereto respecting the subject matter hereof, whether written or oral, are merged herein and shall be of no further force or effect. This Agreement may not be changed, modified, discharged, or terminated, except by an instrument in writing signed by all of the parties hereto.

11. Counterparts. This Agreement may be executed in one or more counterparts, each of which shall be deemed to be an original, but all of which shall be one and the same document.

12. Parties Bound. This Agreement shall be binding upon the Recipient and its respective successors. The foregoing shall not be affected by the failure of any Related Party to join in this Agreement or to execute and deliver an Acknowledgement hereof.

13. Authority. The undersigned individual(s) executing this Agreement on behalf of the Recipient below represent(s) that they are authorized to execute this Agreement on behalf of the Recipient and to legally bind such party.

14. Disclosure of Ownership Rights or License. Nothing contained herein shall be construed as the granting or conferring by the Port Authority of any rights by ownership, license or otherwise in any Information.

15. No Liability. Neither the Commissioners of the Port Authority, nor any of them, nor any officer, agent or employee thereof, shall be charged personally by the Recipient with any liability, or held liable to the Recipient under any term or provision of this Agreement, or because of its execution or attempted execution or because of any breach, or attempted or alleged breach thereof.

16. Construction. This Agreement is the joint product of the parties hereto and each provision of this Agreement has been subject to the mutual consultation, negotiation, and agreement of the parties hereto, and shall not be construed for or against any party hereto. The captions of the various sections in this Agreement are for convenience only and do not, and shall not be deemed to, define, limit or construe the contents of such Sections.

[*No further text on this page; signatures appear on next page*]

IN WITNESS WHEREOF, the Recipient has executed this Agreement as of the date first above written.

Dated: New York, New York

_____ ____, _____

RECIPIENT:

_____

By: _____

Title: _____

Date: _____

EXHIBIT A

ACKNOWLEDGMENT BY RELATED PARTY ENTITY

The undersigned, _____ (name of authorized signatory), is the _____(Title) of _____ (name of entity), a _____(type of entity and jurisdiction of formation) ("**Related Party**"), located at _____ (address of entity), and is duly authorized to execute this Acknowledgment on behalf of the above Related Party. The above Related Party is involved with the functions of _____ (describe scope of work of Related Party) in connection with _____(describe Project) for The Port Authority of New York and New Jersey (the "**Port Authority**"). I acknowledge and confirm that the above named Related Party has been provided with a copy of and shall be bound and shall abide by all of the terms, requirements and conditions set forth in the Non Disclosure and Confidentiality Agreement dated _____ ____, _____, between _____ (the "**Recipient**") and the Port Authority (hereinafter the "**Agreement**"), and by the Port Authority Handbook described in the Agreement. Appropriate and responsible officers and employees of the Related Party have carefully read and understand the terms and conditions of the Agreement. The Related Party has notice and acknowledges that any breach or violation of such terms, requirements and conditions may result in the imposition of remedies or sanctions as set forth or otherwise described therein against such Related Party.

Signed: _____

Print Name: _____

Title: _____

Date: _____

ACKNOWLEDGMENT BY RELATED PARTY INDIVIDUAL

I, _____ (name of employee) ("**Related Party**"), am employed as a(n) _____(job title) by _____ (name of employer). I have been provided with and have read the Non Disclosure and Confidentiality Agreement between _____ (the "**Recipient**") and The Port Authority of New York and New Jersey (the "**Port Authority**") dated _____ ____, _____ (hereinafter the "**Agreement**"), and the Port Authority Handbook attached to the Agreement. I understand that because of my employer's relationship with _____ (name of Recipient, or the Port Authority if Related Party Individual is an employee of Recipient), both my employer and I may be provided with access to, and/or copies of, sensitive security materials or confidential information. If it is required for me to review or receive Confidential Information, as it is defined in the aforementioned Agreement, I acknowledge that I will be bound by each and every term and provision contained therein, and that failure to do so may include, but is not limited to, the imposition of disciplinary action and sanctions, and/or the institution of legal action seeking injunctive relief, monetary and/or criminal penalties for violation of law and/or Port Authority policies and procedures, as well as for violation of federal and/or state regulations.

To the extent that I am currently in the possession of, or have previously come into contact with, marked information as it relates to the aforementioned Agreement, I agree to conform my handling procedures for Confidential Information to the practices and procedures set forth and defined herein, or risk loss of access to said Information, removal from said Project and/or subjecting myself to the aforementioned disciplinary actions and/or civil and criminal penalties.

Signed: _____

Print Name: _____

Title: _____

Date: _____

APPENDIX A-2

NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT BETWEEN

(INSERT NAME OF COMPANY)

AND

THE PORT AUTHORITY OF NEW YORK AND NEW JERSEY

THIS NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT (this "**Agreement**") is made as of this ____ day of _____, 20___, by and between THE PORT AUTHORITY OF NEW YORK AND NEW JERSEY (the "**Port Authority**") a body corporate and politic created by Compact between the States of New York and New Jersey, with the consent of the Congress of the United States, and having an office and place of business at 225 Park Avenue South, New York, New York, 10003, and _____ having an office and place of business at _____(address) ("**Recipient**").

WHEREAS, the Port Authority desires, subject to the terms and conditions set forth below, to disclose to Recipient Confidential Information (as defined below) in connection with _____-_____(insert description of project/work) (collectively, the "Project(s)", or "Proposed Project(s)"); and

WHEREAS, the Recipient acknowledges that the Port Authority, in furtherance of its performance of essential and critical governmental functions relating to the Project, has existing and significant interests and obligations in establishing, maintaining and protecting the security and safety of the Project site and surrounding areas and related public welfare matters; and

WHEREAS, in furtherance of critical governmental interests regarding public welfare, safety and security at the Project site, the Port Authority has collected information and undertaken the development of certain plans and recommendations regarding the security, safety and protection of the Project site, including the physical construction and current and future operations; and

WHEREAS, the Port Authority and Recipient (collectively, the "**Parties**") acknowledge that in order for Recipient to undertake its duties and/or obligations with regard to its involvement in the Project, the Port Authority may provide Recipient or certain of its Related Parties (as defined below) certain information in the possession of the Port Authority, which may contain or include confidential, privileged, classified, commercial, proprietary or sensitive information, documents and plans, relating to the Project or its occupants or other matters, the unauthorized disclosure of which could

result in significant public safety, financial and other damage to the Port Authority, the Project, its occupants, and the surrounding communities; and

WHEREAS, Recipient recognizes and acknowledges that providing unauthorized access to, or disclosing such information to third parties in violation of the terms of this Agreement could compromise or undermine the existing or future guidelines, techniques and procedures implemented for the protection against terrorist acts or for law enforcement, investigation and prosecutorial purposes, and accordingly could result in significant irreparable harm and injury; and

WHEREAS, in order to protect and preserve the privilege attaching to and the confidentiality of the aforementioned information as well as to limit access to such information to a strict need to know basis, the Port Authority requires, as a condition of its sharing or providing access to such confidential, privileged, classified, commercial, proprietary or sensitive information, documents and plans, that the Recipient enter into this Agreement and that its Related Parties thereafter acknowledge and agree that they will be required to treat as strictly confidential and/or privileged any of such information so provided, as well as the work product and conclusions of any assessments and evaluations or any recommendations relating thereto, and to also fully comply with applicable federal rules and regulations with respect thereto; and

WHEREAS, as a condition to the provision of such information to Recipient and certain Related Parties, the Recipient has agreed to enter into this Agreement with respect to the handling and use of such information and to cause Related Parties to join in and be bound by the terms and conditions of this Agreement.

NOW, THEREFORE, in consideration of the provision by Port Authority of Information for Project Purposes (as each such term is defined below) and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged by the Recipient and each Related Party that receives such Information, the Recipient and each such Related Party agrees, as follows:

1. Defined Terms. In addition to the terms defined in the Recitals above, the following terms shall have the meanings set forth below:

"**Authorized Disclosure**" means the disclosure of Confidential Information strictly in accordance with the Confidentiality Control Procedures applicable thereto: (i) as to all Confidential Information, only to a Related Party that has a need to know such Confidential Information strictly for Project Purposes and that has agreed in writing to be bound by the terms of this Agreement by executing a form of Acknowledgment as set forth in Exhibit A; and (ii) as to Confidential Privileged Information, only to the extent expressly approved in writing and in advance by the Port Authority, and then only the particular Confidential Privileged Information that is required to accomplish an essential element of the Project.

"**Confidential Information**" means and includes collectively, Confidential Proprietary Information, Confidential Privileged Information, and Information that

is labeled, marked or otherwise identified by or on behalf of the Port Authority so as to reasonably connote that such Information is confidential, privileged, sensitive or proprietary in nature. The term Confidential Information shall also include all work product that contains or is derived from any of the forgoing, whether in whole or in part, regardless of whether prepared by the Recipient, the Port Authority or others. The following Information shall not constitute Confidential Information for the purpose of this Agreement:

Particular Information, other than Confidential Privileged Information, that is provided to the Recipient by a source other than the Port Authority, provided that such source is not subject to a confidentiality agreement, or similar obligation, or understanding with or for the benefit of the Port Authority, with respect to such Information and that the identity of such source is not itself part of such Confidential Information.

Information that is or becomes generally available to the public other than as a result of a disclosure by the Recipient or a Related Party in violation of this Agreement.

"**Confidential Privileged Information**" means and includes collectively, (i) any and all Information, documents and materials entitled to protection as a public interest privilege under New York State law and as may be deemed to be afforded or entitled to the protection of any other privilege recognized under New York, and/or New Jersey state laws or Federal laws, (ii) Critical Infrastructure Information, (iii) Sensitive Security Information, and (iv) Limited Access Safety and Security Information.

"**Confidential Proprietary Information**" means and includes Information that contains financial, commercial or other proprietary, business Information concerning the Project, the Port Authority, or its facilities.

"**Confidentiality Control Procedures**" means procedures, safeguards and requirements for the identification, processing, protection, handling, care, tracking and storage of Confidential Information that are required under applicable federal or state law or by the terms of this Agreement.

"**Critical Infrastructure Information**" (CII) has the meaning set forth in the Homeland Security Act of 2002, under the subtitle Critical Infrastructure Information Act of 2002 (6 U.S.C. §131-134), and any rules or regulations enacted pursuant thereto, including, without limitation, the Office of the Secretary, Department of Homeland Security Rules and Regulations, 6 C.F.R. Part 29 and any amendments thereto. CII may also be referred to as "Protected Critical Infrastructure Information" or "PCII," as provided for in the referenced rules and regulations and any amendments thereto.

"**Information**" means, collectively, all information, documents, data, reports, notes, studies, projections, records, manuals, graphs, electronic files, computer

generated data or information, drawings, charts, tables, diagrams, photographs, and other media or renderings containing or otherwise incorporating information that may be provided or made accessible at any time, whether in writing, orally, visually, photographically, electronically or in any other form or medium, including, without limitation, any and all copies, duplicates or extracts of the foregoing.

"**Limited Access Safety and Security Information**" means and includes sensitive Information, the disclosure of which would be detrimental to the public interest and might compromise public safety and/or security as it relates to Port Authority property, facilities, systems and operations, and which has not otherwise been submitted for classification or designation under any Federal laws or regulations.

"**Project Purposes**" means the use of Confidential Information strictly and only for purposes related to Recipient's and its Related Parties' participation and involvement in the Project, and only for such period of time during which Recipient and its Related Parties are involved in Project related activities.

"**Related Party**" and "**Related Parties**" means the directors, employees, officers, partners or members of the Recipient, as applicable, and the Recipient's outside consultants, advisors, accountants, architects, engineers or subcontractors or subconsultants (and their respective directors, employees, officers, partners or members) to whom any Confidential Information is disclosed or made available.

"**Sensitive Security Information**" has the definition and requirements set forth in the Transportation Security Administrative Rules & Regulations, 49 CFR 1520, (49 U.S.C. §114) and in the Office of the Secretary of Transportation Rules & Regulations, 49 CFR 15, (49 U.S.C. §40119) and any amendments thereto.

2. Use of Confidential Information. All Confidential Information shall be used by the Recipient in accordance with the following requirements:

All Confidential Information shall be held in confidence and shall be processed, treated, disclosed and used by the Recipient and its Related Parties only for Project Purposes and in accordance with the Confidentiality Control Procedures established pursuant to Paragraph 2(c), below, and applicable legal requirements. Confidential Information may be disclosed, only if and to the extent that such disclosure is an Authorized Disclosure.

Recipient and each Related Party acknowledges and agrees that (i) any violation by the Recipient or any of its Related Parties of the terms, conditions or restrictions of this Agreement relating to Confidential Information may result in penalties and other enforcement or corrective action as set forth in such statutes and regulations, including, without limitation, the issuance of orders requiring retrieval of Sensitive Security Information and Critical Infrastructure Information to remedy unauthorized disclosure and to cease future unauthorized disclosure

and (ii) pursuant to the aforementioned Federal Regulations, including, without limitation, 49 C.F.R. §§ 15.17 and 1520.17, any such violation thereof or mishandling of information therein defined may constitute grounds for a civil penalty and other enforcement or corrective action by the United States Department of Transportation and the United States Department of Homeland Security, and appropriate personnel actions for Federal employees.

Recipient and each Related Party covenants to the Port Authority that it has established, promulgated and implemented Confidentiality Control Procedures for identification, handling, receipt, care, and storage of Confidential Information to control and safeguard against any violation of the requirements of this Agreement and against any unauthorized access, disclosure, modification, loss or misuse of Confidential Information. Recipient and each Related Party shall undertake reasonable steps consistent with such Confidentiality Control Procedures to assure that disclosure of Confidential Information is compartmentalized, such that all Confidential Information shall be disclosed only to those persons and entities authorized to receive such Information as an Authorized Disclosure under this Agreement and applicable Confidentiality Control Procedures. To assist Recipient in its determination of the adequacy of its Confidentiality Control Procedures, Recipient has been provided with a copy of the Port Authority's Information Security Handbook.

The Port Authority may request in writing that the Recipient or any Related Parties apply different or more stringent controls on the handling, care, storage and disclosure of particular items of Confidential Information as a precondition for its disclosure. The Port Authority may decline any request by the Recipient or any of its Related Parties to provide such item of Confidential Information if the Recipient or any of the Related Parties do not agree in writing to apply such controls.

Nothing in this Agreement shall require the Port Authority to tender or provide access to or possession of any Confidential Information to the Recipient or its Related Parties, whether or not the requirements of this Agreement are otherwise satisfied. However, if such Confidential Information is provided and accepted, the Recipient and its Related Parties shall abide by the terms, conditions and requirements of this Agreement.

The Recipient and each Related Party agrees to be responsible for enforcing the provisions of this Agreement with respect to its Related Parties, in accordance with the Confidentiality Control Procedures. Except as required by law pursuant to written advice of competent legal counsel, or with the Port Authority's prior written consent, neither the Recipient, nor any of the Related Parties shall disclose to any third party, person or entity: (i) any Confidential Information under circumstances where the Recipient is not fully satisfied that the person or entity to whom such disclosure is about to be made shall act in accordance with the Confidentiality Control Procedures whether or not such person or entity has agreed in writing to be bound by the terms of this Agreement or any

"Acknowledgement" of its terms or (ii) the fact that Confidential Information has been made available to the Recipient or such Related Parties, or the content or import of such Confidential Information. The Recipient is responsible for collecting and managing the Acknowledgments signed by Related Parties pursuant to this Agreement. Recipient shall, at the Port Authority's request, provide the Port Authority a list of all Related Parties who have signed an Acknowledgment, and copies of such Acknowledgments.

As to all Confidential Information provided by or on behalf of the Port Authority, nothing in this Agreement shall constitute or be construed as a waiver of any public interest privilege or other protections established under applicable state or federal law.

3. **Disclosures and Discovery Requests**. If a subpoena, discovery request, Court Order, Freedom of Information Request, or any other request or demand authorized by law seeking disclosure of the Confidential Information is received by the Recipient or any Related Party, Recipient shall notify the Port Authority thereof with sufficient promptness so as to enable the Port Authority to investigate the circumstances, prepare any appropriate documentation and seek to quash the subpoena, to seek a protective order, or to take such other action regarding the request as it deems appropriate. In the absence of a protective order, disclosure shall be made, in consultation with the Port Authority, of only that part of the Confidential Information as is legally required to be disclosed. If at any time Confidential Information is disclosed in violation of this Agreement, the Recipient shall immediately give the Port Authority written notice of that fact and a detailed account of the circumstances regarding such disclosure to the Port Authority.

4. **Retention Limitations; Return of Confidential Information**. Upon the earlier occurrence of either the Port Authority's written request or completion of Recipient's need for any or all Confidential Information, such Confidential Information, all writings and material describing, analyzing or containing any part of such Confidential Information, including any and all portions of Confidential Information that may be stored, depicted or contained in electronic or other media and all copies of the foregoing shall be promptly delivered to the Port Authority at Recipient's expense. In addition, as to Confidential Information that may be stored in electronic or other form, such Confidential Information shall be completely removed so as to make such Confidential Information incapable of being recovered from all computer databases of the Recipient and all Related Parties. The Recipient may request in writing that the Port Authority consent to destruction of Confidential Information, writings and materials in lieu of delivery thereof to the Port Authority. The Port Authority shall not unreasonably withhold its consent to such request. If the Port Authority consents to such destruction, the Recipient and each Related Party shall deliver to the Port Authority a written certification by Recipient and such Related Party that such Confidential Information, writings and materials have been so destroyed within such period as may be imposed by the Port Authority. Notwithstanding the foregoing, to the extent required for legal or

compliance purposes, the Recipient may retain a copy of Confidential Information, provided that (a) the Port Authority is notified in writing of such retention, and (b) Recipient continues to abide by the requirements of this Agreement with respect to the protection of such Confidential Information.

5. **Duration and Survival of Confidentiality Obligations**. The obligations under this Agreement shall be perpetual (unless otherwise provided in this Agreement) or until such time as the Confidential Information is no longer considered confidential and/or privileged by the Port Authority.

6. **Severability**. Each provision of this Agreement is severable and if a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

7. **Injunctive and Other Relief**. Recipient and each Related Party acknowledges that the unauthorized disclosure and handling of Confidential Information is likely to have a material adverse and detrimental impact on public safety and security and could significantly endanger the Port Authority, its facilities (including, without limitation, the Project site), its patrons and the general public and that damages at law are an inadequate remedy for any breach, or threatened breach, of this Agreement by Recipient or its Related Parties. The Port Authority shall be entitled, in addition to all other rights or remedies, to seek such restraining orders and injunctions as it may deem appropriate for any breach of this Agreement, without being required to show any actual damage or to post any bond or other security.

8. **Governing Law**. This Agreement shall be governed by and construed in accordance with the laws of the State of New York, without regard to conflict of laws principles. The Port Authority (subject to the terms of the Port Authority Legislation (as defined below)) and the Recipient specifically and irrevocably consent to the exclusive jurisdiction of any federal or state court in the County of New York and State of New York with respect to all matters concerning this Agreement and its enforcement. The Port Authority (subject to the terms of the Port Authority Legislation (as defined below)) and the Recipient agree that the execution and performance of this Agreement shall have a New York situs and, accordingly, they each consent (and solely with respect to the Port Authority, subject to the terms of the Port Authority Legislation (as defined below)) to personal jurisdiction in the State of New York for all purposes and proceedings arising from this Agreement. "**Port Authority Legislation**" shall mean the concurrent legislation of the State of New York and State of New Jersey set forth at Chapter 301 of the Laws of New York of 1950, as amended by Chapter 938 of the Laws of New York of 1974 (McKinney's Unconsolidated Laws §§7101-7112) and Chapter 204 of the Laws of New Jersey of 1951 (N.J.S.A. 32:1-157 to 32:1-168).

9. **Notices**. Any notice, demand or other communication (each, a "**notice**") that is given or rendered pursuant to this Agreement by either party to the other party, shall be: (i) given or rendered, in writing, (ii) addressed to the other party at its required address(es) for notices delivered to it as set forth below, and (iii) delivered by either (x) hand delivery, or (y) nationally recognized courier service (e.g., Federal Express,

Express Mail). Any such notice shall be deemed given or rendered, and effective for purposes of this Agreement, as of the date actually delivered to the other party at such address(es) (whether or not the same is then received by other party due to a change of address of which no notice was given, or any rejection or refusal to accept delivery). Notices from either party (to the other) may be given by its counsel.

The required address(es) of each party for notices delivered to it is (are) as set forth below. Each party, however, may, from time to time, designate an additional or substitute required address(es) for notices delivered to it, provided that such designation must be made by notice given in accordance with this Paragraph 0.

If to the Port Authority: _____

_____

The Port Authority of New York and New Jersey

225 Park Avenue South, __th Floor

New York, NY 10003

with a copy to: The Port Authority of New York and New Jersey

225 Park Avenue South - 15th Floor

New York, NY 10003

Attn: General Counsel

If to the Recipient: _____

_____

_____

with a copy to: _____

_____

_____

10. Entire Agreement. This Agreement contains the complete statement of all the agreements among the parties hereto with respect to the subject matter thereof, and all prior agreements among the parties hereto respecting the subject matter hereof, whether written or oral, are merged herein and shall be of no further force or effect.

This Agreement may not be changed, modified, discharged, or terminated, except by an instrument in writing signed by all of the parties hereto.

11. Counterparts. This Agreement may be executed in one or more counterparts, each of which shall be deemed to be an original, but all of which shall be one and the same document.

12. Parties Bound. This Agreement shall be binding upon the Recipient and its respective successors. The foregoing shall not be affected by the failure of any Related Party to join in this Agreement or to execute and deliver an Acknowledgement hereof.

13. Authority. The undersigned individual(s) executing this Agreement on behalf of the Recipient below represent(s) that they are authorized to execute this Agreement on behalf of the Recipient and to legally bind such party.

14. Disclosure of Ownership Rights or License. Nothing contained herein shall be construed as the granting or conferring by the Port Authority of any rights by ownership, license or otherwise in any Information.

15. No Liability. Neither the Commissioners of the Port Authority, nor any of them, nor any officer, agent or employee thereof, shall be charged personally by the Recipient with any liability, or held liable to the Recipient under any term or provision of this Agreement, or because of its execution or attempted execution or because of any breach, or attempted or alleged breach thereof.

16. Construction. This Agreement is the joint product of the parties hereto and each provision of this Agreement has been subject to the mutual consultation, negotiation, and agreement of the parties hereto, and shall not be construed for or against any party hereto. The captions of the various sections in this Agreement are for convenience only and do not, and shall not be deemed to, define, limit or construe the contents of such Sections.

[*No further text on this page; signatures appear on next page*]

IN WITNESS WHEREOF, the Recipient has executed this Agreement as of the date first above written.

Dated: New York, New York

_____ ____, _____

RECIPIENT:

_____

By: _____

Title: _____

Date: _____

EXHIBIT A

ACKNOWLEDGMENT BY RELATED PARTY ENTITY

The undersigned, _____ (name of authorized signatory), is the _____(Title) of _____ (name of entity), a _____(type of entity and jurisdiction of formation) ("**Related Party**"), located at _____ (address of entity), and is duly authorized to execute this Acknowledgment on behalf of the above Related Party. The above Related Party is involved with the functions of _____ (describe scope of work of Related Party) in connection with _____(describe Project) for The Port Authority of New York and New Jersey (the "**Port Authority**"). I acknowledge and confirm that the above named Related Party has been provided with a copy of and shall be bound and shall abide by all of the terms, requirements and conditions set forth in the Non Disclosure and Confidentiality Agreement dated _____ ____, _____, between _____ (the "**Recipient**") and the Port Authority (hereinafter the "**Agreement**"). Appropriate and responsible officers and employees of the Related Party have carefully read and understand the terms and conditions of the Agreement. The Related Party has notice and acknowledges that any breach or violation of such terms, requirements and conditions may result in the imposition of remedies or sanctions as set forth or otherwise described therein against such Related Party.

Signed: _____

Print Name: _____

Title: _____

Date: _____

ACKNOWLEDGMENT BY RELATED PARTY INDIVIDUAL

I, _____ (name of employee) ("**Related Party**"), am employed as a(n) _____(job title) by _____ (name of employer). I have been provided with and have read the Non Disclosure and Confidentiality Agreement between _____ (the "**Recipient**") and The Port Authority of New York and New Jersey (the "**Port Authority**") dated _____ ____, _____ (hereinafter the "**Agreement**".) I understand that because of my employer's relationship with _____ (name of Recipient, or the Port Authority if Related Party Individual is an employee of Recipient), both my employer and I may be provided with access to, and/or copies of, sensitive security materials or confidential information. If it is required for me to review or receive Confidential Information, as it is defined in the aforementioned Agreement, I acknowledge that I will be bound by each and every term and provision contained therein, and that failure to do so may include, but is not limited to, the imposition of disciplinary action and sanctions, and/or the institution of legal action seeking injunctive relief, monetary and/or criminal penalties for violation of law and/or Port Authority policies and procedures, as well as for violation of federal and/or state regulations.

To the extent that I am currently in the possession of, or have previously come into contact with, marked information as it relates to the aforementioned Agreement, I agree to conform my handling procedures for Confidential Information to the practices and procedures set forth and defined herein, or risk loss of access to said Information, removal from said Project and/or subjecting myself to the aforementioned disciplinary actions and/or civil and criminal penalties.

Signed: _____

Print Name: _____

Title: _____

Date: _____

APPENDIX A-3

PORT AUTHORITY/PATH EMPLOYEE NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT

THIS NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT (this "**Agreement**") is made as of this ____ day of _____, 20___, by and between THE PORT AUTHORITY OF NEW YORK AND NEW JERSEY (the "**Port Authority**") a body corporate and politic created by Compact between the States of New York and New Jersey, with the consent of the Congress of the United States, and having an office and place of business at 225 Park Avenue South, New York, New York, 10003, and _____, an employee of the Port Authority or PATH ("**Employee**"), having the Port Authority or PATH Employee Number: _____.

WHEREAS, security is of critical importance to the Port Authority in carrying out its mission and in providing a safe and secure environment for its patrons and employees, as well as properly protecting its properties, facilities and operations; and

WHEREAS, the safeguarding of confidential and sensitive information is an essential factor in the Port Authority's ability to carry out its responsibilities; and

WHEREAS, the Port Authority recognizes the need for providing its employees with access to certain information which may contain or include confidential, privileged, classified, commercial, proprietary or sensitive information, documents and plans, on a need to know and/or an as-needed basis; and

---

WHEREAS, every employee having access to Confidential Information (as hereinafter defined) has the obligation and the responsibility to properly safeguard such information and prevent its unauthorized disclosure or release.

NOW THEREFORE, Employee hereby agrees, as follows:

1. **Defined Terms.** In addition to the terms defined in the Recitals above, the following terms shall have the meanings set forth below:

a. "**Confidential Information**" means and includes collectively, Confidential Proprietary Information, Confidential Privileged Information, and Information that is labeled, marked or otherwise identified by or on behalf of the Port Authority so as to reasonably connote that such Information is confidential, privileged, sensitive or proprietary in nature. The term Confidential Information shall also include all work product that contains or is derived from any of the forgoing, whether in whole or in part.

b. "**Confidential Privileged Information**" means and includes collectively, (i) any and all Information, documents and materials entitled to protection as a public interest privilege under New York State law and as may be deemed to be afforded or entitled to the protection of any other privilege recognized under New York, and/or New Jersey state laws or Federal laws, (ii) Critical Infrastructure Information, (iii) Sensitive Security Information, and (iv) Limited Access Safety and Security Information.

c. "**Confidential Proprietary Information**" means and includes Information that contains financial, commercial, or other proprietary, business Information concerning the Port Authority or its facilities.

d. "**Critical Infrastructure Information**" (CII) has the meaning set forth in the Homeland Security Act of 2002, under the subtitle Critical Infrastructure Information Act of 2002 (6 U.S.C. §131-134), and any rules or regulations enacted pursuant thereto, including, without limitation, the Office of the Secretary, Department of Homeland Security Rules and Regulations, 6 C.F.R. Part 29 and any amendments thereto. CII may also be referred to as "Protected Critical Infrastructure Information" or "PCII," as provided for in the referenced rules and regulations and any amendments thereto.

e. "**Information**" means, collectively, all information, documents, data, reports, notes, studies, projections, records, manuals, graphs, electronic files, computer generated data or information, drawings, charts, tables, diagrams, photographs, and other media or renderings containing or otherwise incorporating information that may be provided or made accessible at any time, whether orally, visually, in writing, photographically, electronically or any other form, including, without limitation, any and all copies of the foregoing.

f. "**Limited Access Safety and Security Information**" means and includes sensitive Information, the disclosure of which would be detrimental to the public interest and might compromise public safety and/or security as it relates to Port Authority property, facilities, systems and operations, and which has not otherwise been submitted for classification or designation under any Federal laws or regulations.

g. "**Port Authority Handbook**" means The Port Authority of N.Y. & N.J. Information Security Handbook, as may be amended by the Port Authority, from time to time.

h. "**Sensitive Security Information**" has the definition and requirements set forth in the Transportation Security Administrative Rules & Regulations, 49

CFR 1520, (49 U.S.C. §114) and in the Office of the Secretary of Transportation Rules & Regulations, 49 CFR 15, (49 U.S.C. §40119) and any amendments thereto.

2. **Compliance with the Port Authority Handbook.** All Confidential Information is to be handled by the Employee with the utmost care and in a manner designed to prevent its disclosure to unauthorized third parties consistent with Port Authority security policy, practices and procedures, as set forth in the Port Authority Handbook. Employee must maintain and dispose of Confidential Information in a manner consistent with this Agreement and in conformity with the Port Authority Handbook.

3. **Use of Confidential Information.** Confidential Information provided to or obtained by Employee may only be used in the performance of duly authorized activities relating to the Employee's job duties, and may not be used for any other purpose, unless expressly authorized by this Agreement, or as expressly directed in writing by the Port Authority.

4. **Disclosure of Information.** Until such time as the Information is no longer considered Confidential by the Port Authority, and that fact is communicated to the Employee in writing, the Information must be held and treated in the strictest confidence and may not, except in accordance with Paragraph 5, below, be disclosed to any person who has not agreed to be bound by a Non-Disclosure and Confidentiality Agreement. When disclosure of such Information is permitted under these circumstances, it will only be provided to such individuals to the extent that it is necessary for that person to perform his/her duly authorized activities at or in connection with their job responsibilities and may only be provided on a need-to-know-basis. Copies of documents or materials in any form, format or medium, which contain disclosures of such Information, may only be made pursuant to the procedures established in the Port Authority Handbook.

5. **Disclosures and Discovery Requests**. If a subpoena, discovery request, Court Order, Freedom of Information Request, or any other request or demand authorized by law is received by the Employee seeking disclosure of Confidential Information, the Employee must immediately notify his/her Supervisor and Departmental Information Security Officer in order to permit the Port Authority to seek to quash the subpoena, seek a protective order, or take such other action regarding the request as it deems appropriate, and the Employee will fully cooperate in the Port Authority's efforts in this regard. If at any time Confidential Information is disclosed in violation of this Agreement, the employee will immediately report that fact and the circumstances regarding such disclosure to his/her Supervisor and Departmental Information Security Officer.

6. **Unauthorized Disclosure and Disciplinary Actions.** The unauthorized disclosure or improper handling of Confidential Information could have an adverse and detrimental impact on public safety and security and could significantly endanger the Port Authority, its operations, its facilities, its patrons and the general public. Because of this, the obligations of confidence required hereunder are extraordinary and unique, and are vital to the security and well being of the Port Authority. Any

failure to comply with, or any violation of, this Agreement, may result in legal action and/or disciplinary action against Employee.

7. **Duration and Survival of Confidentiality Obligations.** The obligations under this Agreement shall be perpetual, or until such time as the Confidential Information is no longer considered confidential and/or privileged by the Port Authority, and that fact is communicated in writing to Employee.

IN WITNESS WHEREOF, the Employee has executed this Agreement as of the date below.

Dated: New York, New York
_____ ____, 20___

EMPLOYEE:

_____

By: _____

Title: _____

Date: _____

APPENDIX B

INSTRUCTIONS ON NON-DISCLOSURE AND MAINTENANCE OF CONFIDENTIALITY OF PORT AUTHORITY CONFIDENTIAL INFORMATION

WHEREAS, security is of critical importance to the Port Authority of New York and New Jersey (the "Port Authority") in carrying out its mission and in providing a safe and secure environment for its patrons and employees, as well as properly protecting its properties, facilities and operations; and

WHEREAS, the safeguarding of certain confidential and sensitive information is an essential factor in the Port Authority's ability to carry out its responsibilities; and

WHEREAS, the Port Authority recognizes the need for providing its employees with access to certain information which may contain or include confidential, privileged, classified, commercial, proprietary or sensitive information, documents and plans, on a need to know and/or an as-needed basis; and

WHEREAS, every employee having access to Confidential Information (as hereinafter defined) has the obligation and the responsibility to properly safeguard such information and prevent its unauthorized disclosure or release; and

WHEREAS, these instructions on non-disclosure of confidential information ("Non-Disclosure Instructions" or "NDI") are intended to facilitate an employee's ability to perform his or her job, while at the same time ensuring the security of such Confidential Information.

ACCORDINGLY, You, as the employee-recipient of these Instructions ("Employee"), are hereby informed that:

1. **Defined Terms.** In addition to the terms defined in the Recitals above, the following terms shall have the meanings set forth below:

a. "**Confidential Information**" means and includes collectively, Confidential Proprietary Information, Confidential Privileged Information, and Information that is labeled, marked or otherwise identified by or on behalf of the Port Authority so as to reasonably connote that such Information is confidential, privileged, sensitive or proprietary in nature. The term Confidential Information shall also include all work product that contains or is derived from any of the forgoing, whether in whole or in part.

b. "**Confidential Privileged Information**" means and includes collectively, (i) any and all Information, documents and materials entitled to protection as a public interest privilege under New York State law and as may be deemed to be afforded or entitled to the protection of any other privilege recognized under New York, and/or New Jersey state laws or Federal laws, (ii) Critical Infrastructure Information, (iii) Sensitive Security Information, and (iv) Limited Access Safety and Security Information.

c. "**Confidential Proprietary Information**" means and includes Information which contains financial, commercial, or other proprietary, business Information concerning the Port Authority or its facilities.

d. "**Critical Infrastructure Information**" (CII) has the meaning set forth in the Homeland Security Act of 2002, under the subtitle Critical Infrastructure Information Act of 2002 (6 U.S.C. §131-134), and any rules or regulations enacted pursuant thereto, including, without limitation, the Office of the Secretary, Department of Homeland Security Rules and Regulations, 6 C.F.R. Part 29 and any amendments thereto. CII may also be referred to as "Protected Critical Infrastructure Information" or "PCII," as provided for in the referenced rules and regulations and any amendments thereto.

e. "**Information**" means, collectively, all information, documents, data, reports, notes, studies, projections, records, manuals, graphs, electronic files, computer generated data or information, drawings, charts, tables, diagrams, photographs, and other media or renderings containing or otherwise incorporating information that may be provided or made accessible at any time, whether orally, visually, in writing, photographically, electronically or any other form, including, without limitation, any and all copies of the foregoing.

f. "**Limited Access Safety and Security Information**" means and includes sensitive Information, the disclosure of which would be detrimental to the public interest and might compromise public safety and/or security as it relates to Port Authority property, facilities, systems and operations, and which has not otherwise been submitted for classification or designation under any Federal laws or regulations.

g. "**Port Authority Handbook**" means The Port Authority of N.Y. & N.J. Information Security Handbook.

h. "**Sensitive Security Information**" has the meaning set forth in the Transportation Security Administrative Rules & Regulations, 49 CFR 1520,

(49 U.S.C. §114) and in the Office of the Secretary of Transportation Rules & Regulations, 49 CFR 15, (49 U.S.C. §40119) and any amendments thereto.

2. **Compliance with the Port Authority Handbook.** All Confidential Information is to be handled by the Employee with the utmost care and in a manner designed to prevent its disclosure to unauthorized third parties consistent with Port Authority security policy, practices and procedures, as set forth in the Port Authority Handbook. Employee must maintain and dispose of Confidential Information in a manner consistent with this Agreement and in conformity with the Port Authority Handbook.

3. **Use of Confidential Information.** Confidential Information provided to or obtained by Employee may only be used in the performance of duly authorized activities relating to the Employee's job duties, and may not be used for any other purpose, unless expressly authorized by this Agreement, or as expressly directed in writing by the Port Authority.

4. **Disclosure of Information.** Until such time as the Information is no longer considered Confidential by the Port Authority, and that fact is communicated to the Employee in writing, the Information must be held and treated in the strictest confidence and may not, except in accordance with Paragraph 5, below, be disclosed to any person who has not agreed to be bound by a Non-Disclosure and Confidentiality Agreement, or who has not been given these Non-Disclosure Instructions. When disclosure of such Information is permitted under these circumstances, it will only be provided to such individuals to the extent that it is necessary for that person to perform his/her duly authorized activities at or in connection with their job responsibilities and may only be provided on a need-to-know-basis. Copies of documents or materials in any form, format or medium, which contain disclosures of such Information, may only be made pursuant to the procedures established in the Port Authority Handbook.

5. **Disclosures and Discovery Requests**. If a subpoena, discovery request, Court Order, Freedom of Information Request, or any other request or demand authorized by law is received by the Employee seeking disclosure of Confidential Information, the Employee must immediately notify his/her Supervisor and Departmental Information Security Officer in order to permit the Port Authority to seek to quash the subpoena, seek a protective order, or take such other action regarding the request as it deems appropriate, and the Employee will fully cooperate in the Port Authority's efforts in this regard. If at any time Confidential Information is disclosed in violation of this Agreement, the employee will immediately report that fact and the circumstances regarding such disclosure to his/her Supervisor and Departmental Information Security Officer.

6. **Unauthorized Disclosure and Disciplinary Actions.** The unauthorized disclosure or improper handling of Confidential Information could have an adverse and detrimental impact on public safety and security and could significantly endanger the Port Authority, its operations, its facilities, its patrons and the general public. Because of this, the obligations of confidence required hereunder are extraordinary and unique, and are vital to the security and well being of the Port Authority.

Accordingly, you are further instructed that your failure to comply with these Non-Disclosure Instructions may result in legal action and/or disciplinary action being taken against you.

7. **Duration and Survival of Confidentiality Obligations.** The obligations in these Non-Disclosure Instructions shall be perpetual, or until such time as the Confidential Information is no longer considered confidential and/or privileged by the Port Authority, and that fact is communicated in writing to Employee.

COPY PROVIDED TO:

_____

By: _____

Title: _____

Date: _____

APPENDIX C

Background Screening Criteria

S.W.A.C.™
Secure Worker Access Consortium

CONTENTS:

- Background Screening Specifications
- High Access Level Criteria
- Medium Access Level Criteria
- Standard Access Level Criteria

Criminal History
Background Screening Specifications

Social Security Number — Positive Identity Verification (PIV)
Federal District Court Search (each district of residence and employment)*
National Criminal Search*
Statewide Criminal Check (each state of residence and employment)*
County Criminal Search (each county of residence and employment)*
Sexual Offender Search (each resident state)*
Alien Immigrant Search
Immigration Violation Check
Fake Identification Convictions
State Driving Record
Check for material false statement or omission on application form
National Terrorist Watch List Search (OFAC-SDN)

Note* Within ten (10), seven (7), or five (5) years preceding date of application as noted on the HIGH, MEDIUM, and STANDARD Level of Clearance forms.

Level of Clearance

HIGH Secure Access Control Areas
and CONFIDENTIAL PRIVILEGED INFORMATION

I. No convictions ever in your lifetime: an individual has a disqualifying criminal offense if the individual was convicted, or found not guilty by reason of insanity, in a civilian or military jurisdiction of any of the following criminal offenses:

(1) Terrorism—A crime listed in 18 U.S.C. Chapter 113B—or a State law that is comparable.
(2) Violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. 1961, et. seq., or a State law that is comparable.
(3) A crime involving a severe transportation security incident.
(4) Making any threat, or maliciously conveying false information knowing the same to be false, concerning the deliverance, placement, or detonation of an explosive or other lethal device in or against a place of public use, a state or government facility, a public transportations system, or an infrastructure facility.
(5) Improper transportation of a hazardous material under 49 U.S.C. 5124, or a state law that is comparable;
(6) Murder.
(7) Espionage.
(8) Sedition.
(9) Treason.
(10) Unlawful possession, use, sale, distribution, manufacture, purchase, receipt, transfer, shipping, transporting, import, export, storage of, or dealing in an explosive or explosive device.
(11) Conspiracy or attempt to commit any of the criminal acts listed in paragraph I.

II. An individual has a disqualifying criminal offense if the individual was convicted, or found not guilty by reason of insanity, in a civilian or military jurisdiction, within the **past ten (10) years** from completion of sentence preceding the date of the application, of the following offenses:

(1) Forgery of certificates, false marking of aircraft, and other aircraft registration violation;
(2) Interference with air navigation;
(3) Aircraft piracy;
(4) Interference with flight crewmembers or flight attendants;
(5) Commission of certain crimes aboard aircraft in flight;
~~(6) Carrying a weapon or explosive aboard aircraft;~~
(7) Conveying false information and threats; (e.g., bomb threats, explosives in briefcase, etc. in security areas)
(8) Aircraft piracy outside the special aircraft jurisdiction of the United States;
(9) Lighting violations involving transporting controlled substances;
(10) Unlawful entry into an aircraft or airport area that serves air carriers or foreign air carriers contrary to established security requirements;
(11) Destruction of an aircraft or aircraft facility;
(12) Assault with intent to murder.
(13) Kidnapping or hostage taking.
(14) Rape or aggravated sexual abuse.
(15) Extortion.
(16) Armed or felony unarmed robbery.

(17) Distribution of, possession with intent to distribute, or importation of a controlled substance.
(18) Felony arson.
(19) Felony involving a threat.
(20) Felony involving—
  (i) Willful destruction of property;
  (ii) Importation or manufacture of a controlled substance;
  (iii) Burglary or Robbery
  (iv) Theft;
  (v) Dishonesty, fraud, or misrepresentation, including identity fraud and money laundering;
  (vi) Possession or distribution of stolen property;
  (vii) Aggravated assault;
  (viii) Bribery; or
  (ix) Illegal possession of a controlled substance punishable by a maximum term of imprisonment of more that 1 year;
  (x) Smuggling;
  (xi) Immigration violations; or
(21) Violence at international airports;
(22) Unlawful possession, use, sale, manufacture, purchase, distribution, receipt, transfer, shipping, transporting, delivery, import, export of, or dealing in a firearm or other weapon. A firearm or other weapon includes, but is not limited to, firearms as defined in 18 U.S.C. 921(a)(3) or 26 U.S.C.5 845(a), or items contained on the U.S. Munitions Import List at 27 CFR 447.21.
(23) Conspiracy or attempt to commit any of the criminal acts listed in paragraph II.

Under want, warrant, or indictment. An applicant who is wanted, or under indictment in any civilian or military jurisdiction for a felony listed in section II, is disqualified until the want or warrant is released or the indictment is dismissed.

Level of Clearance

Up To MEDIUM Secure Access Control Areas and CONFIDENTIAL INFORMATION

I. No convictions ever in your lifetime: an individual has a disqualifying criminal offense if the individual was convicted, or found not guilty by reason of insanity, in a civilian or military jurisdiction of any of the following criminal offenses:

(1) Terrorism—A crime listed in 18 U.S.C. Chapter 113B—or a State law that is comparable.

(2) Violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. 1961, et. seq., or a State law that is comparable.

(3) A crime involving a severe transportation security incident.

(4) Making any threat, or maliciously conveying false information knowing the same to be false, concerning the deliverance, placement, or detonation of an explosive or other lethal device in or against a place of public use, a state or government facility, a public transportations system, or an infrastructure facility. (3) Improper transportation of a hazardous material under 49 U.S.C. 5124, or a state law that is comparable;

(5) Improper transportation of a hazardous material under 49 U.S.C. 5124, or a state law that is comparable;

(6) Murder.

(7) Espionage.

(8) Sedition.

(9) Treason.

(10) Unlawful possession, use, sale, distribution, manufacture, purchase, receipt, transfer, shipping, transporting, import, export, storage of, or dealing in an explosive or explosive device.

(11) Conspiracy or attempt to commit any of the criminal acts listed in paragraph I.

II. An individual has a disqualifying criminal offense if the individual was convicted, or found not guilty by reason of insanity, in a civilian or military jurisdiction for the following offenses, within the **past ten (10) years** from completion of sentence for the offense preceding the date of the application:

(1) Extortion.

(2) Armed or felony unarmed robbery.

(3) Felony involving—

(i) Importation or manufacture of a controlled substance;

(ii) Burglary or Robbery;

(iii) Theft;

(iv) Dishonesty, fraud, or misrepresentation, including identity fraud and money laundering;

(v) Possession or distribution of stolen property;

(vi) Bribery; or

(4) Conspiracy or attempt to commit any of the criminal acts listed in paragraph II.

Under want, warrant, or indictment. An applicant who is wanted, or under indictment in any

civilian or military jurisdiction for a felony listed in section II, is disqualified until the want or warrant is released or the indictment is dismissed.

III. An individual has a disqualifying criminal offense if the individual was convicted, or found not guilty by reason of insanity, in a civilian or military jurisdiction for the following offenses, within the **past seven (7) years** from completion of sentence for the offense preceding the date of the application:

(1) Assault with intent to murder.

(2) Kidnapping or hostage taking.

(3) Rape or aggravated sexual abuse.

(4) Distribution of, possession with intent to distribute, or importation of a controlled substance.

(5) Felony arson.

(6) Felony involving a threat.

(7) Felony involving—

- (i) Willful destruction of property;
- (ii) Aggravated assault;
- (iii) Smuggling;
- (iv) Immigration violations;

(8) Violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. 1961, et. seq., or a State law that is comparable, other than the violations listed in paragraph (b) of Section I.

(9) Unlawful possession, use, sale, manufacture, purchase, distribution, receipt, transfer, shipping, transporting, delivery, import, export of, or dealing in a firearm or other weapon. A firearm or other weapon includes, but is not limited to, firearms as defined in 18 U.S.C. 921(a)(3) or 26 U.S.C.5 845(a), or items contained on the U.S. Munitions Import List at 27 CFR 447.21.

(10) Conspiracy or attempt to commit any of the criminal acts listed in paragraph III.

Under want, warrant, or indictment. An applicant who is wanted, or under indictment in any civilian or military jurisdiction for a felony listed in section III, is disqualified until the want or warrant is released or the indictment is dismissed.

Level of Clearance

Up To STANDARD
Secure Access Control Areas

I. No convictions ever in your lifetime: an individual has a disqualifying criminal offense if the individual was convicted, or found not guilty by reason of insanity, in a civilian or military jurisdiction of any of the following criminal offences:

(1) Terrorism —A crime listed in 18 U.S.C. Chapter 113B—or a State law that is comparable.

(2) Violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. 1961, et. seq., or a State law that is comparable.

(3) Espionage.

(4) Sedition.

(5) Treason.

(6) Unlawful possession, use, sale, distribution, manufacture, purchase, receipt, transfer, shipping, transporting, import, export, storage of, or dealing in an explosive or explosive device.

(7) Conspiracy or attempt to commit any of the criminal acts listed in paragraph I.

II. An individual has a disqualifying criminal offense if the individual was convicted, or found not guilty by reason of insanity, in a civilian or military jurisdiction for the following offenses, within the **past ten (10) years** from completion of sentence for the offense preceding the date of the application:

(1) Extortion.

(2) Felony involving—

(i) Theft;

~~(ii) Dishonesty, fraud or misrepresentation, including identity fraud and money~~ laundering;

(iii) Unlawful sale, distribution, manufacture, import or export of a controlled substance that resulted in the conviction of an A Felony in the New York State Penal Law, or any comparable law in any State, or comparable Federal law.

(3) Conspiracy or attempt to commit any of the criminal acts listed in paragraph II.

III. An individual has a disqualifying criminal offense if the individual was convicted, or found not guilty by reason of insanity, in a civilian or military jurisdiction for the following offenses, within the **past five (5) years** from completion of sentence for the offense preceding the date of the application:

(1) Violent Felony Offenses (as defined in the New York State Penal Law §70.02) or any comparable law in any State.

(2) Conspiracy or attempt to commit any criminal act listed in paragraph III.

APPENDIX D

Secure Worker Access Consortium (S.W.A.C.)

Secure Worker Access Consortium (S.W.A.C.) is accessed by an online application that enables the secure collection, processing, maintenance and real-time positive identity verification (PIV) of individuals. As of January 29, 2007, S.W.A.C. is the only Port Authority approved provider to be used to conduct background screening, except as otherwise required by federal law and or regulation. Additional information about S.W.A.C., corporate enrollment, online applications, and location of processing centers can be found at http://www.secureworker.com, or S.W.A.C. may be contacted at (877) 522-7922.

o Consultants / Contractors

- Step 1: - A firm representative completes the Corporate Membership Application Form online at www.secureworker.com. Firms are encouraged to establish a Corporate Membership Account through which their workers will be processed.
- Step 1a: Employees & Workers of Contractors — Individual completes the Individual Membership Application Form online. (A company administrator may complete this form on someone's behalf.)
- Step 2: The applicant is photographed, provides a digital signature and presents the required identification documents at an operational S.W.A.C. Processing Center.
- Step 3: S.W.A.C. ID Card is available for pickup. The typical length of the process is one week. To verify that an ID Card is ready for pickup, call (877) 522-7922.

o Individuals

- Go to any operational S.W.A.C. Processing Center and the agent will assist you through the application process. A method of payment will be required. Required identification documents will need to be presented.

- **S.W.A.C. Processing Centers** - check the S.W.A.C. website to verify the locations, and days and times of operation of the Processing Centers.

George Washington Bridge Port Authority Administration Building, Main Lobby
220 Bruce Reynolds Boulevard
Bridge Plaza South
Fort Lee, NJ 07024
Tuesdays, 6:00 AM to 12:00PM

John F. Kennedy International Airport
Building #14
RE's Office Conference Room
Jamaica, NY
* Fridays, 6:00AM to 12:00PM

Port Authority Bus Terminal
625 Eighth Avenue (at 40th Street)
South Wing, 2nd Floor
New York, NY 10018
Tuesdays, 6:00AM to 12:00PM

Port Ivory Marine Terminal
40 Western Avenue
(near the Goethels Bridge)
RE's office - 1st Floor
Staten Island, NY 10303
Tuesdays, 6:00AM to 12:00PM

LaGuardia Airport (LGA)
Port Authority Administration Building
Hanger #7S, 2nd Floor
Flushing, NY 11371
Wednesdays, 6:00AM to 12:00PM

Newark Liberty International Airport (EWR)
70 Brewster Road
Building #70 Lobby
Newark, NJ 07114
Mondays & Thursdays, 7:30AM to 3:30PM

Journal Square Transportation Center (JSTC)
One PATH Plaza
Concourse Level
(to right of EXCEL Federal Savings)
Jersey City, NJ 07306
Monday, Wednesday, and Friday, 7:30AM to 1:30PM.

World Trade Center
65 Trinity Place
(corner of Exchange Alley, across from SYMS clothing store)
New York, NY 10006
Monday through Friday, 6:00 AM to 12:00 PM

APPENDIX E

[insert department name] DEPARTMENT

PORT AUTHORITY OF NY & NJ

CONFIDENTIAL PRIVILEGED INFORMATION

"WARNING": The attached is the property of The Port Authority of New York and New Jersey (PANYNJ). It contains information requiring protection against unauthorized disclosure. The information contained in the attached document cannot be released to the public or other personnel who do not have a valid need to know without prior written approval of an authorized PANYNJ official. The attached document must be controlled, stored, handled, transmitted, distributed and disposed of according to PANYNJ Information Security Policy. Further reproduction and/or distribution outside of the PANYNJ are prohibited without the express written approval of the PANYNJ.

At a minimum, the attached will be disseminated only on a need to know basis and when unattended, will be stored in a locked cabinet or area offering sufficient protection against theft, compromise, inadvertent access and unauthorized disclosure.

Document Control Number: CP-[insert dept acronym]- [insert year]-[insert sequential number] – [insert copy number]

APPENDIX F

[insert address of Receipient]

Date:

From:

The [insert department, division or project name] is providing a copy of the following items to (insert recipient's name and address).

Description	Date	Copy Number
Describe item	00/00/00	CP-[dept abbreviation]-XX-XX-XX

Upon receipt, the items listed above must be safeguarded in accordance with the procedures identified in the "The Port Authority of New York & New Jersey Information Security Handbook " dated October 15, 2008.

PLEASE SIGN AND RETURN TO:

Document Control
[insert Port Authority department, division or unit]
Attn: [SIM or SPM}
[Address]

I acknowledge receipt of the above items listed above and accept full responsibility for the safe handling, storage and transmittal elsewhere of these items.

Name (PRINT): _____

Organization: _____

Signature: _____

Date: _____

Title: _____

APPENDIX G

GUIDELINES FOR THE STORAGE OF CONFIDENTIAL INFORMATION

I. GENERAL

This section describes the preferred methods for the physical protection of Confidential Information in the custody of PANYNJ personnel and their contractors, consultants, architects, engineers, et al. Where these requirements are not appropriate for protecting specific types or forms of such material, compensatory provisions shall be developed and approved by the Chief Information Security Officer (CISO). Nothing in this guideline shall be construed to contradict or inhibit compliance with any applicable law, statute or code. Cognizant Security Information Managers (SIM) shall work to meet appropriate security needs according to the intent of this guideline and at acceptable cost.

II. CONFIDENTIAL INFORMATION STORAGE

A. Approved Containers

The following storage containers are approved for storage of PANYNJ Confidential Information:

1. A safe or safe-type steel file container that has a built-in three- position dial combination lock or electronic combination lock.

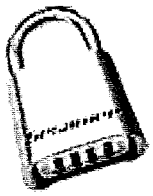
2. Any steel file cabinet that has four sides and a top and bottom (all permanently attached by welding, rivets or peened bolts so the contents cannot be removed without leaving visible evidence of entry) and is secured by a rigid metal lock bar and an approved key operated or combination padlock. The keepers of the rigid metal lock bar shall be secured to the cabinet by welding, rivets, or bolts so they cannot be removed and replaced without leaving evidence of the entry. The drawers of the container shall be held securely so their contents cannot be removed without forcing open the drawer.

B. Approved Locks and Locking Devices

The following locks and locking devices are approved for storage of PANYNJ Confidential Information:

1. Any restricted keyway 7-pin tumbler lock or equivalent pick resistant lock where the keys are clearly marked "Do Not Duplicate."

2. A combination padlock such as a Sesamee four-position dial padlock. See photo at right.



C. Combinations to Security Containers, Cabinets, and Vaults

Only a minimum number of authorized persons shall have knowledge of combinations to authorized storage containers. Containers shall bear no external markings indicating the level of material authorized for storage therein.

1. A record of the names of persons having knowledge of the combination shall be maintained.

2. Security containers, vaults, cabinets, and other authorized storage containers shall be kept locked when not under the direct supervision of an authorized person entrusted with the contents.

3. The combination shall be safeguarded in accordance with the same protection requirements as the Confidential Information contained within.

4. If a record is made of a combination, the record shall be marked with the category of material authorized for storage in the container, i.e. CP or SSI.

D. Changing Combinations

Combinations shall be changed by a person authorized access to the contents of the container, or by the SIM or his or her designee. Combinations shall be changed as follows:

1. The initial use of an approved container or lock for the protection of Confidential Information.

2. The termination of employment of any person having knowledge of the combination, or when the Confidential Information access granted to any such person has been withdrawn, suspended, or revoked.

3. The compromise or suspected compromise of a container or its combination, or discovery of a container left unlocked and unattended.

4. At other times when considered necessary by the SIM or CISO.

E. Supervision of Keys and Padlocks

Use of key-operated padlocks are subject to the following requirements:

1. A key and lock custodian shall be appointed to ensure proper custody and handling of keys and locks used for protection of Confidential Information.

2. A key and lock control register shall be maintained to identify keys for each lock and their current location and custody.

3. Keys shall be inventoried with each change of custody.

4. Keys and spare locks shall be protected equivalent to the level of classified material involved.

5. Locks shall be replaced after loss or compromise of their operable keys.

6. Making master keys is prohibited.

F. Document Retention Areas

Due to the volume of the Confidential Information in possession, or for operational necessity, it may be necessary to construct Document Retention Areas for storage because approved containers or safes are unsuitable or impractical. Access to Document Retention Areas must be controlled to preclude unauthorized access. During hours of operation this may be accomplished through the use of a cleared person or by an approved access control device or system. Access shall be limited to authorized persons who have an NDA on file, received appropriate training on the protection of information and have a bonafide need-to-know for the Confidential Information material/information within the area. All other persons (i.e. visitors, maintenance, janitorial, etc.) requiring access shall be escorted at all times by an authorized person where inadvertent or unauthorized exposure to Confidential Information cannot otherwise be effectively prevented. During

non-working hours and during working hours when the area is unattended, admittance to the area shall be controlled by locked entrances and exits secured by either an approved built-in combination lock, an automated access control system or an approved key-operated lock. Doors secured from the inside with an emergency panic bar will not require additional locking devices.

G. Construction Requirements for Document Retention Areas

This paragraph specifies the minimum safeguards and standards required for the construction of Document Retention Areas that are approved for use for safeguarding Confidential Information. These criteria and standards apply to all new construction and reconstruction, alterations, modifications, and repairs of existing areas. They will also be used for evaluating the adequacy of existing areas.

1. **Hardware:** Only heavy-gauge hardware shall be used in construction. Hardware accessible from outside the area shall be peened, pinned, brazed, or spot welded to preclude removal.

2. **Walls:** Construction may be of material offering resistance to, and evidence of, unauthorized entry into the area. If insert-type panels are used, a method shall be devised to prevent the removal of such panels without leaving visual evidence of tampering.

3. **Windows:** During nonworking hours, the windows shall be closed and securely fastened to preclude surreptitious entry.

4. **Doors:** Doors shall be constructed of material offering resistance to and detection of unauthorized entry. When doors are used in pairs, an astragal (overlapping molding) shall be installed where the doors meet.

5. **Ceilings:** Where surrounding walls do not extend to the true ceiling, the ceiling shall either be hard capped with the same construction materials as the surrounding walls or removable tiles shall be clipped in place such that they cannot be removed without destroying tiles and providing evidence of intrusion.

APPENDIX H

GUIDELINES FOR THE DISPOSAL AND DESTRUCTION OF CONFIDENTIAL INFORMATION.

I. GENERAL

This section describes the preferred methods for the disposal and destruction of Confidential Information in the custody of PANYNJ personnel and their contractors, consultants, architects, engineers, et al. Where these requirements are not appropriate for disposal or destruction of specific types or forms of such material, compensatory provisions shall be developed and approved by the Chief Information Security Officer (CISO). Cognizant Security Information Managers (SIM) shall work to meet appropriate security needs according to the intent of this guideline and at acceptable cost.

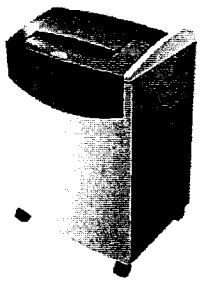
Confidential Information no longer needed shall be processed for appropriate archiving or disposal. Confidential Information approved for destruction shall be destroyed in accordance with this section. The method of destruction must preclude recognition or reconstruction of the Confidential Information or material.

All persons in possession of Confidential materials shall establish procedures for review of their Confidential holdings on a recurring basis to reduce these inventories to the minimum necessary for effective and efficient operations. Multiple copies, obsolete material, and Confidential waste shall be destroyed as soon as practical after it has served its purpose. Any appropriate downgrading actions shall be taken on a timely basis to reduce the volume and to lower the level of Confidential material being retained.

II. DISPOSAL AND DESTRUCTION

A. Destruction Requirements

All persons in possession of Confidential materials shall destroy this material in their possession as soon as possible after it has served the purpose for which it was released, developed or prepared, or as soon as possible after its designated retention period has expired.



B. Methods of Destruction

1. Generally, Confidential material shall be destroyed by commercial grade cross cut shredders located conveniently throughout the workplace for use by authorized individuals. Shred size shall not exceed 5/32" x 1 1/8".

2. Additionally, Confidential material may be destroyed by burning, pulping, melting, mutilation, chemical decomposition, or pulverizing (for example, hammer mills, choppers, and hybridized disintegration equipment) where shredding may not be appropriate. Whatever method is employed must preclude recognition or reconstruction of the Confidential Information or material.

3. Confidential material in microform, that is: microfilm, microfiche, or similar high data density material, may be destroyed by burning or chemical decomposition, or other methods as approved by the CISO.

4. Commercial destruction facilities may be used only with the approval of, and under conditions prescribed by, the SIM. When commercial destruction facilities are utilized, they shall conform to all appropriate sub-contracting requirements to include appointment of a SIM, adherence to the requirements of the PANYNJ Information Security Handbook, receiving required security training and properly executing a Non-Disclosure and Confidentiality Agreement (NDA).

5. Electronically Stored Confidential Information must be deleted from all computer hard drives, tapes, CD's, DVD's, memory, and/or magnetic, analog, or digital media used to store or transport digital files. The device used to store or transport any Confidential file will require a bit-by-bit overwrite of the storage area used by the file. This overwrite process will write random data to each data byte that was previously occupied by Confidential Information, and will do so a minimum of seven (7) times. This will protect against having the deleted file recovered using data recovery tools. Commercial tools are available to automate this process.

C. Witness to Destruction

Confidential material shall only be destroyed by authorized personnel, whether in-house or contracted, who meet all of the PANYNJ criteria for awarding access authorization, have met all training requirements, have a properly executed NDA on file and have a full understanding of their responsibilities to ensure proper control of the materials while in their possession and complete destruction thereof.

D. Destruction Records

Confidential Information is accountable and therefore any disposal in approved waste containers or destruction via convenience shredders must be reported to the issuing SIM, or his/her document control representative, indicating which documents were disposed/destroyed and the date of such action.

Confidential waste shall be destroyed as soon as practical. This applies to all waste material containing Confidential Information. Pending destruction, Confidential waste shall be appropriately safeguarded. (See also Appendix G - Guidelines for the Storage of Confidential Information.)

III. CONFIDENTIAL WASTE

A. Approved Receptacles

1. Receptacles utilized to accumulate Confidential waste shall be constructed of substantial materials that would provide evidence of tampering. Hinges and lids shall not be removable while the container is secured without leaving evidence thereof.

2. All such receptacles shall be clearly identified as containing Confidential material.

3. Slots shall be provided in such receptacles that allow for easy deposit of materials for destruction but preclude removal of deposited waste by insertion of a person's hand or tool.

4. Locks, and the control thereof, on all Confidential waste receptacles shall meet or exceed the requirements of the PANYNJ Guideline for Storage of Confidential Information.

B. Oversize Waste Materials

PANYNJ projects often involve large drawings and other materials associated with construction projects, which cannot be conveniently disposed of via office shredders or placed in typical slots on secure trash receptacles. In no cases shall such material be permitted to be placed or accumulate adjacent to secure receptacles while awaiting destruction. Oversize materials awaiting destruction may be stored as follows:

1. Within an approved Document Retention Area.

2. Within a specially constructed secure waste receptacle where disposal slots have been specifically designed for accepting rolled drawings or other oversize materials and preclude the removal there from.

3. Within a standard secure waste receptacle where the receptacle has been opened by an authorized individual to allow placement of the oversized item(s) into the container and it has been secured thereafter.

APPENDIX I

Audit Procedures

COMPANY / ORGANIZATION

- Is the Company Non-Disclosure and Confidentiality Agreement properly executed and maintained in current status?
- Has a senior management official been designated as Security Information Manager (SIM), as required by the Handbook for Protecting Security Information? Has a deputy SIM been identified?

ACCESS AUTHORIZATIONS

- Has a Non-Disclosure Agreement been executed by each employee who has been afforded access?
- Is a current record maintained of all employees authorized access to Confidential Information at the firm?
- Does the contractor provide a roster of all cleared employees to the PA as required? Is it current?

SECURITY EDUCATION

- Does the contractor provide that all employees who have access to Confidential Information with security training and briefings commensurate with their involvement with the information?
- Are contractors who employ persons at other locations ensuring the required security training?
- Are the Non-Disclosure Agreements executed by employees prior to accessing the sensitive information?
- Do initial security briefings contain the minimum required information?
- Does the contractor's security education program include refresher security briefings?
- Are employees debriefed at the time of a termination, reassignment or project's completion regarding the requirements for continued safeguarding of Confidential

Information?

- Has the contractor established internal procedures that ensure authorized awareness of their responsibilities for reporting pertinent information to the SIM?
- Has the contractor established a graduated scale of administrative disciplinary action to be applied against employees who violate the Handbook?
- Are employees aware of Emergency Procedures?
- Does management support the program for safeguarding Port Authority Confidential and Privileged Security Information?

STANDARD PRACTICE PROCEDURES

- Is the Confidential Information Practice and Procedures ("CIPP") document current and does it adequately implement the requirements of the Handbook?
- A CIPP only needs to be prepared when the Departmental Information Security Officer ("DISO") believes it necessary for the proper safeguarding of Confidential Information.

SUBCONTRACTING

- Have all Subcontractors properly executed the Non-Disclosure and Confidentiality Agreement?
- Has a Non-Disclosure Agreement been executed by each of the Subcontractor's employees who has been afforded access?
- Is a current roster maintained of all Subcontractor employees authorized access to Confidential Information at the firm?
- Does the Subcontractor provide this roster to the Prime Contractor's SIM as required? Is it current? Does it include the date that the agreement was signed? Is it included in the Prime Contractor's Team Roster?
- Does the contractor complete all actions required in the Handbook prior to release or disclosure of Port Authority Confidential Information to subcontractors? Has the Subcontractor been provided a Handbook?
- Has a senior management official of the Subcontractor been designated as the Security Information Manager (SIM), if required by a CIPP?

- Has a deputy SIM been identified?
- Is the safeguarding capability of all subcontractors determined as required?
- Is the requirement to abide by security procedures identified in the Handbook incorporated into each subcontract?
- Does the Subcontractor have an adequate understanding of the Handbook's requirements and the types of information that require safeguarding?

VISIT CONTROL

- Are procedures established to ensure positive identification of visitors prior to disclosure of Confidential Information?

CLASSIFICATION

- Does the contractor have adequate procedures for evaluating Confidential material being created, extracted, or summarized?
- Is contractor-developed Confidential Information appropriately marked, and protected?

PUBLIC RELEASE

- Does the contractor obtain the approval of the Port Authority prior to public disclosure of *ANY* information pertaining to a security program contract?

STORAGE

- Has the contractor established a system of security checks at the close of each working day to ensure that sensitive material is secured?
- How would the Confidential material be safeguarding during an emergency?
- Is a record of the names of persons having knowledge of the combinations to security containers maintained?
- When combinations to containers are placed in written form, are they stored appropriately?
- Do authorized persons, when required, change combinations to security

containers?

MARKINGS

- Is all Confidential material, regardless of its physical form, marked properly?
- Is all Confidential material marked to show the name and address of the facility responsible for its preparation and the date of preparation?
- Are overall markings marked conspicuously as required?
- Are protective markings applied to Confidential compilations if required?

TRANSMISSION

- Is Confidential Information properly prepared for transmission outside the facility?
- Are Transmittal Receipts included with Confidential Information if required?
- Is a suspense system established to track transmitted documents until the signed receipt is returned?
- Are authorized methods used to transmit Confidential material outside the facility?
- Is the NDA of the receiving facility determined prior to transmission of Confidential Information?

CONFIDENTIAL INFORMATION CONTROLS

- Do contractor employees understand their safeguarding responsibilities?
- Is the contractor's accountability system capable of facilitating the retrieval and disposition of Confidential material as required?
- Are external receipts and dispatch records maintained as required?
- Is all Confidential material received at the contractor facility and delivered directly to designated personnel?

- Do contractor employees promptly report the loss, compromise, or suspected compromise of Confidential Information to the SIM?

DISPOSITION

- Is a program established to review Confidential retention on a recurring basis for the purpose of reduction?
- Is Confidential material destroyed as soon as possible after it has served its purpose?
- Does the contractor employ an effective method of destruction?
- Is Confidential material destroyed by the appropriate employees?
- Is Confidential waste properly safeguarded until its timely destruction?

REPRODUCTION

- Does the facility's reproduction control system keep reproduction of Confidential material to a minimum?
- Is the reproduction of Confidential Information accomplished only by properly authorized, and knowledgeable employees?
- Is reproduction authorization obtained as required?
- Are reproductions of Confidential material reviewed to ensure that the markings are proper and legible?

AUTOMATED INFORMATION SYSTEMS (AIS)

- Are appropriate physical controls being exercised over approved AIS?
- Are AIS media containing Confidential Information handled in a manner consistent with the handling of Confidential documents?
- Are all AIS storage media, internal memory, and equipment, that contain Confidential Information, properly sanitized prior to removal from protection?

Suggested Questions When Interviewing Employees NOT Authorized Access to Confidential Information:

- What is Confidential Information?
- Have you ever seen Confidential Information?
- If you found Confidential Information unprotected, what would you do?

Suggested Questions When Interviewing Employees Authorized Access to Confidential Information:

- What is your job title/responsibility?
- Which contract or program requires you to access this information?
- How do you access the information?
- How long have you been authorized access?
- When was your last access to Confidential Information?
- Have you ever had access to Confidential Information outside of this facility?
- Did anyone else from the facility accompany you?
- Did you take any Confidential notes or Confidential Information back to the facility?
- What procedures were followed to protect this information?
- Where is this information now?
- Have you ever provided access to Confidential Information to visitors?
- How did you determine their need-to-know?
- Have you ever been approached by anyone requesting Confidential Information?
- Do you ever work overtime and access Confidential Information?
- When was the last time that you had a security briefing?
- What can you recall from this briefing?
- Have you ever been cited for a security violation?
- What would YOU do if YOU committed a security violation or discovered one?
- Do you have the combination to any storage containers?

- Who other than yourself has access to these containers?
- Is a record maintained of the safe combination? If so, where?
- Do you reproduce or generate Confidential Information?
- Where do you typically work when you generate Confidential Information?
- What procedures do you follow to protect Confidential Information while working on it?
- Do you ever use a computer to generate Confidential Information? How do you mark this Information?
- Please produce the guidance that you used. Is it accurate?
- What procedures do you employ when hand carrying Confidential material?
- Have you reproduced Confidential Information? Describe the procedures.
- Have you destroyed Confidential Information? What procedures were used?
- Do you have any questions regarding security?

ATTACHMENT H – CUSTOMER CARE REQUIREMENTS

The Authority is interested in evaluating proposals from contractors willing to rise to the challenge of providing the services as described herein, as further described in the RFP and Form of Contract, and to become an important member of the Airport community, dedicated to meeting and exceeding the needs of the Airport's customers.

The Port Authority has established a policy that proactive, responsive, respectful and helpful customer service is of the utmost importance. This policy not only extends to all Port Authority employees and contractors, but also includes the companies (airport partners) whose staffs have direct customer contact while providing services at the airports. Many of the employees providing the services under this Agreement are involved directly with the Airport's customers. The demeanor and attitude of the Contractor's employees, including supervisory staff, will leave customers with a lasting impression of the Airports.

The Port Authority conducts ongoing customer satisfaction surveys that identify Courtesy *, Professionalism and Security Awareness of Airport Employees, Signs and Directions, Facility Cleanliness and Condition, Quality and Variety of Food, Beverage and Retail Services, Gate Area Experience and Airport Access as the current drivers of customer satisfaction, and that recognize improvements in those areas would maximize any efforts in exceeding customers' expectations. At its sole expense, the Port Authority currently retains independent third party contractors to conduct a quality assurance program of random surveys and inspections to measure performance consisting of, but not limited to, the "Mystery Shopper Program", the "Annual Terminal-by-Terminal Quality Assurance Program" and the "Annual Terminal-by-Terminal Survey Program", hereinafter referred to as the "Programs". The Programs elicit information on staff courtesy* and helpfulness, cleanliness and condition of the facilities and equipment, staff appearance and such other measures of performance and compliance with standards referenced in the "Airport Customer Care Service Standards" manual as exhibited elsewhere in this document. Additionally, the Programs will be conducted by persons trained by the independent contractor who shall base their evaluations on both their interactions with and observations of the contractor's staff, operations and facilities.

In order to ensure that contractors provide excellent performance and customer care service, the Contractor must clearly demonstrate to the satisfaction of the Port Authority, that it will meet and exceed expectations with respect to performance under this Contract through the understanding and adoption of the following:

*Courtesy as used in this section shall encompass employee attitude, appearance, awareness and knowledge.

A. Airport Customer Care Service Standards

The Port Authority has committed to an aggressive, on-going service improvement campaign to ensure that staff provides levels of service that consistently exceed customer expectations. With input from its airport partners, the Port Authority has adopted Airport Customer Care Service Standards that identify the aspects of airport services that impact customer satisfaction and provide a means by which the services provided can be measured. The Contractor shall be responsible for, and take all necessary measures to ensure compliance by all staff with all applicable sections of the most recent edition of the attached Airport Standards Manual.

B. Customer Care Program

Delivering a consistent quality of service within an airport is a challenging task, since most of the process steps are planned and carried out by individual companies, following their internal regulations, philosophy and identity. To minimize any differences that may compromise the delivery of services at the airports, the Port Authority has adopted a mission statement set forth in the Section entitled Contract Mission and Compliance and expects every "airport partner" to share in that principle.

One of the key goals of the Port Authority is to demonstrate the value of customer service orientation throughout the entire Airport operation. Hence, the Port Authority's aim is to involve all employees who are in direct contact with the public. *A team approach is* required to develop a program that enables the Port Authority to create a common philosophy, language and set of behaviors for all companies and their employees concerning courtesy at the airports.

To help achieve service excellence, the Port Authority continues to refine the customer care program by developing; (1) customer care training modules, (2) an employee recognition and award program. Training modules will supplement the contractor's own training programs for improving courtesy of employees.

Further, the Contractor is expected to present to the Port Authority a detailed outline of the Customer Service training it provides its employees. This outline must be consistent with the most recent edition of Airport Standards Manual and a determination will be made regarding its adequacy and further training needs, if any. The Contractor is expected to follow through on any training recommendations made by the Port Authority and bear all associated expenses.

All Contractors to the Port Authority with direct customer contact employees must have all employees participate in the Port Authority's customer care training program.

ATTACHMENT I – CUSTOMER CARE MANUAL

THE PORT AUTHORITY OF NY & NJ

Kennedy · Newark Liberty · LaGuardia · Stewart
Teterboro · Downtown Manhattan Heliport

Customer Care

Airport Standards Manual

Fifth Edition • July 2008

Port Authority
Customer
Care

THE PORT AUTHORITY OF NY & NJ

William R. DeCota
Director

July 2008

To our Airport Partners:

Almost ten years ago, we set out on a journey to improve customer satisfaction at The Port Authority of New York and New Jersey's airports. The foundation of our program continues to be our Airport Standards and I am pleased to share with you this 5th Edition of the Airport Standards Manual—Customer Care Standards that have been developed in cooperation and assistance from you, our Airport Partners.

The overall objective of our Customer Care Program is to improve the customer experience at the Port Authority airports regardless of who provides the service. Every airport employee, whether they are Port Authority employees or Partner employees, contributes to the ultimate quality our customers' experience.

This updated edition also includes some basic standards for cargo services as a start to evolving a Cargo Care Program. These standards will form the baseline of our performance measurement program under development for the cargo business at our airports. The cargo standards will evolve with the assistance and partnership of our cargo partners as we move forward to measure and monitor performance in all areas of the airport experience.

As a team and airport community, we have made tremendous progress with our customers over the years, as our customers have recognized improvements year over year and have become more delighted and pleased with the services provided by all of us. But improvement only comes with conscientious effort and determination. Through the Customer Care Program, we have offered customer care training to all airport employees; we utilize a bi-weekly mystery shopping program, a semi-annual facility quality assurance inspection program as well as our annual customer satisfaction survey. As we listen to our customers and partners, we seek to implement best industry practices as we jointly develop the "Airport of the Future" using tested and new technologies and comply with ever changing government regulations. This manual is another tool in this toolkit of performance enhancement strategies and I recommend you employ its contents in your daily operation, and ensure that all your employees and contractors are familiar with its guidelines and requirements.

We at The Port Authority of New York and New Jersey want to thank you and the many people who work together at the airports everyday to provide a positive and affirming experience for our customers. With your continued support and our joint commitment, we believe that Customer Care will continue to thrive at our airports.

Sincerely,

Lysa C. Scully
Assistant Director
Customer, Cargo, Concessions & Airport Services
Aviation Department

Port Authority Customer Care

Aviation Department
225 Park Avenue South, 9th Floor
New York, NY 10003

Customer Care
Airport Standards Manual

John F. Kennedy International Airport

Newark Liberty International Airport

LaGuardia Airport

Stewart International Airport

Teterboro Airport

Downtown Manhattan Heliport

Prepared and Published by
The Port Authority of New York & New Jersey – Aviation Department
Customer, Cargo, Concessions & Airport Services Division

Copyright © 2008 The Port Authority of New York & New Jersey
All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or database, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of The Port Authority of New York & New Jersey.

INTRODUCTION & PERFORMANCE MEASUREMENT PROGRAM

1.0	Employee Attitude, Appearance, Awareness and Knowledge	16
2.0	Curbside	19
3.0	Flight Check-in Areas	21
4.0	Walkways, Corridors, Elevators & Escalators	24
5.0	Passenger & Baggage Screening Areas	26
6.0	Restrooms	28
7.0	Gate Areas	31
8.0	Retail Services	34
9.0	Food & Beverage Services	38
10.0	Baggage Claim	42
11.0	Ground Transportation & Welcome Centers	45
12.0	Taxi Dispatch Service	50
13.0	Parking Lots & Garage Services	51
14.0	Construction	54
15.0	Charter Operations	56
16.0	Ramp & Airside Areas	58
17.0	Assistance to Stranded Passengers	61
18.0	AirTrain Stations and Vehicles	63
19.0	Assistance to Passengers with Reduced Mobility (PRM)	69
20.0	Public Circulation & Queue Management	73
21.0	Orderly Evacuation & Resumption of Services	76
22.0	Cargo Services	81

Airport Standards Manual

The Port Authority, in cooperation with its partners, the airlines, terminal operators and service providers, developed this edition of the Airport Standards Manual (ASM)—Customer Care Standards for the benefit of all airport customers. The ASM serves as the primary document outlining the customer care and service-related responsibilities incumbent upon employees working at Port Authority airports. The Standards focus on the elements of airport services and facilities that most impact customer satisfaction at Port Authority airports as determined by analysis of customer surveys and other customer feedback mechanisms. The Standards fall under three broad categories:

- Customer Care (including cargo);
- Signing and Wayfinding;
- Terminal Planning and Design Standards (Passenger and Cargo Facilities)

The ASM will continue to evolve and grow to meet the demands of our customers through changes in operating procedures, facilities, government regulations and the introduction of technology by the aviation industry.

I. PURPOSE

The Port Authority, in cooperation with its partners, the airlines, terminal operators and service providers, developed this edition of the ASM—Customer Care Standards for the benefit of all airport customers. The Port Authority's objective is to maximize utilization of the ASM as one tool to effectively manage customer care.

This ASM defines *Customer Care Standards* and the *Airport Performance Measurement Program*. It is made available to all partners. Hence, it is expected that the Port Authority and all employers on the airports *will strive to meet or exceed these standards.*

The ASM will continue to evolve and grow to meet the demands of our customers through changes in operating procedures, facilities, government regulations and the introduction of technology by the aviation industry.

II. THE STANDARDS

The *Customer Care Standards* focus on the most salient elements of airport services and facilities that impact customer care satisfaction.

Separate publications promulgate several design-related standards, such as:

- "Adequate" or "Sufficient" lighting standards that conform to the **Illuminating Engineering Society of North America (IES-NA) Lighting Handbook, 8th Edition, Section 11** as they pertain to the respective areas and activities.

- All signs shall be in conformance with the **Port Authority Aviation Department Signing and Wayfinding Standards Manual** as well as those areas addressed in this manual.

- All Terminal Planning shall be in conformance with the **Port Authority Aviation Department Terminal Planning and Design Standards,** including recommended design guidelines for Restrooms, Check-in Areas, Gate Areas, Security Checkpoints, Corridors and Walkways, Concessions Locations are subject to ***Tenant Alteration Application (TAA) Procedures and Standards Guide*** reviews and subsequent addenda.

- All Airport Partners must adhere to the **Airport Rules and Regulations**.

The Customer Care Standards implemented at Port Authority airports are measured and reviewed regularly against best industry practices to gauge the need for changes or augmentation. The measurement process includes, but is not limited to customer surveys, mystery shopping, facility quality assurance evaluations, focus groups and other data gathered for the Port Authority.

This edition of the ASM introduces a set of cargo standards and performance measures for specific areas. Focusing on the areas that most impact our cargo customers, these initial standards will continue to evolve through the assistance and cooperation of our air cargo business partners.

Given that the standards evolve over time, the enumeration and numbering of these standards within the ASM may differ from prior ASM editions due to modifications, additions or deletions of standards. A designation at the end of each of the standards, where applicable, indicating whether the standard is a ***high or routine priority. High priority standards*** typically require capital intensive or long-term solutions or are possible life-safety issues. ***Routine priority standards*** are cleanliness, maintenance or conditional issues that may be immediately remedied via currently available staff and equipment without impeding customers or causing life-safety concerns. All standards of Employee Attitude, Appearance, Awareness and Knowledge are considered ***high*** in nature.

III. IMMEDIATE ACTION ITEMS

Certain aspects of the Mystery Shopping and Quality Assurance Facility Evaluation process are deemed to be ***"Immediate Action Items,"*** requiring immediate attention. These items include:

- **Safety and Security concerns**
- **Rudeness/indifference to customers**
- **Excessive disrepair**

If Mystery Shoppers/Q.A. Facility Evaluators witness any of these conditions they will immediately notify the proper airport contacts to call:

- EWR: 973-961-6154
- JFK: 718-244-8158
- LGA: 718-533-3700

Airport Performance Measurement Program (APMP)

I. SERVICE COMMITMENT

The Airport Performance Measurement Program (APMP) provides the framework outlining the process that encourages actions and a commitment to customer care regardless of who provides the service. More specifically, the APMP is designed to:

1) Recognize **"Satisfactory"** performance by Partners who continue to improve customer satisfaction.

2) Provide a useful management tool to identify to Partners the areas that **"Needs Improvement."**

3) Monitor actions taken to address deficiencies in a timely manner.

All airport employees are responsible for upholding the Airport Standards Manual (ASM)—Customer Care Standards and The Port Authority and its Partners are responsible for adopting these standards and implementing them within their respective service areas.

Commitment to upholding the standards is essential for providing quality customer care. High levels of customer satisfaction should be the natural outcome of commitment to and compliance with the Standards. A Partner's performance is considered to be **"Satisfactory"** when it achieves high marks in a series of objective evaluations designed to measure performance of contractual responsibilities in light of ASM requirements.

There is, however, an important distinction between the level of customer satisfaction achieved by a Partner, and the Partner's level of commitment and compliance to the ASM. Customer satisfaction is useful in measuring the customers' perceptions about each Airport's services, but does not directly evaluate a Partner's commitment, compliance, or performance. Similarly, Partner compliance is a useful measure to determine how committed a Partner is to implementing the ASM; yet this may not be reflected in the Partner's level of customer satisfaction. Where feasible, the two elements, customer satisfaction and Partner's commitment, must be measured and evaluated together to determine a Partner's true effectiveness and the effect the ASM—Customer Care Standards and the APMP have on customer care.

II. OBJECTIVES

The overall objective of the APMP is to improve the quality of customer care offered at Port Authority airports regardless of who provides the service. Every airport employee, whether they are Port Authority employees or Partner employees, contributes to the quality of customer care.

Where the ASM—Customer Care Standards defines good customer care, the APMP defines performance measurement and provides a management tool to recognize **"Satisfactory"** performance and to monitor actions taken to address areas that **"Needs Improvement."**

By using the ASM and the APMP together, the Port Authority and its Partners gain an understanding of the commitment necessary for quality airport customer care.

The APMP also outlines how **"Scorecards"** are developed and explains the method used in periodically determining each Partner's performance. The Scorecard is the measure of a Partner's performance in a specific area. The Scorecard may be a combination of several different measurement tools including customer satisfaction surveys, mystery shopping and quality assurance facility evaluations.

III. METHODOLOGY

This section proposes a general framework for a quantitative strategy to:

(1) Measure Partners' performance.
(2) Provide an objective means for recognizing **"Satisfactory"** performance.
(3) Monitor actions required by Port Authority staff and Partners in areas that **"Needs Improvement"** that will help improve performance.

Accordingly, the APMP identifies the elements that are most important to customer care and provides a recommended strategy for assessing Partners' performance.

To begin with, **Figure 1** briefly illustrates the various steps of the Customer Care process used to develop the ASM Customer Care Standards and to integrate them with the APMP. There are three major components to the development of the APMP:

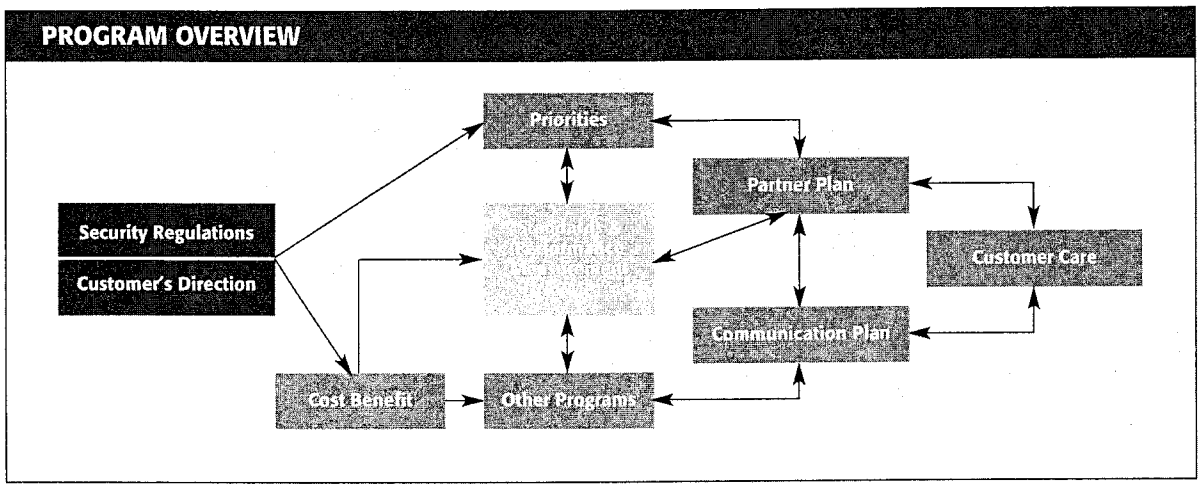


Figure 1

1. **Airport Standards Manual (ASM) Development.** The Port Authority's objective is to maximize utilization of the ASM as an effective customer care management tool. See page 1.

2. **Port Authority Contracts and Permits.** This component encompasses the development and introduction of standard language for contracts and permits requiring the commitment of all Partners to improve customer care through several actions including, but not limited to, Employees Attitude, Appearance, Awareness and Knowledge, Cleanliness, Condition and Functionality of all public areas impacting a customer's airport experience.

3. **Port Authority Leases.** All references to the "Airport Standards Manual" in the standard lease document shall be interpreted as a commitment to all components of the latest edition of the Airport Standards Manual including Customer Care Standards, Signing and Wayfinding Standards and Passenger and Cargo Facilities Design & Planning Standards. Any new construction, terminal modifications or renovations shall be handled in accordance with existing Port Authority Tenant Alteration Application (TAA) procedures.

The APMP is a process designed to facilitate Partners' efforts in this area and is described in more detail in the following paragraphs.

A. Monitoring Tools

The Port Authority has developed a quantitative performance measurement strategy that measures Partners' performance. By limiting the data measurement tools to a few key sources rather than a multitude of sources that employ different collection techniques and scoring methodologies, the Port Authority and its Partners can focus on a few critical metrics. Mystery shopping, quality assurance facility evaluations, and additional non-survey data collection, all monitor Partners' performance. The customer satisfaction survey measures customer perception of various services and facilities at each airport. These measuring tools are proactive efforts undertaken periodically to track compliance to or implementation of the ASM with the objective of improving customer care:

1. **Customer Satisfaction Survey**—The annual Customer Satisfaction Survey conducted in the spring (May /June) quantifies customer evaluations regarding the quality of the facilities and services. Randomly chosen departing passengers in the gate hold lounges and arrival passengers in the Baggage Claim area, curbside and at AirTrain platform entrances (EWR only) are asked to rate various service and facility attributes on a scale of 1 to 10 (1 being "unacceptable" and 10 being "outstanding"). Passengers assigning a rating of 8 to 10 are deemed to be "highly satisfied." A satisfaction score is obtained by dividing the number of passengers who are highly satisfied with the service/facility by the total number of passengers polled.

2. **Mystery Shopping**—The mystery shopping is conducted semi-monthly and its report, **Figure 2**, summarizes the performance and quality of various operators and services at each of the airports based on selected criteria representative of all the key attributes for each Airport Standard with a focus on Employee Attitude, Appearance, Awareness and Knowledge. Each of the criteria are given a score of "0" if the service meets the Standard or "1" if it does not meet the Standard. The results are then totaled and a corresponding percentage "Gap to Acceptability" (defined as the percentage of standards measured that are deemed deficient) is reported for each Partner. This method of data collection provides some measure of Partner performance for all of the service standard categories.

MYSTERY SHOP SUMMARY REPORT

Property Number: EWR-TO
Property Name: Newark Terminal Operator – PA
Date of Evaluation: 4/3/2007
Previous Evaluation: 3/7/2007

	Standards Missed	Standards Evaluated	Rolling Average	Previous Score	Gap to Acceptability
TERMINAL	56	212	42.33	39	26%
CURBSIDE DEPARTURE	13	44	10.67	8	30%
Overall Cleanliness/ Conditions	7		6.00		
Curbside Departure	13				
Standards of Cleanliness	4				
Standards of Condition	3				
Standards of Functionality	1				
Signs, Directions, and Information	0				
Standards of Employee Attitude, Appearance and Knowledge	5		3.33		

Figure 2

3. **Quality Assurance Facility Reports**—Quality assurance facility reports, **Figure 3**, provide summarized routine and *high priority* deficiencies. Based on cleanliness, condition and functionality. Each criteria are given a score of "0" if the standard is met or "1" if it does not meet the standard. *Routine* deficiencies are quick fixes identified with mostly cleaning or management issues, while *high priority* deficiencies are those addressing condition and functionality and are more likely to be capital intensive and/or long term fixes. The high and routine deficiencies identified through quality assurance facility evaluations are then totaled and distributed to all partners for follow up actions.

QUALITY ASSURANCE FACILITY SUMMARY REPORT

Property Number:	EWR-TO
Property Name:	Newark Terminal Operator – PA
Date of Evaluation:	4/11/2007
Previous Evaluation:	11/9/2006

	Standards Missed	Standards Evaluated	Previous Score	High	Routine
TERMINAL	259	1775	100	30	229
CURBSIDE DEPARTURE	13	25	N/A	1	12
Curbside Departure – Terminal B	13			1	12
Standards of Cleanliness	5			0	5
Standards of Condition	6			1	5
Standards of Functionality	2			0	2
Signs, Directions, and Information	0			0	0

Figure 3

4. **Additional Data Collection and Partners' Information**—This includes working with Partners and monitoring respective action plans and collecting appropriate data such as processing or wait times where queuing or delivery normally takes place. Two areas where measurement began in 2008 are as follows:

   - Baggage Claim—two separate 4-hour mystery shops are conducted per month at each domestic terminal baggage claim. The mystery shopper records the time of the first bag and the time of the last bag for approximately 9 to 12 flights, at various carousels. Three measurements for each flight are recorded: 1) time on blocks from the DOT website; 2) time of first bag; and 3) time of last bag. Data is tracked by month and quarter for each airline, terminal and airport.

   - Check-In—two separate 4-hour mystery shops are conducted per month at each terminal check-in area. The mystery shopper spends approximately one hour at one specific check-in area, and during the course of the mystery shop, evaluates wait times approximately 4-5 varied airline check-in lines at one terminal. Data is tracked by month and quarter for each airline, terminal and airport.

   - Taxi Dispatch—mystery shoppers will also develop sampling of wait times at the taxi dispatch stations at arrivals level along the terminal frontages.

   - Parking lot exit—mystery shoppers also record the wait time on line at the cashier booth as they exit the parking facility.

   - Security Checkpoints and US Entry—Wait or process times are monitored using data collected by DHS at all Port Authority airports.

   - Cargo—The first cargo performance measure to be introduced in 2009 will pertain to truck waiting times. Measurements for this program are under development and will rely on partner information.

Note: Some or all of the above monitoring tools may be included in specific **Scorecards**.

B. Setting Practical Targets

Using the above monitoring tools, performance measurement targets have been established to gauge Partner performance. Mystery shops are performed semi-monthly and will be supplemented with periodic quality assurance facility evaluations and data collection. These two monitoring sources will be used to provide feedback to Partners on an as needed basis. In addition to semi-annual quality assurance facility reports, scorecards will be calculated using one or more of the following measures: the customer satisfaction survey, mystery shops, quality assurance facility evaluations and/or other data collection.

For Port Authority contractors, the Port Authority or its designated representative may conduct random quality assurance facility evaluations for cleanliness, condition and functionality based on the ASM—Customer Care Standards. The Port Authority shall have the right, in its sole discretion and without prior notice to the contractor, to modify the staff quality assurance facility evaluations.

For Port Authority contractors, performance over the entire contract period will be taken into account. The purpose is to encourage contractors to uphold their performance as a contract nears completion; continuous periods of non-performance will be reflected in the contractor's scorecard and could be applied to future bids if contractors do not show improvement throughout the contract.

IV. SCORECARDS

Scorecards contain an overview of the grading system and the performance targets for several areas. ***Performance targets*** have been set within each scorecard based on achievable scores from previous surveys, mystery shops or quality assurance facility evaluations (see subsequent section on ***Performance target Definitions***). Each Partner will be responsible for meeting or exceeding these targets regardless of whether the Partner was under contract at the time these targets were established. The Partner performance shall be rated **Satisfactory** when targets are met or exceeded across all applicable performance measures, and a **Needs Improvement** rating will result when one or more performance measure does not meet the established performance target. The measurement of performance for some areas may be based upon one or a combination of measurement sources.

Using these results, the Port Authority can provide recognition for continued high-level **Satisfactory** performance or enact remedial actions (e.g., contract renegotiation or termination) for continued under-performance for areas that **Needs Improvement**.

Figure 4 illustrates the performance measurement improvement process leading to appropriate actions when performance is rated as **Satisfactory** or **Needs Improvement**.

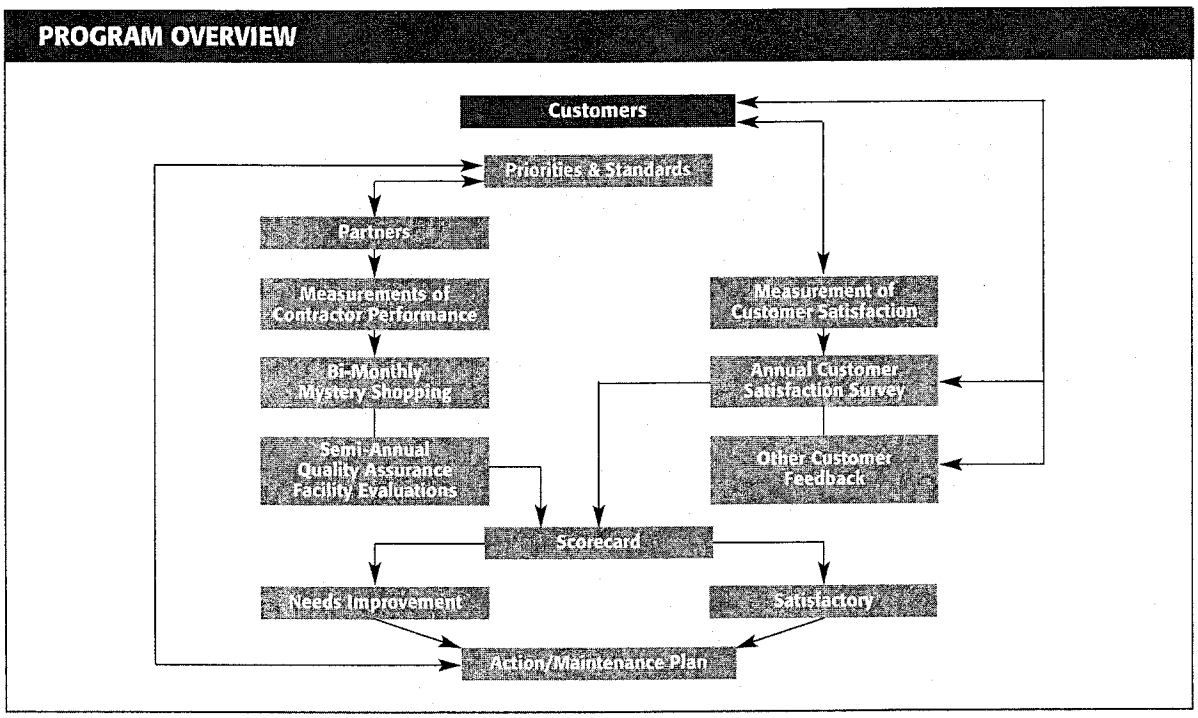


Figure 4

There are two categories of contractors—those under direct contract with the Port Authority, and those under contract with Terminal Operators and Airlines. In many cases, the Port Authority has the ability to recognize **Satisfactory** performance and also to take appropriate action(s) when performance is rated in **Needs Improvement** for its own partners. However, the Port Authority has limited recourse it can take for non-Port Authority partners.

In summary, the APMP is designed to provide the Port Authority and its partners with the framework to evaluate and encourage a commitment to service and facility improvements at the Port Authority's airport facilities. However, this manual can also be extended to assist Partners with fostering commitment to customer service improvements through compliance with the ASM monitoring of third-party partner's performance.

A. Applicable Airport Elements

The following is a list of existing scorecards measuring courtesy of employees:

Concessions (retail, food & beverage)
Security Screening
Departure Curbside
Welcome Centers including Customer Care Representatives
Parking Lot and Garage Services
Taxi Dispatch
On Airport Bus

The following is a list of existing scorecards measuring cleanliness, condition and functionality of the area:

Concessions (retail, food & beverage)
Flight Check-in Areas
Parking Lots and Garage Services
Gate Lounges
Security Screening
Departure Curbside
Baggage Claim Area
Taxi Dispatch Service
AirTrain Stations/Vehicles
On-Airport Bus
Restrooms
Corridors/Walkways/Elev./Escal.
Arrival Curbside
Welcome Centers

The following is a list of wait or process times and what functions they are collected for:

Bag Claim
Check-in
TSA Security Checkpoint
Taxi Dispatch Service
Parking Lot Exit
CBP US Entry

B. Performance Target Definitions

The ***Performance Target Definition*** for Customer Satisfaction and Mystery Shopping that appears in each Scorecard is uniformly calculated for any airport element being evaluated:

- **Customer Satisfaction Performance Target (Range)**

  It is based on the average of the highest departure passenger satisfaction score from each airport for the airport element being evaluated. This average serves as the highest value of the performance target range. By subtracting 5 percentage points from the upper bound, we obtain the lowest value of the range. The Performance Target will never be more lenient (lower) than the prior year's target range.

- **Mystery Shopping Performance Target**

  It is based on a rolling 6-month average of the mystery shopping deficiency counts for a given airport element from each airport. The lowest deficiency count for each airport is then averaged to become the Performance Target. The Performance Target will never be more lenient **(higher)** than the prior year's target.

The ***Performance Target Definition*** for the Quality Assurance Facility Evaluation varies depending on the airport element measured.

- **Quality Assurance Performance Target**

  It is based on the average number of deficiencies allowable per measurement unit. It is calculated as a ratio of the number of deficiencies to number of units across all terminals or applicable areas at the airports. The Performance Target will never be more lenient **(higher)** than the prior year's target.

  The measurement unit and allowable deficiencies varies by the airport element being evaluated and are subject to change. The current unit definitions are listed below:

  - Restrooms: Fixtures (toilet stalls, urinals and sinks). *One deficiency allowable for approximately every 8 fixtures.*
  - Gates: Square footage. *One deficiency for approximately every 8,400 sq. ft. of gate space.*
  - Flight Check-in Area: Square footage. *One deficiency for approximately every 2,700 sq. ft. of check-in space.*
  - Concessions: Square footage. *One deficiency for approximately every 1,400 sq. ft. of concessions space.*
  - Screening Area: Number of security lanes. *One deficiency for approximately every 2 security lanes within the screening area.*

- Baggage Claim: Square footage. *One deficiency for approximately every 4,400 sq.ft. of baggage claim space.*
- Departure Curbside: Square footage. *One deficiency for approximately every 1,600 sq. ft. of departure curbside space.*
- Arrival Curbside: Square footage. *One deficiency for approximately every 1,600 sq. ft of arrival curbside space.*
- Corridors/Walkways/Elevators/Escalators: Number of Corr/WW/Elev/Escal. *One deficiency for approximately every 3 Corridor/Walkway/Elevator/Escalator units.*
- Welcome Centers: Number of Welcome Centers. *1.5 deficiencies per Welcome Center.*
- Parking Lot and Garage Services: Number of parking spaces at lots/garages. *One deficiency allowable for approximately every 340 parking spaces.*
- Taxi Dispatch Service: Number of taxi dispatches. *Two deficiencies for each taxi dispatch booth.*
- On-Airport Buses: Number of buses in operation during peak periods. *One deficiency per bus.*
- AirTrain Stations: Square footage. *One deficiency allowable for approximately every 4,600 sq. ft. of station area.*
- AirTrain Vehicles: Number of vehicles in operation during peak periods. *One deficiency for every 12 vehicles.*

For all three monitoring tools (Customer Satisfaction, Mystery Shopping and Quality Assurance Facility Evaluation) the Actual Performance is compared against the Performance Target. If the Actual Performance is THE SAME OR BETTER than the Performance Target, the result is **Satisfactory**. If the Actual Performance is WORSE than the Performance Target, the result is **Needs Improvement**.

C. Scorecards Descriptions & Methodology

- A Sample **Needs Improvement** Scorecard [**Figure 5**]

2007 PERFORMANCE MEASUREMENT SCORECARD—GATE AREA

Terminal XYZ – Airport Y

Gates	Gate Sq. Ft.	Avg. Mvmt. Per Day	Avg. Mvmt. Per Gate Per Day	Outbound Pax. 12 Months Ending June 2007	Avg. Sq. Ft. Gate Area	Sq. Ft. Average Daily Pax	IATA Level of Service
38	43,500	457	13	6,949,150	1,145	2.3	F

	Customer Satisfaction (% Highly Satisfied)	Mystery Shopping (# of Deficiencies)	Quality Assurance (# of Deficiencies)
	Overall	Condition	Standards Missed - All Items
Timeframe	Annual - June 2007	6-Mon. Rolling Average - June 2007	Annual - April 2007
Actual Score	38	4	51
Performance Target (PT)	53-58	2	29
Specific Results	Needs Improvement	Needs Improvement	Needs Improvement

Overall Progress Since 2006	Customer Satisfaction Score increased 1% point, remaining at Needs Improvement Mystery Shopping Deficiencies increased 1 point, remaining at Needs Improvement Quality Assurance Deficiencies unchanged, remaining at Needs Improvement

Notes/Recommendations

- Cleaning up the terminal/gate areas, improving/upgrading facilities, offering more comfortable seating, a larger gate area to reduce crowding, more frequent updates when there are delays, better lighting, more WiFi connections, more electrical outlets and more entertainment options are all key items that air passengers say needs attention in order to improve their rating of the terminal. Comfortable seating, cleanliness/condition of the gate area and concessions offerings near the gate area are rated lower than other gate elements, more so among business travelers.
- Remove heavy accumulation of dust at ceiling vents/fixtures, everywhere. More frequent cleaning of gate areas needed, especially during peak times (paper/food/ debris/residue on floor/seats, windows smeared/smudged and debris on window sills at many gates, phones have adhesive residue and dust -- C9 phone bank damaged).
- Replace all damaged and/or missing ceiling tiles (present at most gates), ceiling damaged at A2, D10, HVAC cover damaged at C3). Repair scuffed/scratched/scraped/ gouged walls/columns/doors in all concourses (e.g., wall vinyl curling/damaged at A7/ B1/ B3/C2/D1 outlet covers missing at A6, walls gouged at A1).
- Clean carpet in all gate hold areas to remove stains; also repair torn/worn/damaged carpet/floor at A2/A3—trim strip missing, A7—carpet taped and matted, stairs worn at B5A, B7 & B8.
- Some seating torn at A5-6, B1, B2, B7, C2, C4-6, D2, D6. Counters/podiums chipped/worn at most gates, some also have adhesive residue (graffiti on C5 jetway counter).
- Many non-working ceiling lights and/or missing light covers (e.g., A1, B4, C1-3, C5-6, C11). Lighting insufficient relative to IES standards at gates A5, B1-3, C10-11, D1-10.

Figure 5

• A Sample **Satisfactory** Scorecard [**Figure 6**]

2007 PERFORMANCE MEASUREMENT SCORECARD—DEPARTURE CURBS Terminal ABC							
#Curbside Check-in Locations	Outbound Domestic Passengers 12 Months Ending June 2007		Outbound International Passengers 12 Months Ending June 2007		Curbside		
Counter/Podium Stations	%	Total #	%	Total #	Total Sq. Ft.	Length	Width
4	41%	1,029,798	59%	1,494,324	25,650	855	30
OTHER INFORMATION							
	Customer Satisfaction (% Highly Satisfied)		Mystery Shopping (# of Deficiencies)		Quality Assurance (# of Deficiencies)		
	Condition/Cleanliness		Courtesy	Condition	Standards Missed		
Timeframe	Annual - June 2007		6-Mon. Rolling Average - June 2007		Annual - April 2007		
Actual Score	62		1	2	13		
Performance Target (PT)	60-65		1	3	17		
Specific Results	Satisfactory		Satisfactory	Satisfactory	Satisfactory		
Overall Progress Since 2006	Customer Satisfaction Score increased 5% point, remaining Satisfactory. Mystery Shopping Deficiencies changed for Courtesy and decreased 1 point for Condition, both remaining Satisfactory. Quality Assurance Deficiencies increased 5 points, remaining Satisfactory.						

Notes/Recommendations

• Passengers tell us that reducing the traffic congestion at the curbside is one way to improve their ratings of the terminal. International and leisure travelers are moe satisfied with their departure curbside experience than others.

• On most occasions, skycaps are attentive and offered a warm, friendly greeting, but on two occasions they were inattentive and unfriendly.

• Roadways and walkways stained (also gum on walkways) and cracked in places. Terminal entry doorways had residue at bottom and small glass and frames are chipped/scratched. Windbreaker at doorway #3 needs cleaning; broken glass near doorway #2.

• Skycap counters have adhesive residue and are scratched.

Figure 6

The Scorecards are created by the Aviation Department based on the information obtained through various measurement sources. The top portion of the Scorecard presents background information for the particular airport element being evaluated, providing a backdrop to better understand the airport environment that existed during the measurement cycle. The middle portion of the Scorecard presents current and trended ratings for the airport element being evaluated for the period under review. From the amalgamation of the data, targets are set and a rating assigned based on each areas' performance. The bottom portion of the Scorecard highlights specific areas that should be addressed via capital planning improvements, customer care training programs, and discussions with contractor management regarding performance review and enhancement. Below is a description of how the targets are set for each of the measurement methods and interpretation of the results.

- **Customer Satisfaction Survey:** The customer satisfaction survey is conducted annually. In each functional area, the highest score from each airport is combined and averaged to set the target. A five (5)-point margin below the target is allowed and each terminal is rated on their performance relative to this target. In **Figure 5**, the target for the gate area is 53-58 percent. The gate areas (38%) are deemed unacceptable because its score is not within the acceptable range, thereby receiving a classification of **Needs Improvement**. **Figure 6** illustrates a scorecard in which all targets have been met or exceeded (62 is within the range 60-65) and therefore performance is rated as **Satisfactory**.

- **Mystery Shopping:** Mystery Shopping is performed semi-monthly, with each terminal being shopped twice per month. The scoring of the Mystery Shopping is based on the number of standards missed in the shops (i.e., deficiencies). The lower the number missed, the better the score. Each functional area's score for the six-month period preceding the issuance of the scorecard constitutes its "rolling average." The lowest "rolling average" score in each functional area from each airport is averaged to obtain the ***Performance Target*** score. To be considered Satisfactory, the area must equal or fall below the target. In **Figure 5**, the deficiencies (4) exceeds the Performance Target (2), thereby receiving a classification of **Needs Improvement**. In **Figure 6**, actual deficiencies for courtesy and condition (1 and 2, respectively) are equal to or less than the Performance Targets (1 and 3, respectively) and are deemed **Satisfactory**.

- **Quality Assurance Facility Evaluations:** The quality assurance facility evaluation is performed semi-annually. The scoring for the quality assurance facility evaluation is based on the number of standards missed (i.e., deficiencies). Much like mystery shopping, the goal is to have the lowest score possible. Each functional area is assigned measurement criteria; for example, the gate areas and concessions use the surface area (in square feet) as a base for measurement (for detailed information, please refer to the prior section entitled **"Quality Assurance Performance Target"**). By taking the aggregate of all the deficiencies within a functional area across all the airports and dividing this number into the total of the respective measurement criteria, we calculate the quality assurance facility evaluation ***Performance Target*** score. This provides a pro-rated score that is applied to each terminal or location to assess its performance relative to the rest of the airports. The total number of deficiencies is summed and divided by the total number of units across the airports providing a "per unit" number of acceptable deficiencies. This score is then multiplied by the number of units per functional area to determine the target number (upper limit) of deficiencies. In **Figure 5**, the deficiencies (54) exceeds the ***Performance Target*** (29), thereby receiving a classification of **Needs Improvement**. In **Figure 6**, actual deficiencies (13) falls under the Performance Target (17) and is deemed **Satisfactory**.

1.0 - Employee Attitude, Appearance, Awareness and Knowledge

All airport employees are required to be courteous and helpful at all times with every customer and other employees. ***All standards in this section are high priority.***

Standards of Employee Attitude, Appearance, Awareness and Knowledge

All employees will meet or exceed the following standards:

1.1 Attitude, all employees shall:

1.1.1 Greet all customers in a friendly and professional manner.

1.1.2 Address customers proactively—be friendly and approachable—anticipate customer's needs. Customers and passengers shall not have to initiate contact.

1.1.3 Display a smile and eye contact towards passengers and fellow employees at all times.

1.1.4 Project a pleasant, friendly and attentive demeanor and maintain proper posture at all times.

1.1.5 Be capable of communicating clearly when in contact with customers.

1.1.6 Refrain from using foul or inappropriate language at any time.

1.1.7 Use a proper and courteous vocabulary and a pleasant tone of voice with customers and fellow employees.

1.1.8 Make every effort to satisfy customers' needs, even when those needs are outside the employee's specific job scope.

1.1.9 Focus on customers and not gather in a group to chat while on duty.

1.1.10 Not eat, drink, (including alcoholic beverages), chew gum or smoke in other than designated areas of the workplace, especially in view of customers when in uniform.

1.1.11 Assure that the customers' needs are met by providing or calling for the appropriate services.

1.1.12 Not nap or sleep while on duty or in a public area.

1.1.13 Not use personal electronic devices, including but not limited to cell phones and MP 3 players, while on duty.

1.2 Appearance, all employees shall:

1.2.1 Be well groomed, clean and present a professional appearance.

1.2.2 Wear only appropriate accessories, as determined by your employer, while on duty.

1.2.3 Wear nametags and/or official identification that is visible to the public at all times.

1.2.4 Wear clean, neat and pressed uniforms including appropriate footwear while on duty.

1.2.5 When speaking to customers, remove sunglasses (unless medically required otherwise) to facilitate eye contact. Sunglasses may only be worn outdoors and during daylight hours.

1.3 Awareness, all employees shall:

1.3.1 Be obligated to challenge persons and to report suspicious items and/or activity.

1.3.2 Be aware that all service vehicle operators ensure that unattended vehicles are locked and shall inspect the vehicle each time it has been left unattended.

1.3.3 Ensure that all catering company's unattended vehicles are locked and that catering supplies intended for carriage on passenger flights are only accessible to catering employees.

1.3.4 Ensure that all AOA doors and gates are closed properly after each use.

1.3.5 Not allow persons to follow them through an AOA door or gate. Each individual must swipe their airport-issued identification card each time they enter the AOA or SIDA.

1.3.6 Not write AOA or SIDA access codes on identification cards, and employees shall enter codes in a secure manner not visible to the public.

1.3.7 Airline employees shall not accept consignments of cargo, courier and express parcels or mail for carriage on passenger flights unless the security of such consignments is accounted for.

1.3.8 Report unattended or suspicious items and/or activity to Port Authority Police or other law enforcement personnel.

1.3.9 Report any item or area that is in need of repair to the appropriate airport representative.

1.3.10 Report any alarm for security or fire to the Port Authority Police or other law enforcement personnel through the appropriate airport protocol.

1.3.11 Report the illegal solicitation of ground transportation services by unauthorized personnel ("Hustlers") to the Port Authority Police.

1.4 Knowledge, all employees shall:

1.4.1 Be well informed, capable of providing directions and know where and how to obtain requested information or services for customers.

1.4.2 Convey accurate information using clear and understandable terms.

1.4.3 Obtain the facts when encountering a dissatisfied customer; state any applicable policy clearly and politely; and be able to offer a solution or an adequate alternative to the customer. If unable to satisfy the customer or resolve the issue, direct the customer to immediate supervisor.

1.4.4 Know where and how to obtain assistance to resolve customers' questions or problems if language barrier arise.

1.4.5 Know where and how to obtain assistance in order to respond to medical emergencies and operational disruptions as referred to in Standard 20.0 (Orderly Evacuation and Resumption of Services)

1.4.6 Know where and how to obtain assistance in order to respond to medical emergencies including those relating to Passengers with Reduced Mobility being assisted.

2.0 - Curbside

Curbside General Requirements

a) Baggage carts shall be readily available at all cart racks at all times. {H}

b) Smoking receptacles shall be readily available on the curbside. {R}

c) Skycap service shall be readily available where applicable. {R}

2.1 Standards of Cleanliness

2.1.1 All frontages, sidewalks and crosswalks shall be clean and free of debris including gum and cigarettes. {R}

2.1.2 Entrance and exit doors shall be clean free of smudges, dirt and grime. {R}

2.1.3 All glass shall be clean and free of streaks and smudges. {R}

2.1.4 Trash receptacles shall be clean and emptied to prevent the overflow of debris. {R}

2.1.5 Awnings or canopies, where present, shall be clean at all times. {R}

2.1.6 Walls shall be clean and free of graffiti. {R}

2.1.7 Curbside check-in counters and self-service check-in kiosks shall be clean and organized, free of debris and baggage tape and without visible damage. {R}

2.1.8 Light fixtures and assemblies shall be clean and free of dust. {R}

2.1.9 Smoking receptacles shall be clean and emptied on a regular basis. {R}

2.2 Standards of Condition

2.2.1 All frontages, sidewalks and crosswalks shall be smooth and free of large cracks and missing surface areas. {H}

2.2.2 Entrance and exit doors shall be maintained in good working order. {R}

2.2.3 All glass shall be in good condition with no visible damage. {R}

2.2.4 Trash receptacles shall be in good condition, without dents, marks or peeling paint. {R}

2.2.5 Smoking receptacles shall be in good condition, without dents, marks or peeling paint. {R}

2.2.6 Awnings or canopies, where present, shall be in good condition, free of rips and tears. {R}

2.2.7 Walls shall be free of scratches, marks and scuffs. {R}

2.2.8 Curbside check-in counters and self-service check-in kiosks shall be in good condition, free of dents, marks and scuffs. {R}

2.2.9 All light fixtures shall be in working order with all visible lamps operating and all burned out lights replaced with no visible broken parts. {R}

2.2.10 Snow and ice shall be removed from walkways and roadways. {H}

2.2.11 Roadways shall be well maintained and free of potholes. {R}

2.3 Standards of Functionality

2.3.1 Unattended and unofficial parked vehicles shall not be present at frontages. Illegally parked vehicles will be ticketed, and towed at the owner's expense. {H}

2.3.2 Unattended baggage carts shall be returned to dispenser racks promptly and not allowed to collect in an unsightly manner. {R}

2.3.3 Public address systems shall be clear and audible. {R}

2.3.4 All lighting shall conform to Illuminating Engineering Society of North America (IES) standards for this area and application. {H}

2.3.5 All doors shall operate properly. {R}

2.3.6 All curbside computer equipment shall be in good working order. {R}

2.3.7 All baggage conveyor belts and curtains shall be in good working order with no visible broken parts. {R}

2.4 Signs, Directions, and Information

2.4.1 Directional signs shall be visible, legible and accurate. {R}

2.4.2 Signs shall clearly indicate the location of services. {R}

2.4.3 Handwritten signs shall not be used and all temporary signs shall be consistent with the Port Authority Aviation Signing and Wayfinding Standards. {R}

2.4.4 Airline names shall be posted at drop-off and, when practical, pick-up locations. {R}

2.4.5 Appropriate directional signs shall be visible at every decision point and be consistent with Port Authority Aviation Signing and Wayfinding Standards. {R}

3.0 - Flight Check-In Areas

Flight Check-In Area General Requirements

a) Minimum seating shall be provided in adjacent area for Passengers with Reduced Mobility. {R}

b) Trash receptacles shall be available in the airline check-in areas. {R}

c) Flight Information Display Systems should be provided. {R}

3.1 Standards of Cleanliness

3.1.1 Counters and kiosks shall be clean and free of graffiti. {R}

3.1.2 Workspaces shall always appear uncluttered and organized. {R}

3.1.3 Seating shall be clean and free of stains. {R}

3.1.4 Windowsills shall be free of dust and debris. {R}

3.1.5 Windows shall be free of streaks and smudges. {R}

3.1.6 Wastebaskets shall be clean and not overflowing. {R}

3.1.7 Walls shall have a clean appearance, free of dirt and marks. {R}

3.1.8 Carpet and floors shall be free of debris and stains and shall appear clean. {R}

3.1.9 Floors shall be dry, free from spills and water. {H}

3.1.10 Ceilings shall be clean and free of dust. {R}

3.1.11 Light fixtures and assemblies shall be clean and free of dust. {R}

3.1.12 Telephones and telephone areas shall be clean and free of debris. {R}

3.1.13 Heating and air conditioning units shall be clean and free of dust. {R}

3.1.14 Stanchions, ropes and "tensa barriers" shall be clean and free of dust, tape and smudges. {R}

3.2 Standards of Condition

3.2.1 Counters and kiosks shall be well maintained and in good repair. {R}

3.2.2 Workspaces shall be in good condition, free of dents, marks, scratches and scuffs. {R}

3.2.3 Seating shall be free of rips, tears, stains and broken parts. {R}

3.2.4 Windowsills shall be in good condition, free of broken parts and marks. {R}

3.2.5 All windows shall be in good condition with no visible damage, chips or marks. {R}

3.2.6 Wastebaskets shall be in good condition, with no visible damage. {R}

3.2.7 Walls shall be in good condition, with no dents, chips, marks or scuffs. {R}

3.2.8 Carpets shall be free of holes; rips, worn or frayed areas and flooring shall be free of large cracks, gouges and broken pieces. {H}

3.2.9 Ceilings shall be in good condition, evenly aligned and free of visible damage. {R}

3.2.10 All light fixtures shall be in working order with no visible broken parts. {R}

3.2.11 All telephones and telephone areas shall be in good condition, with no visible damage. {R}

3.2.12 Unattended baggage carts shall be returned to dispenser racks promptly or located so as not to impede the flow of passengers, and not allowed to collect in an unsightly manner. {R}

3.2.13 Heating and air conditioning units shall be in good working condition. {R}

3.2.14 Stanchions, ropes and, "tensa barriers" shall be well maintained and in good repair. {R}

3.2.15 Employees' personal belongings shall not be visible to customers. {R}

3.3 Standards of Functionality

3.3.1 Flight Information Display System (FIDS) monitors shall be in working order. {R}

3.3.2 Telephones shall be in working order. {R}

3.3.3 All lighting shall conform to the Illuminating Engineering Society of North America (IES) standards: **Terminal Ticket Counter—45-foot candles.** {R}

3.3.4 Stanchions, ropes, "tensa barriers" shall be arranged in a neat and orderly fashion and not stored in public view. {R}

3.3.5 Public address system shall be clear and audible in the check-in area. {H}

3.3.6 All baggage conveyor belts shall be in working order with no visible broken parts. {R}

3.3.7 All self-service kiosks shall be in good working order with no visible broken parts. {R}

3.3.8 Check-in wait time shall not exceed ten (10) minutes during peal periods. {R}

3.4 Signs, Directions, and Information

3.4.1 Clear, visible and accurate signing shall be placed at key decision points and must be consistent with Port Authority Aviation Signing and Wayfinding Standards. {R}

3.4.2 Flight Information Display System (FIDS) monitors shall be clear, visible and accurate. All flights, regardless of airline, shall be shown on the FIDS for that terminal. {R}

3.4.3 Handwritten signs shall not be used and temporary signs must be consistent with Port Authority Aviation Sign Standards. {R}

3.4.4 Customers shall be informed in a timely manner of flight delays via Flight Information Display Systems (FIDS), through appropriate public announcements and other *e-methods* used by the industry. {R}

4.0 - Walkways/Corridors/Elevators/Escalators

4.1 Standards of Cleanliness

4.1.1 Carpet and floors shall be free of debris and stains and appear clean. {R}

4.1.2 Floors shall be dry, free of spills or water. {H}

4.1.3 Ceilings shall be clean and free of dust. {R}

4.1.4 Light fixtures and assemblies shall be clean and free of dust. {R}

4.1.5 Pictures, frames and advertising along walkways and corridors shall be clean and dust free. {R}

4.1.6 Elevator interiors and floors shall be clean and free of debris and graffiti. {R}

4.1.7 Trash receptacles shall be emptied in order to prevent the overflow of debris. {R}

4.1.8 Heating and air conditioning units shall be clean and dust free. {R}

4.1.9 Water fountains shall be clean and free from debris and stains. {R}

4.2 Standards of Condition

4.2.1 Carpets shall be free of holes, rips, worn or frayed areas and flooring shall be free of large cracks, gouges and broken pieces. {H}

4.2.2 Ceilings shall be in good condition, evenly aligned and free of visible damage. {R}

4.2.3 All light fixtures shall be in working order with no visible broken parts. {R}

4.2.4 Pictures, frames and advertising shall be in good condition, free of tears, scratches, graffiti and other marks. {R}

4.2.5 Elevators, escalators and moving walkways shall be in working condition. All routine and preventive maintenance shall be scheduled to minimize passenger inconvenience. {H}

4.2.6 Elevator button lights and switches shall be in good condition. {R}

4.2.7 Each elevator emergency phone or communication device shall be in working condition. {R}

4.2.8 Water fountains shall have no visible broken parts. {R}

4.2.9 Corridors and walkways shall be free of obstructions. {R}

4.2.10 Heating and air conditioning units shall be in working order. {R}

4.2.11 Trash receptacles shall be in good condition, without dents, marks or peeling paint. {R}

4.3 Standards of Functionality

4.3.1 All monitors, including Flight Information Display Systems (FIDS), shall be in working order. {R}

4.3.2 Elevator button lights and switches shall be operational. {R}

4.3.3 Public address system shall be in working order and audible from all areas. {H}

4.3.4 All lighting shall conform to the Illuminating Engineering Society of North America (IES) standards: **Elevators—30 foot-candles; Corridors/Walkways—15 foot-candles**. {H}

4.3.5 Water fountains shall be in good working order. {R}

4.4 Signs, Directions, and Information

4.4.1 All elevator buttons, internal and external, shall be clearly marked and indicate appropriate services (e.g. Ticketing, Baggage Claim, Parking). {R}

4.4.2 Appropriate directional signing shall be visible at every decision point and consistent with Port Authority Aviation Signing and Wayfinding Standards. {R}

4.4.3 When elevators, escalators and walkways are being repaired, appropriate signs shall advise customers of other means of access in closest proximity. {R}

4.4.4 All monitors, including Flight Information Display Systems (FIDS), shall be clear, visible with accurate information. {R}

4.4.5 Handwritten signs shall not be used and temporary signs must be consistent with the Port Authority Aviation Signing and Wayfinding Standards. {R}

5.0 - Passenger and Baggage Screening Areas

This standard will apply to both arriving and departing passenger and baggage screening areas, which are under the jurisdiction of the Transportation Security Administration (TSA) and Customs and Border Protection (CBP).

5.1 Standards of Cleanliness

5.1.1 Carpet and floors surrounding baggage and passenger screening areas shall be free of debris and stains and shall appear clean. {R}

5.1.2 Baggage and Passenger screening equipment shall be clean, uncluttered and free of debris and baggage tape. {R}

5.1.3 All furnishings, including but not limited to, bins, tables, chairs, floor mats and private screening areas, shall be clean, uncluttered, free of debris and baggage tape. {R}

5.1.4 Walls and partitions shall have a clean appearance, free of dirt and marks. {R}

5.1.5 Ceilings shall be clean and free of dust. {R}

5.2 Standards of Condition

5.2.1 Floors shall be free of large cracks, gouges and excessively worn areas. {R}

5.2.2 Carpets shall be free of holes, rips and worn or frayed areas. {R}

5.2.3 All baggage and passenger equipment shall be in good condition, free of marks, scuffs and broken pieces. {H}

5.2.4 All furnishings, including but not limited to, tables, chairs, bins etc, shall be in good condition with no deep scratches, gouges, graffiti or broken pieces. {R}

5.2.5 Walls, columns and partitions shall be free of large cracks, holes and graffiti. {R}

5.2.6 Ceilings shall be free from stains and broken tiles. {R}

5.2.7 Sign frames, holders and stands shall be in good condition. {R}

5.2.8 Stanchions, ropes and "tensa barriers" shall be well maintained and in good repair. {R}

5.2.9 Employee's personal belongings shall not be visible to customers. {R}

5.3 Standards of Functionality

5.3.1 All equipment, including but not limited to, baggage conveyers, magnetometers, wands, x-ray machines and all other passenger and baggage screening areas machinery, bins and aids shall be maintained and in working order. {H}

5.3.2 Stanchions, ropes and "tensa barriers" shall be arranged in a neat and orderly fashion and not stored in public view. {R}

5.4 Departure Screening Wait Times

5.4.1 Queue time at the departing passenger screening areas on average shall not exceed ten (10) minutes. {H}

5.4.2 Queue time for passengers at the departing baggage screening areas on average shall not exceed ten (10) minutes. {H}

5.5 International Arrivals Clearance Wait Times

5.5.1 The United States Customs and Border Protection (CBP) has established one (1) hour, including wait time, as a standard for clearing formalities for passengers going through primary process. {H}

5.6 Signs, Directions, and Information

5.6.1 Internal notices shall not be displayed in public areas. {R}

5.6.2. Handwritten signs shall not be used and temporary signs must be consistent with Port Authority Aviation Signing and Wayfinding Standards. {R}

5.6.3 Clear, visible and accurate signing shall be place at key decision points and consistent with Port Authority Signing and Wayfinding Standards. {R}

5.6.4 Only approved regulatory signs shall be used. {R}

6.0 - Restrooms

Restrooms General Requirements

a) Restrooms shall have sinks with soap dispensers. {R}

b) All restrooms shall have sanitary seat covers available. {R}

c) All stall doors must have door locks or latches. {H}

d) All stalls shall be equipped with a clothes hook or a pocketbook holder. {R}

e) All restrooms shall be equipped with an adequate number of trash receptacles to meet peak traffic flow {R}

f) Paper products shall be provided in adequate supply to meet peak traffic flow. {H}

6.1 Standards of Cleanliness

6.1.1 Floors shall be free of debris and stains and appear clean. {R}

6.1.2 Floors shall be dry, free of spills or water. {H}

6.1.3 Unpleasant odors shall not be detected. {R}

6.1.4 Mirrors shall be free of streaks, smudges and watermarks. {R}

6.1.5 Sinks shall be clean, and faucets shall have a polished appearance. {R}

6.1.6 Entranceways and doors shall be clean and free of debris. {R}

6.1.7 Paper towel holders and/or automatic hand dryers shall be clean. {R}

6.1.8 Urinals shall be clean and free of debris. {R}

6.1.9 Tiles and walls shall be clean. {R}

6.1.10 Soap dispensers shall be clean and free of soap scum. {R}

6.1.11 Toilets and toilet bowls, including the rim, base, seat, cover, chrome fixtures and hinges shall have a polished appearance. {R}

6.1.12 Light fixtures and assemblies shall be clean and free of dust. {R}

6.1.13 Sanitary dispensers shall be clean. {R}

6.1.14 Trash and sanitary receptacles shall be clean, not overflowing and odor free. {R}

6.1.15 Baby changing stations shall be clean. {R}

6.1.16 All walls, doors and partitions shall be clean. {R}

6.1.17 Ceilings shall be clean and free of dust. {R}

6.1.18 Countertops shall be clean and free of debris and pooling water. {R}

6.2 Standards of Condition

6.2.1 Floor tiles shall not be broken, missing or stained or have gouges and grout shall be free of missing pieces and discoloration. {R}

6.2.2 Mirrors shall be in good condition, free of scratches, marks, de-silvering, cracks and broken pieces. {R}

6.2.3 Sinks shall be in good condition, free of scratches, stains and broken pieces. {R}

6.2.4 Entranceways and doors shall be in good condition, free of scratches, dents, marks and scuffs. {R}

6.2.5 Paper towel holders and/or automatic hand dryers shall be in good condition, free of marks, scratches, rust and broken pieces. {R}

6.2.6 Urinals shall be in good condition, free of chips, marks and broken pieces. {R}

6.2.7 Wall tiles shall be in good condition, free of chips, marks and broken pieces and grout shall be free of missing pieces and discoloration. {R}

6.2.8 Soap dispensers shall be in good condition. {R}

6.2.9 Toilets and toilet bowls, including the rim, base, seat, cover, chrome fixtures and hinges shall be in good condition with no broken pieces. {R}

6.2.10 All light fixtures shall be in working order with no visible broken parts. {R}

6.2.11 Sanitary dispensers shall be in good condition, free of marks, scratches and broken pieces. {R}

6.2.12 Trash and sanitary receptacles shall be in good condition. {R}

6.2.13 Baby changing station shall be in good condition, with all necessary parts and free of marks, scratches and scuffs. {R}

6.2.14 All walls, doors and partitions shall be free of graffiti, scratches and peeling paint. {R}

6.2.15 Ceilings shall be free of cracks and stains. {R}

6.2.16 Countertops shall be in good condition with no scratches, cuts, gouges or marks. {R}

6.2.17 All caulking joints between fixtures and wall or floor shall be fully filled without gaps. {R}

6.3 Standards of Functionality

6.3.1 Public address system shall be clear and audible in the restroom areas. {H}

6.3.2 Cleaning supplies and equipment shall be stored out of customers' view when not in use and doors to closets kept closed. {H}

6.3.3 All lighting shall conform to the Illuminating Engineering Society of North America (IES) standards: **Restrooms—23 foot-candles**. {H}

6.3.4 Automatic hand dryers and paper towel dispensers shall be in working order. {H}

6.3.5 Toilets and urinals shall be in working order. {H}

6.3.6 Door locks and latches shall be in working order. {H}

6.3.7 Sink drains and faucets shall be in working order. {R}

6.3.8 Baby changing stations shall be in working order. {H}

6.3.9 Sanitary dispensers shall be filled and in working order. {R}

6.3.10 Soap dispensers shall be in working order and have soap available. {R}

6.3.11 Unpleasant odors shall not be detected. {R}

6.4 Signs, Directions, and Information

6.4.1 Handwritten signs shall not be used and all temporary signs shall be consistent with the Port Authority Aviation Signing and Wayfinding Standards. {R}

6.4.2 Restroom identifiers (Men/Ladies/Families) shall be clear and visible and consistent with Port Authority Aviation Signing and Wayfinding Standards. {R}

6.4.3 When restrooms are being cleaned, or are closed for any reason, appropriate signing shall advise customers of other restrooms in close proximity. {R}

6.4.4 If sanitary dispensers are not available in the restrooms, an appropriate sign in the restroom shall reflect the nearest place to purchase these items. {R}

7.0 - Gate Areas

Gate Areas General Requirements

a) Seating shall be consistent with Port Authority Aviation Terminal Planning Standards. {R}

b) Public address system shall be available in every gate area. {R}

c) Flight Information Display Systems shall be available in or around the gate areas. {R}

7.1 Standards of Cleanliness

7.1.1 Seating shall be clean and free of debris and stains. {R}

7.1.2 Windowsills shall be free of dust and debris. {R}

7.1.3 Windows shall be clean and free of streaks and smudges. {R}

7.1.4 Trash receptacles shall be clean and not overflowing. {R}

7.1.5 Walls and columns shall have a clean appearance free of dirt and marks. {R}

7.1.6 Carpet and floors shall be free of debris and stains and shall appear clean. {R}

7.1.7 Floors shall be dry, free of spills or water. {H}

7.1.8 Ceilings shall be clean and free of dust. {R}

7.1.9 Light fixtures and assemblies shall be clean and free of dust. {R}

7.1.10 Telephones and telephone areas shall be clean and be free of debris. {R}

7.1.11 Heating and air conditioning units shall be clean and dust free. {R}

7.1.12 Stanchions, ropes and "tensa barriers" shall be clean and free of dust, tape and smudges. {R}

7.1.13 Counters/podiums and kiosks shall be clean, uncluttered and free of debris. {R}

7.1.14 Advertising and display areas shall be clean and free of debris. {R}

7.2 Standards of Condition

7.2.1 Seating shall be free of rips, tears and broken parts. {R}

7.2.2 Windowsills shall be in good condition, with no marks, scratches or broken pieces. {R}

7.2.3 Windows shall be in good condition, free of scratches or marks. {R}

7.2.4 Trash receptacles shall be in good working condition, without dents, marks, or peeling paint. {R}

7.2.5 Walls and columns shall be in good condition, without marks, scuffs, dents or gouges. {R}

7.2.6 Carpet shall be free of holes, rips, worn or frayed areas and flooring shall be free of large gouges, cracks and broken pieces. {H}

7.2.7 Ceilings shall be in good condition, evenly aligned and free of visible damage. {R}

7.2.8 All light fixtures shall be in working order with no visible broken parts. {R}

7.2.9 Telephone and telephone areas shall be in good condition, with no broken pieces. {R}

7.2.10 Heating and air conditioning units shall be in good working condition. {R}

7.2.11 Stanchions, ropes and "tensa-barriers" shall be in good working condition, with no visible damage or broken parts. {R}

7.2.12 Counters/podiums and kiosks shall be in good condition with no gouges, scratches, graffiti or broken pieces. {R}

7.2.13 Advertising and display areas shall be in good repair and shall be consistent with Port Authority Aviation Signing and Wayfinding Standards. {R}

7.2.14 Cleaning supplies and equipment shall be stored out of customers' view when not in use and closet doors kept closed. {H}

7.3 Standards of Functionality

7.3.1 The Public Address System shall be clear and audible at all times. {H}

7.3.2 All lighting shall conform to the Illuminating Engineering Society of North America (IES) standards: **Gate Areas—38 foot-candles**. {H}

7.3.3 Flight Information Display System (FIDS) monitors shall be clear, visible, accurate and in working order. {R}

7.3.4 Telephones shall be in working order. {R}

7.3.5 Television monitors shall be clear, visible and in good working condition. {R}

7.3.6 In the event of delays, cancellations or diversions, Standard 17.0 will apply. {H}

7.4 Signs, Directions, and Information

7.4.1 Signing shall be visible and adequate to direct customers to all services. {R}

7.4.2 Handwritten signs shall not be used and temporary signs must be consistent with the Port Authority Aviation Signing and Wayfinding Standards. {R}

7.4.3 Appropriate directional signing shall be visible at every decision point and consistent with Port Authority Aviation Signing and Wayfinding Standards. {R}

8.0 - Retail Services

8.1 Standards of Cleanliness

8.1.1 All public areas in the retail space shall be clean, well maintained and free of unpleasant odors. {R}

8.1.2 Carpet and floors shall be free of debris and stains and shall appear clean. {R}

8.1.3 Glass windows and display cases shall be clean. {R}

8.1.4 Light fixtures and assemblies shall be clean and free of dust. {R}

8.1.5 All walls and columns shall be clean. {R}

8.1.6 Ceilings shall be clean and free of dust. {R}

8.1.7 Sales and cashier areas shall appear neat, organized and clean. {R}

8.1.8 Heating and air conditioning units and vents shall be clean and free of dust. {R}

8.1.9 Television monitors shall be clean and free of dust. {R}

8.2 Standards of Condition

8.2.1 Carpets shall be free of holes, rips and worn or frayed areas. {R}

8.2.2 Floors shall be free of large cracks, gouges and excessively worn areas. {R}

8.2.3 Entranceways shall be in good condition, free of marks, scratches or any visible damage. {R}

8.2.4 Security grille/shutters and/or roll gates shall be without defect when deployed or otherwise kept out of sight. {R}

8.2.5 Furniture, display cases, shelving and fixtures shall be in good condition with no gouges, scratches, graffiti or broken pieces. {R}

8.2.6 All light fixtures shall be in working order with no visible broken parts. {R}

8.2.7 Walls and columns shall be free of large cracks, holes and graffiti. {R}

8.2.8 Apparel and accessories shall be neatly folded or hung in the appropriate area. {R}

8.2.9 All displays and racks shall be arranged so as to permit free movement by customers with carry-on baggage. {R}

8.2.10 Stock shall be stored out of view of customers and stored within one (1) hour of delivery. {R}

8.2.11 Ceilings shall not be stained or have any broken tiles. {R}

8.2.12 Employees' personal belongings shall not be visible to customers. {R}

8.2.13 Heating and air conditioning units shall be in good working order. {R}

8.2.14 Packaging, shipping materials and delivery carts shall be removed within one (1) hour from all public areas. {R}

8.3 Standards of Functionality

8.3.1 In the event of flight delays, essential services shall remain open for passengers in the terminal after normal business hours. {H}

8.3.2 All lighting shall conform to the Illuminating Engineering Society of North America (IES) standards: **Retail – 72 foot-candles**. {H}

8.3.3 Music system shall be in a clear and audible working condition with appropriately set volume level. {H}

8.3.4 All entrances to establishments shall be kept clear of merchandise and sales/advertising stanchions. {R}

8.3.5 Television monitors shall be clear, visible and in good working condition. {R}

8.4 Signs, Directions, and Information

8.4.1 Store policies regarding credit cards, returns/refunds, etc. shall be clearly displayed. {R}

8.4.2 Operators shall prominently display "Street Pricing" signing. {R}

8.4.3 A telephone number shall be visible so customers can call with complaints or compliments. {R}

8.4.4 Tip receptacles are not permitted. {R}

8.4.5 Hours of operations shall be prominently displayed and fully observed. {R}

8.4.6 Appropriate signing shall be visible, and clearly direct customers to all retail facilities. {R}

8.4.7 Handwritten signs shall not be used and temporary signs shall be consistent with the Port Authority Aviation Signing and Wayfinding Standards. {R}

8.4.8 Illuminated signs shall be in proper working condition. Flashing or blinking signs shall not be used, and the use of red LED (Light Emitting Diode) signs is discouraged. Red LED signs shall not be used in all new installations. {R}

8.4.9 Retail areas under construction shall be provided with professional signs on barricades with an "opening date" whenever possible, and may include a rendering of the new facility. Signing shall be updated as necessary. {R}

8.4.10 When a retail outlet is closed for unscheduled reasons, appropriate signs shall be posted advising customers of the nearest, similar operating retail outlet. {R}

8.4.11 There shall be no unauthorized postings. {R}

8.4.12 All retail outlets offering sale of Metro Cards shall have appropriate signing. {R}

8.5 Standards of Retail Employees

In addition to the following standards, all employees shall conform to the same Employee Attitude, Appearance, Awareness and Knowledge as outlined in Standard 1.0.

8.5.1 Employees shall be able to direct customers to other outlets if item is not available in their shop. {R}

8.5.2 Employees shall always offer customers a receipt and say "thank you" or an appropriate pleasant closing. {R}

8.5.3 Employees shall always give correct change. {R}

8.5.4 Employees shall make every effort to make change for customers or direct customers to nearest change machine, i.e. for telephone calls. {R}

8.5.5 All shops shall have sufficient cash available immediately upon opening to make change for early morning sales. {R}

8.5.6 Any complaints shall be dealt with promptly. {R}

8.5.7 Employees shall have appropriate knowledge of items being sold. {R}

8.5.8 Employees shall not use personal electronic devices, including but not limited to cell phones and MP3 players. The only musical audible to customers shall be provided by the audio system. {R}

8.6 Standards of Product

8.6.1 All items shall be sold at "Street Prices" as defined in the lease/permit. {R}

8.6.2 Merchandise shall be attractively displayed. {R}

8.6.3 Terminal Operators shall ensure that concessionaires provide a variety of items that meet customers' needs, both before and after security, including: reading materials (selection of periodicals and books), candy and snacks, health and beauty items, travel and business supplies, discretionary items such as local gifts, souvenirs and toys, and other sundries. {R}

8.6.4 Damaged merchandise shall be removed from display areas immediately. {R}

8.6.5 Displays shall be maintained to provide an uncluttered appearance. {R}

8.6.6 All prices shall be clearly displayed. {H}

8.6.7 No items shall remain on shelves past expiration dates. {R}

8.6.8 Merchandise shall be stocked in quantities sufficient for normal customer traffic. {R}

8.6.9 Merchandise shall be delivered to shops in appropriate carts and at non-peak periods or during off-hours whenever possible. {H}

9.1 Standards of Cleanliness

9.1.1 All areas in the establishment shall be clean and well maintained. {R}

9.1.2 Debris shall be removed from tables and counters within two minutes. {R}

9.1.3 Area shall be free of unpleasant odors. {R}

9.1.4 Carpet and floors shall be free of debris and stains and shall appear clean. {R}

9.1.5 Entranceways and frames shall be free of smudges, dirt and grime. {R}

9.1.6 Ceilings shall be clean and free of dust. {R}

9.1.7 Glass windows and display cases shall be clean. {R}

9.1.8 All food used for display purposes shall be changed regularly. {R}

9.1.9 Sales and cashier areas shall appear organized and clean. {R}

9.1.10 Tray slides shall be clean. {R}

9.1.11 Trays shall be sanitized after every use. {H}

9.1.12 Light fixtures and assemblies shall be clean and free of dust. {R}

9.1.13 Exhaust hoods, ducts, fans and filters shall be clean and appropriately maintained. {R}

9.1.14 All visible cooking equipment shall be clean. {R}

9.1.15 Trash receptacles shall be emptied in order to prevent the overflow of debris. {R}

9.1.16 Heating and air conditioning units and vents shall be clean and free of dust. {H}

9.1.17 Television monitors shall be clean and free of dust. {R}

9.2 Standards of Condition

9.2.1 Carpets shall be free from holes, rips and worn or frayed areas. {R}

9.2.2 Floors shall be free of large cracks, gouges and excessively worn areas. {R}

9.2.3 Entranceways and frames shall be in good condition, free of marks, scratches or any visible damage. {R}

9.2.4 All tables, chairs, booths, display cases, and fixtures shall be in good condition with no deep scratches, gouges, graffiti or broken pieces. {R}

9.2.5 All visible cooking equipment shall be well maintained and in good working order. {R}

9.2.6 Ceilings shall be free of stains and broken tiles. {R}

9.2.7 All light fixtures shall be in working order with all visible lamps operating and all burned out lights replaced, with no broken visible parts. {R}

9.2.8 Packaging, shipping materials and delivery carts shall be removed within one (1) hour from all public areas. {R}

9.2.9 Cleaning supplies and equipment shall be stored out of customers' view when not in use and closet doors kept closed. {H}

9.2.10 Trash receptacles shall be clean and in good condition, without dents, marks or peeling paint. {R}

9.2.11 Employees' personal belongings shall not be visible to customers. {R}

9.2.12 Heating and air-conditioning units shall be in good condition, free of any visible damage. {R}

9.2.13 Television monitors shall be clear, visible and in good working condition. {R}

9.3 Standards of Functionality

9.3.1 In the event of flight delays or cancellations, hours of operations shall be extended to accommodate passengers. {H}

9.3.2 All lighting shall meet and conform to the Illuminating Engineering Society of North America (IES) standards: **Dining Area—23 foot-candles**. {H}

9.3.3 Music system shall be clear and audible with appropriately set volume level. {H}

9.3.4 All entrances to establishments shall be clear of merchandise and sales/advertising stanchions and not obstruct entrance. {R}

9.3.5 Heating and air conditioning units shall be in working order. {R}

9.4 Signs, Directions, and Information

9.4.1 Store policies regarding credit cards shall be clearly displayed. {R}

9.4.2 Operators shall prominently display "Street Pricing" signing. {R}

9.4.3 Tip receptacles are not permitted. {R}

9.4.4 Operators shall clearly display a telephone number for customer complaints or compliments. {R}

9.4.5 Hours of operations shall be prominently displayed and fully observed. {R}

9.4.6 Appropriate signing shall be visible to direct customers to all food and beverage facilities. {R}

9.4.7 Handwritten signs shall not be used and all temporary signs shall be consistent with the Port Authority Aviation Signing and Wayfinding Standards. {R}

9.4.8 Illuminated signs shall be in proper working condition. Flashing or blinking signs shall not be used, and the use of red LED (Light Emitting Diode) signs is discouraged. Red LED signs shall not be used in new installations. {R}

9.4.9 Food and Beverage areas under construction shall be provided with professional signs on barricades with an "opening date" whenever possible and may include a rendering of the new facility. Signing shall be updated as necessary. {R}

9.4.10 When food and beverage facilities are closed, appropriate signs shall be posted advising customers of the nearest, operating facilities. {R}

9.4.11 There shall be no unauthorized postings. {R}

9.5 Standards of Food and Beverage Employees

In addition to the following standards, all employees shall conform to the same Employee Attitude, Appearance and Knowledge as outlined in Standard 1.0.

9.5.1 Employees shall be able to direct customers to other outlets if an item is not available in their shop. {R}

9.5.2 Employees shall always provide customers with a receipt and "thank you" or an appropriate pleasant closing. {R}

9.5.3 Employees shall always give correct change. {R}

9.5.4 Employees shall make every effort to make change for customers, i.e. for telephone calls. {R}

9.5.5 Employees shall not use personal electronic devices, including but not limited to cell phones and MP3 players. The only music audible to customers shall be provided by the unit audio system. {R}

9.5.6 All shops shall have sufficient cash available immediately upon opening to make change for early morning sales. {R}

9.5.7 Any complaints shall be dealt with promptly. {R}

9.6 Standards of Product

9.6.1 Terminal Operators shall ensure that concessionaires provide a variety of menu items that meet customers' needs, both before and after security, including: hot and cold menu items for breakfast, lunch and dinner; hot and cold beverages (non-alcoholic and alcoholic); quick serve meals to go; sit down restaurant facilities; and a selection of healthy dishes (low fat, salads, etc.). {R}

9.6.2 Menus shall be well designed, clean and display the correct prices. {R}

9.6.3 All items shall be sold at "Street Prices" as defined in the lease/permit. {R}

9.6.4 No items shall remain on shelves past expiration dates. {H}

9.6.5 Operators shall make every attempt to ensure that all menu items are available. {R}

9.6.6 Hot food shall be delivered hot and cold food shall be delivered cold. {R}

9.6.7 Merchandise shall be delivered, whenever possible, to food and beverage areas in appropriate carts and at non-peak periods or during off-hours. {H}

10.0 - Baggage Claim

Baggage Claim General Requirements

a) Baggage carts shall be readily available at all cart racks at all times. {H}

b) Public Address System (PAS) shall be available. {H}

c) Information display on baggage belt shall be available. {R}

10. 1 Standards of Cleanliness

10.1.1 Baggage carousels shall be wiped clean and be free of debris. {R}

10.1.2 Carpet and floors shall be free of debris and stains and shall appear clean. {R}

10.1.3 Trash receptacles shall be clean and not overflowing with debris. {R}

10.1.4 Heating and air conditioning units shall be clean and free of dust. {R}

10.1.5 Ceilings shall be clean and free of dust. {R}

10.1.6 Light fixtures and assemblies shall be clean and free of dust. {R}

10.1.7 Seating shall be clean and free of stains. {R}

10.1.8 Windowsills shall be free of dust and debris. {R}

10.1.9 Windows shall be clean and free of streaks and smudges. {R}

10.1.10 Walls and columns shall have a clean appearance, free of dirty and marks. {R}

10.1.11 Conveyor curtains shall be clean and free of dirt and debris. {R}

10.2 Standards of Condition

10.2.1 All carousels shall be in good condition with no gouges, scratches, graffiti or broken pieces. {R}

10.2.2 Carpet shall be free of holes, rips, worn or frayed areas and flooring shall be free of large gouges, cracks and broken pieces. {H}

10.2.3 Trash receptacles shall be in good condition, without dents, marks or peeling paint. {R}

10.2.4 Heating and air conditioning units shall be in good working condition. {R}

10.2.5 Ceilings shall be in good condition, evenly aligned and free of visible damage. {R}

10.2.6 Seating shall be free of rips, tears and broken parts. {R}

10.2.7 Windowsills shall be in good condition, free of scratches or marks. {R}

10.2.8 Windows shall be in good condition, free of scratches or marks. {R}

10.2.9 Walls and columns shall be free of large cracks, holes and graffiti. {R}

10.2.10 Cleaning supplies and equipment shall be stored out of customers' view when not in use and closet doors kept closed. {H}

10.2.11 All light fixtures shall be in working order with no visible broken parts. {R}

10.2.12 Unattended baggage carts shall be returned to the dispenser racks promptly and not allowed to collect in an unsightly manner and impede passenger flow. {R}

10.2.13 Conveyor curtains shall be in good condition free of rips, tears and broken parts. {R}

10.3 Standards of Functionality

10.3.1 Baggage carousels shall be in good working order and have no areas that could cause damage to baggage or injury to customers. {H}

10.3.2 The Public Address System shall be clear and audible. {H}

10.3.3 All information display systems shall be clear, visible and accurate and in good working order. {H}

10.3.4 Television monitors shall be in good working condition. {R}

10.3.5 All lighting shall meet and conform to the Illuminating Engineering Society of North America (IES) standards: **Baggage Area—35 foot-candles.** {H}

10.3.6 Unclaimed baggage shall be moved to and stored in a secure area in accordance with Federal and local regulations, as well as air carrier or Terminal Operator's requirements. {R}

10.3.7 Speed of arrival baggage delivery shall be consistent with industry practice ;and may vary depending on load factors, where the aircraft is parked (terminal gate or remote parking location), domestic or international flights but in all cases baggage delivery shall not exceed:

- For all aircraft, the first bag shall be delivered within fifteen (15) minutes after block time or after the first passenger arrives in the baggage claim area. {H}
- For narrow-body aircraft, the last bag shall be delivered within thirty (30) minutes after block time. {H}
- For wide-body aircraft, the last bag shall be delivered within fifty (50) minutes after block time. {H}

10.3.8 Accuracy of baggage delivery shall not exceed monthly average of mishandled baggage as published by the US DOT Air Travel Consumer Report. {H}

10.4 Signs, Directions, and Information

10.4.1 Signing shall be visible and adequate to direct customers to all services. {R}

10.4.2 Handwritten signs shall not be used and temporary signs must be consistent with Port Authority Aviation Signing and Wayfinding Standards. {R}

10.4.3 All baggage carousels shall be clearly identified and where applicable, by airline. {R}

10.4.4 In the event baggage delivery is delayed, a public address announcement regarding the delay shall be made in the baggage claim area. Passengers shall be kept informed as to the status of baggage delivery. {R}

10.4.5 Advertising and display areas shall be in good repair and shall be consistent with Port Authority Aviation Signing and Wayfinding Standards. {R}

11.0 - Ground Transportation & Welcome Centers

11.1 Standards of Cleanliness

Welcome Centers

11.1.1 Counters shall appear clean and organized, uncluttered and without visible damage. {R}

11.1.2 Computers and monitors shall be clean and free of dust. {R}

11.1.3 All telephones, including self-service phones shall be clean and free of debris. {R}

11.1.4 All panels and displays including self-service areas shall be clean and free of debris. {R}

On-Airport Bus Services

11.1.5 All vehicle lighting shall be clean and free of debris. {R}

11.1.6 Vehicle exteriors shall be clean and have a freshly washed appearance. {R}

11.1.7 Vehicle interiors shall be clean and free of debris. {R}

11.1.8 Pictures, frames and advertising shall be clean and free of dust and graffiti. {R}

11.1.9 All glass shall be clean and free of streaks and smudges, and dirt and grime. {R}

11.1.10 Seating shall be clean and free of graffiti. {R}

Permittee Services

11.1.11 Vehicle exteriors shall be clean and have a freshly washed appearance. {R}

11.1.12 Vehicle interiors shall be clean and free of debris. {R}

11.1.13 All glass shall be clean and free of streaks and smudges, and free of dirt and grime. {R}

11.1.14 Seating shall be clean and free of graffiti. {R}

Bus Shelters

11.1.15 All bus shelter exteriors shall be clean and have a freshly washed appearance. {R}

11.1.16 All bus shelter interiors shall be clean and free of debris. {R}

11.1.17 Pictures, frames and advertising shall be clean and free of dust and graffiti. {R}

11.1.18 All glass shall be free of streaks and smudges, and dirt and grime. {R}

11.1.19 Seating shall be clean and free of graffiti. {R}

11.1.20 Light fixtures and assemblies shall be clean and free of dust. {R}

11.1.21 All sidewalks shall be clean and free of debris including gum and cigarettes. {R}

11.2 Standards of Condition

Welcome Centers

11.2.1 Counters and workspaces shall be maintained in good condition with no gouges, scratches, graffiti or broken pieces. {R}

11.2.2 Computers and monitors shall be in good working condition. {R}

11.2.3 All telephones, including self-service phones shall be in good condition. {R}

11.2.4 All panels and displays shall be in good condition, free of marks, scratches, gouges and any visible damage. {R}

11.2.5 Employee's personal belongings shall not be visible to customers. {R}

Airport Bus and Permitee Services

11.2.6 All vehicle lighting shall be operational with all lamps lit and no visible broken parts. {H}

11.2.7 Vehicular body damage shall be repaired promptly. {R}

11.2.8 Pictures, frames and advertising shall be in good condition with no marks, scratches or visible damage. {R}

11.2.9 All glass shall be in good condition, free of scratches, chips and broken pieces. {R}

11.2.10 Seating shall be free of tears, rips and missing or broken pieces. {R}

11.2.11 Employee's personal belongings shall not be visible to customers. {R}

11.2.12 All bus shelters shall be in good condition with no gouges, scratches, graffiti or broken pieces. {R}

Permittee Services

11.2.13 Vehicle exteriors shall be in good condition, with all damage repaired promptly. {R}

11.2.14 Vehicle interiors shall be in good condition. {R}

11.2.15 All glass shall be in good condition, free of marks, scratches and broken pieces. {R}

11.2.16 Seating shall be free of rips, tears and missing or broken pieces. {R}

Bus Shelters

11.2.17 All bus shelter exteriors shall be in good condition with no visible damage. {R}

11.2.18 All bus shelter interiors shall be in good condition, free of missing or broken pieces. {R}

11.2.19 Pictures, frames and advertising shall be in good condition, free of scratches and graffiti. {R}

11.3 Standards of Functionality

Welcome Centers

11.3.1 All customer care representatives shall be knowledgeable in all alternate modes of transportation in the event of transportation delays. {R}

11.3.2 All lighting shall conform to Illumination Engineering Society of North America (IES) standards as they pertain to this area and activity. {R}

11.3.3 All buses must be equipped with automated recording announcements or the bus drivers must make audible announcements of the airport terminal or bus stops. {H}

11.3.4 Computers and monitors shall function properly, {R}

11.3.5 All telephones, including self-service telephones, shall function properly. {R}

On-Airport Bus Services

11.3.6 Vehicles shall not make excessive noise or give off unpleasant odors and fumes. {H}

11.3.7 Air conditioning and heaters shall be in proper working condition and maintain appropriate temperatures. {R}

11.3.8 Doors shall operate properly and easily. {H}

11.3.9 Waiting time during peak periods shall not exceed fifteen (15) minutes. {R}

11.3.10 Public Address systems and announcements shall be clear audible, and up to date. {R}

11.3.11 Handicapped lifts or "kneeling bus" apparatus shall function properly as referenced to Standard 19.0 "Passengers with Reduced Mobility". {R}

Permittee Services

11.3.12 Vehicles shall not make excessive noise or give off unpleasant odors and fumes. {H}

11.3.13 Air conditioning and heaters shall be in proper working condition and maintain appropriate temperatures. {R}

11.3.14 Only authorized permittees shall make pick-ups at designated areas. {R}

11.4 Signs, Directions and Information

Welcome Centers

11.4.1 All signs and postings shall be consistent with Port Authority Aviation Signing and Wayfinding Standards. {R}

11.4.2 Welcome Center waiting area shall be clearly identified. {R}

11.4.3 All transportation information shall be accurate and up to date. {H}

11.4.4. All Ground Transportation telephone information panels shall be consistent with Port Authority Aviation Signing and Wayfinding Standards. {R}

On-Airport Bus Services

11.4.5. Buses, vans and free shuttle vehicles shall be easily identifiable and have route/destination signs clearly posted. {R}

11.4.6. Pick-up locations shall be clearly designated. {R}

11.4.7. Handwritten signs shall not be used and temporary signs must be consistent with Port Authority Aviation Signing and Wayfinding Standards. {R}

11.4.8. All "Variable Message Signs" shall operate properly and display the correct information. Red "LED" (Light Emitting Diodes) signs shall not be used in new applications. {R}

11.4.9. Airline directories, where posted, shall be current and up-to-date. {R}

Bus Shelters

11.4.10. Bus wait times shall be prominently displayed. {R}

11.4.11. Airline directories, where posted, shall be current and up-to-date. {R}

11.5 Assistance to Passengers with Reduced Mobility by Permitted Ground Transportation Operators (See Standard 19.0)

11.5.1 Permitted bus and van ground transportation operators will provide regular service or para-transit or other special transportation service at no additional cost for persons with reduced mobility, including those persons using non-collapsible motorized wheelchairs. {R}

11.5.2 Permitted bus and van ground transportation operators should provide the service described above at posted times or as agreed upon for pre-arranged service or within fifteen (15) minutes of the agreed upon pick-up time at the Welcome Center.{R}

12.0 - Taxi Dispatch Service

12.1 Standards of Cleanliness

12.1.1 Taxi booths shall have clean windows and be free of graffiti. {R}

12.1.2 Taxi booth interiors shall be clean and free of visible clutter, such as newspapers, books, magazines and personal electronic devices. {R}

12.1.3 Taxi passengers waiting areas shall be clean and free of debris including gum and cigarettes. {R}

12.2 Standards of Condition

12.2.1 Taxi booths windows shall be in good condition, free of scratches and broken pieces. {R}

12.2.2 All taxi booths shall be in good condition with no dents, scrapes, debris or peeling paint. {R}

12.2.3 Taxi passenger waiting areas shall be in good condition with no cracks or missing surface areas. {R}

12.2.4 Queue line railing, where installed, shall be free of defects. {R}

12.3 Functionality

12.3.1 In the event of a shortage of taxicabs, staff shall advise customers of alternative means of transportation. {R}

12.3.2 Queues for taxi service shall not exceed twenty (20) customers on line or customers shall not wait more than ten (10) minutes. {H}

12.4 Signs, Directions, and Information

12.4.1 Handwritten signs shall not be used and temporary signs shall be consistent with the Port Authority Aviation Signing and Wayfinding Standards. {R}

12.4.2 A plaque with the Taxi Dispatcher's name shall be clearly visible at each Taxi Dispatch Booth. {R}

12.4.3 Taxi rate information must be posted or be provided to the passengers. {R}

12.5 Standards of Taxi Dispatch Employees

In addition to the following standards, all employees shall conform to the same Employee Attitude, Appearance and Knowledge standards as outlined in Standard 1.0.

12.5.1 Taxi dispatch employees must be knowledgeable regarding taxi fares, tolls and distances to locations. {H}

12.5.2 Taxi dispatch employees shall not solicit or accept any tips. {H}

13.0 - Parking Lots & Garage Services

13.1 Standards of Cleanliness

13.1.1 Crosswalks, sidewalks and parking lot surfaces shall be clean and free of all dirt and debris. {R}

13.1.2 Escalators and elevators shall be clean and free of debris. {R}

13.1.3 Trash receptacles shall be emptied in order to prevent the overflow of debris. {R}

13.1.4 All structures and equipment shall be free of dirt and graffiti. {R}

13.1.5 All light fixtures and assemblies shall be clean and free of graffiti. {R}

13.1.6 All windows shall be clean and free of streaks and smudges and be clear of obstructions. {R}

13.1.7 Parking lot bus shelters shall be clean and free of debris. {R}

13.1.8 Cashier booth interiors shall be clean and free of visible clutter, such as newspapers, books, magazines, and personal belongings. {R}

13.1.9 Drains shall be clear and free of debris. {R}

13.1.10 Unpleasant odors shall not be detected. {R}

13.1.11 Telephones and telephone areas shall be clean and free of debris. {R}

13.2 Standards of Condition

13.2.1 Parking lot surfaces shall be well maintained, smooth and free of potholes and weeds. {R}

13.2.2 Escalators and elevators shall be in good condition with no gouges, scratches, graffiti and broken pieces. {R}

13.2.3 Trash receptacles shall be in good condition, without dents, marks or peeling paint. {R}

13.2.4 All equipment including Ticket Issuing Machines (TIM's) shall be in good condition. {R}

13.2.5 All structures shall be in good condition with no gouges, scratches, graffiti or broken pieces or rust. {R}

13.2.6 All light fixtures shall be in working order with no visible broken parts. {R}

13.2.7 All windows shall be in good condition, free of marks, scratches and broken or missing pieces. {R}

13.2.8 All bus shelters shall be in good condition with no gouges, scratches, graffiti or broken pieces. {R}

13.2.9 There shall be no standing water more than one-half inch (1/2") deep, eight (8) hours after a rainstorm. {R}

13.2.10 Phone and intercoms shall be in good condition with no gouges, scratches, graffiti or broken pieces. {H}

13.2.11 Striping shall be visible. {R}

13.2.12 Unattended baggage carts and wheelchairs shall be returned to dispenser racks or appropriate location promptly or located so as not to impede the flow of passengers or vehicles, and not allowed to collect in an unsightly manner. {R}

13.2.13 All fences and barriers shall be well maintained, rust free and properly secured. {R}

13.3 Standards of Functionality

13.3.1 All lighting shall conform to Illumination Engineering Society of North America (IES) standards as they pertain to this area and activity. {H}

13.3.2 Properly uniformed and identifiable personnel shall be readily available to assist customers during designated travel periods and to respond to emergency situations within twenty (20) minutes of the customer's request. {H}

13.3.3 All equipment shall be functioning and in good working order. {R}

13.3.4 Every parking lot shelter shall have an emergency phone in good working order with clear instructions. {H}

13.3.5 All telephone and intercoms shall be in good working order with appropriate volume and all functions operating. {H}

13.3.6 Escalators and elevators shall be in working order. {R}

13.3.7 Elevator button lights and switches shall be operational. {R}

13.3.8 Each elevator emergency phone or communication device shall be in working condition. {H}

13.3.9 A "red light" shall be displayed indicating a closed lane. {R}

13.3.10 Vehicle queues at parking exit plazas shall not exceed a maximum allowable queue length or other measurable criteria as defined in the parking operators agreement with the Port Authority. {R}

13.4 Signs, Directions, and Information

13.4.1 Parking rates and fees, indicating the maximum rate for a 24-hour period as well as the credit cards accepted, shall be prominently displayed at all entrances and consistent with Port Authority Aviation Signing and Wayfinding Standards. {R}

13.4.2 Handwritten signs shall not be used and all temporary signs shall be consistent with the Port Authority Aviation Signing and Wayfinding Standards. {R}

13.4.3 Aisle numbers and markings shall be visible and consistent with Port Authority Aviation Signing and Wayfinding Standards. {R}

13.4.4 Signing in bus shelters shall display the bus stop number, the schedule, or frequency of service, airline locations (at LGA) and route information and be consistent with Port Authority Aviation Signing and Wayfinding Standards. {R}

13.4.5 Signing for "help" phones and services shall be clear and visible and consistent with Port Authority Aviation Signing and Wayfinding Standards. {R}

13.4.6 A plaque with the cashier's name and a telephone number for customer comment or complaint shall be clearly visible at each cashier booth. {R}

13.4.7 Emergency phones shall be clearly marked/identifiable and readily available. {H}

13.5 Standards of Parking Employees

In addition to the following standards, all employees shall conform to the same Employee Attitude, Appearance and Knowledge as outlined in Standard 1.0.

13.5.1 If requested, parking employees shall be capable of providing driving directions to other major airports and off airport areas verbally and/or with printed materials. {R}

13.5.2 Employees shall provide a "thank you" or an appropriate pleasant closing to every customer. {R}

13.5.3 Parking employees shall not solicit or accept any tips. {H}

14.0 - Construction

All areas undergoing renovation or construction shall present a neat appearance with all necessary signing in place and appropriate safety measures taken. Moreover, adherence to all procedures outlined in the Tenant Alteration Procedures and Standards Guide is essential.

14.1 Standards of Cleanliness

14.1.1 All surface areas in proximity to the work site shall be free of dust and debris and present a clean appearance. {R}

14.1.2 Temporary walls and screening shall be free of graffiti, dirt and debris. {R}

14.2 Standards of Condition

14.2.1 No work area shall present a hazard, which may cause a customer or employee to slip, fall or be hit by falling debris or construction materials. {H}

14.2.2 Temporary walls shall be finished with visibly attractive scenes or renderings of the project or any temporary signs consistent with Port Authority Aviation Signing and Wayfinding Standards. {R}

14.2.3 Storefronts under construction shall have a "uniform" barrier wall or "window dressing" that is attractive and conceals construction activity, as indicated in the Tenant Alteration Application (TAA). {R}

14.2.4 Air conditioning and heating shall be uninterrupted in the public areas of the airport facility. {H}

14.2.5 Floors shall be dry and free of spills or water. {R}

14.2.6 Temporary walls/barricades shall be well maintained with no holes, dents, marks or tears. {R}

14.2.7 All light fixtures shall be in working order with no visible broken parts. {R}

14.2.8 No unpleasant odors shall be emitted from the construction site. {R}

14.2.9 Sound suppression efforts shall be employed that meets the airport's operational restrictions on noise in passenger terminal buildings. This may include confining work to certain times of the day. Whenever possible, construction equipment, electrical equipment and tools shall not be visible to customers. {R}

14.2.10 Construction workers shall obtain and prominently display official identification. {H}

14.3 Standards of Functionality

14.3.1 Placement of construction walls or other interior construction activities shall not degrade existing lighting quality or standards in the vicinity of the construction area. {R}

14.3.2 All lighting shall conform to Illuminating Engineering Society of North America (IES) standards. {R}

14.3.3 Construction activity shall be designed to minimize interference with passenger circulation paths, and if construction does impede with circulation alternative routes will be established in a safe manner. {H}

14.3.4 Construction employees shall comply with all relevant Port Authority "Airport Rules and Regulations". {R}

14.4 Signs, Directions, and Information

14.4.1 Signing and information shall be made available to customers explaining the benefits of the project, what is being renovated or constructed, and when it will be completed. {R}

14.4.2 Signs designating alternate facilities shall provide clear directions and hours of operation. {R}

14.4.3 Adequate directional signing, consistent with Port Authority Aviation Signing and Wayfinding Standards, shall be provided when construction barricades hide or obstruct facilities, egress, and services. {R}

14.4.4 Handwritten signs shall not be used and temporary signs must be consistent with Port Authority Aviation Signing and Wayfinding Standards. {R}

15.0 - Charter Operations

These standards are being issued to Terminal Operators, Aircraft Owners and/or Tour Operators involved in the operation of charter flights and exclude scheduled carriers. All standards in this section are rated as high priority.

15.1 Standards for Representation

15.1.1 For arrivals only, an authorized representative of the aircraft owner and/or tour operator shall sign in and sign out with the Terminal Operator and be on duty one (1) hour prior to the scheduled arrival of the aircraft and two (2) hours after aircraft arrival.

15.1.2 For departures only, the aircraft owner or tour operator(s) shall have a minimum of one authorized representative on duty at least two and one-half (2-1/2) hours prior to the scheduled departure of the aircraft and shall remain on duty until the flight is airborne. The representative shall sign-in and sign-out with the Terminal Operator.

15.1.3 Aircraft owner or tour operator(s) representatives shall be empowered to assist stranded passengers in all areas of customer service. (See Standard 17.0)

15.1.4 Prior to the approval of a schedule, the aircraft owner or tour operator(s) shall provide the Port Authority and the Terminal Operator with:

a. The name of the Company responsible for providing information, assistance and accommodations to passengers in the event of a delay, cancellation or other problem situation;

b. Name(s) of all authorized representative(s) on duty;

c. 24-hour telephone contact;

d. 24-hour fax number;

e. E-mail address;

f. Mailing address;

g. The name of ground handling company;

h. Name and contact of handling company's authorized representative;

i. Name of company or party responsible for all fees including, but not limited to: landing, passenger fees, handling, fuel, catering, security, passengers' inconvenience, mishandled baggage, additional maintenance, etc.

j. Provide website address for posting of information.

15.1.5 The Company responsible for all fees and ancillary costs shall post a bond in an amount and form at the discretion of the Port Authority prior to each season during which it plans to operate.

15.1.6 The Company responsible for all fees and ancillary cost shall confirm in writing to the Port Authority and the Terminal Operator that it has obtained all slot approvals and shall identify the handling company and location for processing arriving and departing passengers and baggage for all tenant operated facilities.

15.1.7 An Airline or ground handling company that enters into an agreement with an aircraft owner or tour operator(s) to provide facilities, passenger and baggage check-in and assistance on arrival, shall include these standards in the arrangements and make every effort to assist stranded passengers.

15.2 Standards for Information

15.2.1 The proposed flight schedule shall be provided to the Port Authority at least 72 hours prior to the flights scheduled arrival or departure time. For EWR Terminal B operation requests, flight schedules shall be submitted at least fifteen (15) days prior.

15.2.2 Passengers shall be provided with access to 24 hour a day arrival and departure information.

15.2.3 Passengers shall be notified of all check-in and arrival location information including terminals, check-in locations and time requirements, as well as scheduled arrival time and procedures prior to their arrival at the airport.

15.2.4 For international flights, the aircraft owner or tour operator(s) shall notify passengers of all required documentation for originating and destination country.

15.3 Standards for Services in case of flight delay or cancellation

15.3.1 Authorized representative(s) shall inform passengers of flight status (delay or cancellation) no later than fifteen (15) minutes after scheduled departure time, and shall repeat an advisory process every thirty (30) minutes, or as required.

15.3.2 In accordance with airline's and/or terminal operator's procedures, food, refreshments, restroom facilities and medical assistance shall be made available as required.

15.3.3 When ticket prices for chartered flights include a package of airfare, hotel, meals and ground transportation, passengers shall be informed in advance and in writing of any re-accommodation, compensation or refund policy in the event of extensive (24 hours or more) delay or cancellation.

16.0 - Ramp and Airside Areas

Ramp and airside areas are clearly visible to the traveling public from departing and arriving aircraft as well as from airport terminals. Ramp condition, cleanliness and general appearance can greatly influence the overall perception of the airport and work towards accomplishing the goal of achieving customer satisfaction. These standards shall apply to all terminal operators, airlines, cargo facility operators, the Port Authority, ground service/handling companies and all their contractors and sub-contractors.

In order to implement and enforce the Ramp and Airside Airport Standards, a separate facility quality assurance review program will be developed with partners

16.1 Standards of Ramp Cleanliness

16.1.1 All Ramp/Airside areas shall be free of Foreign Object Debris (FOD) in accordance with FAA advisory Circular 150/5380-5B and Port Authority Rules and Regulations. {H}

16.1.2 All ramp areas under the responsibility of terminal operators or the airport authority shall be clean and free of debris, grease and oil and have "speedi-dry" type material available. {H}

16.1.3 Entrance and exit doors and frames to/from ramp areas shall be free of dirt and grime. {R}

16.1.4 All windows visible from ramp/airside shall be clean and free of streaks and smudges. {R}

16.1.5 All trash receptacles shall be emptied in order to prevent the overflow of debris. {R}

16.1.6 Walls, columns and doors shall be clean and free of graffiti. {R}

16.1.7 All service roads, as well as walkways and sidewalks shall be clean and free of debris. {R}

16.1.8 Interline Baggage transfer areas shall be clean and free of debris. {R}

16.1.9 All drains shall be clear and free of debris. {R}

16.1.10 Guard booth interiors shall be clean, free of debris, clutter and graffiti and have no personal items visible. {R}

16.1.11 Guard booth windows shall be clean and free of streaks and smudges, and dirt and grime. {R}

16.2 Standards of Equipment Cleanliness

16.2.1 All ground support equipment (motorized and non-motorized equipment) shall be clean and free of debris. {R}

16.2.2 Buses and/or Mobile Lounges shall be clean and have a freshly washed appearance. {R}

16.2.3 Bus and/or Mobile Lounge seating shall be clean and free of graffiti. {R}

16.2.4 Bus and/or Mobile Lounge windows shall be clean and free of streaks and smudges and free of dirt and grime. {R}

16.2.5 Bus and/or Mobile Lounge carpet and floors shall be free of debris and stains and shall appear clean. {R}

16.2.6 Aircraft loading bridges shall be clean and free of debris and have a freshly washed appearance. {R}

16.3 Standards of Ramp Condition

16.3.1 Unserviceable equipment (motorized and non-motorized) shall not be stored at the Air Terminal. Storage of such equipment is permitted on a temporary basis in cargo and/or compound areas, out of sight of the general public, while scheduling the equipment's removal from airport property. {R}

16.3.2 All service roads, as well as walkways and sidewalks shall possess clearly defined pavement markings. {R}

16.3.3 All fences and barriers shall be well maintained, rust free and properly secured. {R}

16.3.4 All light fixtures shall be in working order with no visible broken parts. {R}

16.3.5 All ramp surface areas shall be smooth and free of potholes and weeds. {R}

16.3.6 All service roads shall be well maintained and free of potholes and weeds. {R}

16.3.7 Guard booths shall present a well-maintained appearance, free of clutter, debris and graffiti. {R}

16.3.8 Trash receptacles shall be in good condition, without dents, marks or peeling paint. {R}

16.3.9 All ramp surface areas shall be clearly marked to support marshalling program of both aircraft and ground support equipment. {H}

16.4 Standards of Equipment Condition

16.4.1 Ground Support Equipment shall be parked and stored in clearly striped, designated areas. {R}

16.4.2 Ground Support Equipment shall be in good condition and in accordance with Port Authority Police inspections. {R}

16.4.3 Bus and/or Mobile Lounge seating shall be free of rips, tears and broken parts. {R}

16.5 Standards of Equipment Functionality

16.5.1 Buses and/or Mobile Lounges shall be in good working order. {R}

16.5.2 Buses and/or Mobile Lounges heating and air conditioning units shall be in working condition. {R}

16.5.3 Buses and/or Mobile Lounges shall not make excessive noise or give off unpleasant odors and fumes. {R}

16.5.4 Communication equipment on Buses and/or Mobile Lounges shall be clear and audible. {R}

16.5.5 Ramp equipment and cargo including containers shall be staged in an orderly fashion. {R}

16.5.6 Ground Support Equipment shall be maintained in good working order with no obvious fuel, oil or grease leaking on the ramp surface. {R}

16.5.7 Aircraft loading bridges shall be in good working order. {R}

16.5.8 Interline baggage transfer equipment shall be in good working order. {R}

16.5.9 Where applicable Terminal Operators shall provide clearly marked walkways from terminal to aircraft so as to safely deplane and board passengers and flight crews. {R}

16.6 Signs, Directions, and Information

16.6.1 Handwritten signs shall not be used and any temporary signs shall be consistent with Port Authority Aviation Signing and Wayfinding Standards. {R}

16.6.2 Gate numbers shall be clearly marked and visible at all times. {R}

17.0 - Assistance to Stranded Passengers

In order to implement and provide customer service during severe delays, a joint committee consisting of Terminal Operators, Airlines and the Port Authority will establish an arrangement to house, feed and transport, or provide cots, blankets and pillows to passengers during late night hours when such services are not usually available.

The Port Authority will arrange for the presence of necessary Port Authority service providers to furnish applicable services during late night hours.

The Following Defines "Stranded Passengers"

Passengers are considered stranded ***on board an aircraft***, when an aircraft is delayed at a remote parking position for more than two (2) hours on departure and one (1) hour on arrival, with no access to lavatories, food, beverage, medical assistance or communication, or are unable to disembark or unable to be transported to a terminal building.

Passengers are considered stranded ***inside a terminal***, when a flight is delayed or cancelled and the airline or terminal operator is unable to provide timely information on the status of the flight or alternate means of accommodations. Passengers will also be considered stranded ***inside a terminal*** when they are unable to arrange landside transportation for any number of reasons.

The Following Defines "Areas of Responsibility"

Assistance to arriving or departing passengers stranded on board an aircraft shall be the responsibility of the airline. Assistance to departing or arriving passengers stranded inside a terminal is the responsibility of the airline, and in some cases the Terminal Operator or the Port Authority. Airlines shall be responsible for providing accurate and up to date information to the general public. The Port Authority of NY & NJ has pledged to assist airlines during flight delay situations. PAPRICA (Port Authority Passenger Recovery in Cooperation with the Airlines) is the guideline airlines shall use during flight delays.

17.1 Assistance to passengers stranded on board an aircraft

17.1.1 Passengers shall be informed, in a timely and frequent manner, of existing traveling conditions, whether a delay or cancellation, and the arrangements to deplane the aircraft when stranded on board an aircraft for two (2) hours or longer. {H}

17.1.2 Passengers shall be provided with essential needs such as food, water, heat and air conditioning and restroom facilities on board. {H}

17.2 Assistance to passengers stranded inside the terminal

17.2.1 Airlines and/or terminal operators shall keep passengers informed of known delays, cancellations and diversions with frequent announcements as established by each airline. {R}

17.2.2 In accordance with airline's and/or terminal operator's procedures, food, refreshments, restroom facilities and medical assistance shall be made available as required. {H}

17.2.3 In accordance with airline procedures, reasonable efforts shall be made to safeguard the travel of passengers with down line connections and reservations including making alternate arrangements as required. {R}

17.2.4 Airlines are encouraged to provide passengers with any additional services as required by federal regulation{R}

17.3 Passengers with Reduced Mobility

17.3.1 Special attention shall be provided to passengers with reduced mobility (PRM) or special needs such as the elderly, disabled, passengers with medical conditions, unaccompanied minors, passengers with young children and passengers speaking foreign languages. {H}

17.4 Arriving flight information provided to the general public

17.4.1 Airlines and/or terminal operators shall have a responsibility to provide accurate and timely information to the general public including but not limited to scheduled time of arrival, estimated time of arrival, notices (or announcements) explaining reason for flight delay, cancellation or diversion, and updating the arrival information recorded messages and all electronic flight information systems on a timely basis. {R}

18.0 - AirTrain Stations and Vehicles

18.1 Standards of Cleanliness

Stations: Interior

18.1.1 Seating shall be clean and free of stains. {R}

18.1.2 Floors shall be free of debris and stains and shall appear clean. {R}

18.1.3 All floor mats shall be clean and properly aligned. {R}

18.1.4 All planters shall be clean and free of dust and debris. {R}

18.1.5 Windowsills shall be free of dust and debris. {R}

18.1.6 Windows and doors shall be clean and free of streaks and smudges. {R}

18.1.7 Trash receptacles shall be clean and not overflowing. {R}

18.1.8 Walls shall have a clean appearance, free of dirt and marks. {R}

18.1.9 Floors shall be dry, free of spills or water. {H}

18.1.10 Ceilings shall be dust free and unsoiled. {R}

18.1.11 Light fixtures and assemblies shall be clean and free of dust. {R}

18.1.12 Telephones and telephone areas shall be clean and free of debris. {R}

18.1.13 Pictures, frames, directories and advertising shall be clean and free of dust and graffiti. {R}

18.1.14 Heating and air conditioning units shall be clean and free of dust. {R}

18.1.15 Elevator cab walls and floors shall be clean and free of debris and graffiti. {R]

18.1.16 Escalators shall be clean and free of debris and graffiti. {R}

18.1.17 All Flight Information Display System (FIDS) and Train Information Display System (TIDS) monitors shall be clean and free of dust. {R}

Stations: Exterior

18.1.18 Entrance and exit doors shall be clean and free of smudges, dirt and grime. {R}

18.1.19 Windows shall be free of streaks and smudges. {R}

18.1.20 Trash receptacles shall be clean and emptied to prevent the overflow of debris. {R}

18.1.21 Awnings, where present, shall be clean at all times. {R}

18.1.22 Walls shall be clean and free of graffiti. {R}

18.1.23 Light fixtures and assemblies shall be clean and free of dust. {R}

18.1.24 Seating shall be clean and free of stains. {R}

Trains:

18.1.25 Exteriors shall be clean and have a freshly washed appearance. {R}

18.1.26 Pictures, frames, directories and advertising shall be clean, and free of dust and graffiti. {R}

18.1.27 Seating shall be clean and free of stains. {R}

18.1.28 Walls shall be clean and free of graffiti and scratches. {R}

18.1.29 Ceilings shall be dust free and unsoiled. {R}

18.1.30 Carpet shall be free of holes, rips, worn or frayed areas and flooring shall be free of large gouges, cracks, gum and stains. {R}

18.1.31 Floors shall be dry, free of spills and water. {H}

18.1.32 Windows shall be free of streaks and smudges. {R}

18.1.33 Doors shall be clean. {R}

18.1.34 Light fixtures and assemblies shall be clean and free of dust. {R}

18.1.35 Passenger Information Display System (PIDS) monitors shall be clean and free of dust. {R}

18.2 Standards of Condition

Stations: Interior

18.2.1 Seating shall be free of missing or broken parts. {R}

18.2.2 Tile and floors shall be free of large gouges, cracks and missing pieces. {H}

18.2.3 Floor mats shall be in good condition, without obvious wear and frays. {R}

18.2.4 Planters shall be in good condition, free of any visible damage. {R}

18.2.5 Windowsills shall be in good condition without any missing or broken pieces. {R}

18.2.6 Glass in windows and doors shall have no broken or cracked panes. {H}

18.2.7 Trash receptacles shall be in good condition with no dents, marks or peeling paint. {R}

18.2.8 Walls and columns shall be in good condition, free of marks, scuffs, dents or gouges. {R}

18.2.9 Ceilings shall be in good condition, evenly aligned and free of visible damage. {R}

18.2.10 All light fixtures shall be in working order with no visible broken parts. {R}

18.2.11 Telephones and telephone areas shall be in good condition, with no broken pieces. {R}

18.2.12 Pictures, frames and advertising shall be in good condition, free from marks, scratches and missing or broken pieces. {R}

18.2.13 Heating and air conditioning units shall be in good working condition. {H}

18.2.14 Escalators and elevators shall be in working condition. {R}

18.2.15 Flight Information Display System (FIDS) and Train Information Display System (TIDS) monitors shall be in good condition, with no visible damage. {R}

18.2.16 Unattended baggage carts shall be returned to dispenser racks promptly or located so as not to impede the flow of passengers or vehicles, and not allowed to collect in an unsightly manner. {R}

18.2.17 Employees' personal belongings shall not be visible. {R}

18.2.18 Platform bumpers shall be free of tears and missing or broken parts. {H}

Stations: Exterior

18.2.19 Sidewalks shall be smooth and free of large cracks or missing surface areas. {H}

18.2.20 Entrance and exit doors shall be in good working order. {R}

18.2.21 Windows shall be in good condition with no scratches, chips or broken pieces. {R}

18.2.22 Trash receptacles shall be in good condition, without dents, marks or peeling paint. {R}

18.2.23 Awnings, where present, shall be in good condition with no visible damage. {R}

18.2.24 Walls and columns shall be in good condition, free of marks, scuffs, dents or gouges. {R}

18.2.25 All light fixtures shall be in working order with all visible lamps operating and all burned out lights replaced. {R}

18.2.26 Only authorized vehicles shall utilize restricted curb areas. {R}

18.2.27 Snow and ice shall be removed from walkways, roadways and guide ways to prevent any safety hazard. {H}

18.2.28 Roadways shall be well maintained and free of potholes. {R}

18.2.29 Baggage carts shall be readily available. {R}

Trains

18.2.30 Exteriors of the trains shall be in good condition, free of visible damage. {R}

18.2.31 Pictures, frames and advertising shall be in good condition, with no marks, scratches or visible damage. {R}

18.2.32 Walls shall be in good condition, free of marks, scuffs, dents or scratches. {R}

18.2.33 Trains shall be in good working order and do not give off unpleasant fumes or noise. {R}

18.2.34 Seating shall be free of tears, rips or graffiti. {R}

18.2.35 Doors shall be in good working order. {H}

18.2.36 Passenger Information Display System (PIDS) shall be in good condition with no visible damage. {R}

18.3 Standards of Functionality

Stations: Interior

18.3.1 Flight Information Display System (FIDS) and Train Information Display System (TIDS), shall be clear, visible and accurate. {R}

18.3.2 Elevator button lights and switches shall be operational. {R}

18.3.3 Each help phone on the platform and each elevator emergency phone or communication device shall be in working condition. {H}

18.3.4 All lighting shall conform to the Illuminating Engineering Society of North America (IES) standards as they pertain to this area and activity. {H}

18.3.5 Public address systems shall be clear and audible. {R}

Stations: Exterior

18.3.6 Unattended baggage carts shall be returned to dispenser racks promptly or located so as not to impede the flow of passengers or vehicles, and not allowed to collect in an unsightly manner. {R}

18.3.7 All lighting shall conform to the Illuminating Engineering Society of North America (IES) standards as they pertain to this area and activity. {H}

Trains:

18.3.8 Waiting times at EWR shall not exceed:

- Three (3) minutes, between the hours of 1100 and 2000
- Four (4) minutes, between the hours of 0500 and 1100, and 2000 and 2400, and
- Twenty-four (24) minutes between 2400 and 0500

Waiting times at JFK shall not exceed:

- Nine (9) minutes, between the hours of 0600 and 1430
- Nine (9) minutes, between 1430 and 0000
- Thirteen (13) minutes, between 0000 and 0600

18.3.9 Air conditioning and heaters shall be in proper working condition and maintain appropriate temperatures. {R}

18.3.10 Automated announcements shall be audible and up-to-date. {R}

18.3.11 Public Address systems shall be clear and audible. {R}

18.3.12 Each help phone, emergency phone or communication device shall be in working order. {H}

18.4 Signs, Directions, and Information

18.4.1 Route/destination signing shall be clearly posted. {R}

18.4.2 Drop-off and Pick-up points shall be clearly designated. {R}

18.4.3 Clear, visible and accurate signing shall be placed at key decision points and be consistent with Port Authority Aviation Signing and Wayfinding Standards.{R}

18.4.4 Signing to gates, concourses and services shall be clear, visible and up-to-date. {R}

18.4.5 Flight Information Display System (FIDS), Passenger Information Display System (PIDS) and Train Information Display System (TIDS) monitors shall be clear, visible and accurate. {R}

18.4.6 Handwritten signs shall not be used and all temporary signs must be consistent with Port Authority Aviation Signing and Wayfinding Standards. {R}

18.4.7 Telephones and/or call boxes shall be easily identified. {R}

18.4.8 Maps and directories shall be accurate, up-to-date and be consistent with Port Authority Aviation Signing and Wayfinding Standards. {R}

19.0 - Assistance to Passengers with Reduced Mobility

Definition of "Passengers with Reduced Mobility"

Passengers with Reduced Mobility include, but are not limited to:

1. Persons with disabilities as defined by the American with Disabilities Act—An individual is "disabled" if he or she meets at least any one of the following tests:

   - He or she has a physical or mental impairment that substantially limits one or more of his/her major life activities
   - He or she has a record of such an impairment
   - He or she is regarded as having such an impairment

2. Passengers traveling with children and infants, or unaccompanied minors.

3. Passengers that do not speak English.

4. Passengers' requiring/requesting the aid of a mobility assistance representative.

Relevant Standards and Regulations

Relevant standards and regulations for accommodating Passengers with Reduced Mobility include, but are not limited to:

- The Air Carrier Access Act and the Department of Transportation rule (Title 14 CFR, Part 382).
- The Americans with Disabilities Act
- The International Civil Aviation Organization (ICAO) Annex 9 that includes a number of Standards and Recommended Practices (SARPs) concerning the access to air services and airport facilities by elderly and disabled persons including revisions by the Facilitation Division (FAL/11).
- Transportation Security Administration Training.

Areas of Responsibility

a. For Passengers with Reduced Mobility requiring or requesting assistance, the airline and/or terminal operator shall assist arriving Passengers with Reduced Mobility deplaning an aircraft and/or requiring assistance from the aircraft to the curb/ground transportation center or another assistance provider.

b. The airline and/or terminal operator shall assist departing Passengers with Reduced Mobility requiring assistance from the ticket counter and/or to board the aircraft.

c. For Passengers with Reduced Mobility requiring or requesting assistance, the Port Authority shall facilitate departing or arriving Passengers with Reduced Mobility between parking facilities and the terminal buildings or between terminals.

d. The terminal operator shall provide amenities (concessions, restrooms, telephones, etc.) directories of accessible areas, and clearly marked signing to facilities to accommodate Passengers with Reduced Mobility.

19.2 Assistance to Passengers with Reduced Mobility by an Airline or Terminal Operator

19.2.1 Passengers with Reduced Mobility shall receive assistance in getting to and boarding the aircraft and deplaning and getting to the curb in addition to making connections to other flights. {H}

19.2.2 Passengers with Reduced Mobility shall not be left unattended at any AirTrain platform or station. {H}

19.2.3 Employees shall receive the necessary training to assist in moving and transporting Persons with Disabilities. {R}

19.2.4 Employees shall receive training in handling mobility aids and assistive devices (electric wheelchairs, respirator equipment, etc.) used by Persons with Disabilities. {R}

19.2.5 Airlines may require up to 48 hours advance notice to accommodate certain mobility aids and assistive devices that require preparation time for transport (e.g., respirator hook-up or transportation of an electric wheelchair on an aircraft). {R}

19.2.6 Unaccompanied minors shall not be left unattended. {H}

19.2.7 Employees shall be available to assist Passengers with Reduced Mobility who are unable to move independently. {H}

19.2.8 Passengers with Reduced Mobility being dropped off shall be able to obtain assistance at the curbside within five (5) minutes. {H}

19.2.9 Each terminal operator shall ensure that telephones equipped with telecommunication devices for the deaf (TDD's) are provided and are clearly marked on directories and above the telephones. {R}

19.3 On-Airport Assistance to Passengers with Reduced Mobility

19.3.1 The Port Authority will make available para-transit or other special transportation services to Persons with Disabilities who cannot use fixed route bus/rail service between terminal buildings. {R}

19.3.2 The fixed route bus/rail services shall be accessible as required by the Americans with Disabilities Act. {R}

19.3.3 The Ground Transportation Information and/or Help Centers shall provide information to Passengers with Reduced Mobility using bilingual or multilingual brochures with internationally recognized symbols and/or interactive display systems. {R}

19.3.4 Unaccompanied minors shall not be left unattended in any parking facility or in an AirTrain station. {H}

19.3.5 Passengers with Reduced Mobility, who cannot move independently, shall not be left unattended in any parking facility or in an AirTrain station. {H}

19.4 Provision of Wheelchairs to Passengers with Reduced Mobility

19.4.1 Each terminal shall provide wheelchairs to assist in the movement of Persons with Disabilities. Wheelchairs shall meet the industry standards. {R}

19.4.2 Airlines shall each provide boarding wheelchairs and rams or mechanical lifts for boarding an aircraft not affixed to a loading bridge. {R}

19.4.3 All wheelchairs may be subject to an inspection of:

a. Armrests—sharp edges, cracks, burrs on screw heads, protruding screws, secure fit and locks engage squarely, all fasteners are present and tight;

b. Wheelchair back—upholstery for rips, tears and tautness; all attaching hardware is present and tight; handgrips are tight and do not rotate on post; back-post brace joints are not cracked, bent or damaged; safety belts are checked for fraying and hardware functionality;

c. Seats, cross braces and frames—upholstery for rips, tears and tautness; attaching hardware is present and tight; check for stripped screws and burrs on screw heads; folding chairs should be checked for sticking; cross braces are checked for bent rails or cracks and the center pin nut is present; front post slides are straight; seat rail guides are present;

d. Wheel locks—securely engage the tire surface and prevent the wheel from turning; rubber tip is present;

e. Large wheels—no wobbling or side-play indicating worn bearings; tires do not have excessive wear or cracks; axles and axle-lock nuts are functioning properly;

f. Casters—check for signs of bending on sides and stems of forks and be sure stem is firmly attached to fork; check stem bearings for excessive play both up and down as well as back and forward; check for excessive wobble in bearings; check tire for excessive wear or cracks; and,

g. Footrest/leg rest—check frame for damage and confirm secure fit of locking mechanism; check for sharp edges in foot plates and foot plate springs; proper operation for length adjustment hardware, all hardware is present and proper tightness; foot rest bumpers are present.

19.4.4 All wheelchairs shall be well maintained and in good condition. {R}

19.4.5 Each airline shall ensure that an adequate number of wheelchairs are available to meet the required demand. {R}

19.4.6 All airline terminals shall provide an adequate number of electric carts to meet the required demand. {R}

19.4.7 All electric carts shall be in good condition, free of dents, ripped seating and any visible damage or broken parts. {R}

19.4.8 All electric carts shall be equipped with an audible and visual alert signal to alert passengers to its' presence. {R}

19.4.9 All electric carts shall operate in a safe manner that at no point compromises the safety of pedestrians in the terminal. {H}

19.5 Signs, Directions and Information

19.5.1 All facilities and devices for Persons with Reduced Mobility shall be clearly marked and be consistent with Port Authority Aviation Signing and Wayfinding Standards. {R}

20.0 - Public Circulation and Queue Management

The Following Defines "Circulation Areas"

Circulation areas are comprised of publicly accessible areas inside or outside the terminal buildings occupied by persons walking or standing, exclusive of those spaces required for organized passenger queuing. Circulation areas include, but are not limited to, ticket lobbies, passenger waiting areas, food court concession areas, concourses, corridors and hallways, sidewalks, escalators and moving walkways, and pedestrian bridges.

The Following Defines "Queuing Area"

Queuing areas are comprised of publicly accessible areas inside or outside the terminal building dedicated to the organization of passengers waiting for service. Queuing areas include, but are not limited to, those areas dedicated to accommodate passengers approaching ticket counters, security screening areas, Customs and Border Protection areas, concessions, self-serve ticket kiosks, gate areas, information kiosks, and ground transportation areas.

Areas of Responsibility

a. Airlines shall manage the circulation and queuing activity in their lease areas including boarding areas, ticket counters, self-serve ticket kiosks, baggage offices, and other areas that are used by passengers to queue for airline services which include areas that may fall outside an airline's lease line.

b. Concession tenants shall manage the circulation and queuing activity within their respective lease areas.

c. The Terminal Operator and/or Airline shall manage circulation and queuing activity at passenger and baggage security screening checkpoints.

d. The terminal operator or the Port Authority shall manage the circulation and queuing activity in all public spaces not included in the lease areas of the airlines or other tenants.

e. Airline employees shall inquire of passengers at check-in queues regarding departure times and destinations and shall assist passengers in resolving problems when lines are lengthy.

f. The terminal operator and/or airline shall manage and control the circulation and queuing activity in their lease areas of the FIS with input from Customs and Border Protection.

20.1 Standards for Managing Passenger Circulation

20.1.1 Unattended baggage carts shall be returned to dispenser racks or removed so as not to impede the flow of passengers. {R}

20.1.2 Objects shall not be placed or installed in a permanent or temporary manner that will obstruct circulation requirements of persons with reduced mobility. (Refer to Standard 19.0). {R}

20.1.3 Objects shall not be placed or installed in a permanent or temporary manner that will obstruct primary public flow paths, doorways, elevator/escalator entrances, and other public circulation areas. {R}

20.1.4 Objects shall not be placed or installed in a permanent or temporary manner in areas where passenger flows must be maintained for purposes of providing public safety, including but not limited to stairways, escalator deboarding areas, roadway curbsides and emergency exit lanes, corridors or access points. {R}

20.1.5 Objects shall not be placed or installed in a permanent or temporary manner that promotes the development of a crowd that results in decreased public mobility or an unsafe condition. {R}

20.1.6 Lighting in public circulation areas shall be provided in accordance with Illuminating Engineering Society of North America (IES) standards. {H}

20.1.7 Preventative maintenance of facilities, cleaning, or other routine activities shall be performed so as to not interfere with primary public circulation paths. {R}

20.1.8 Provide and maintain adequate way finding to promote efficient public circulation. {R}

20.1.9 Objects shall not interfere with the public's visual field so as to affect public orientation and understanding of designated flow paths. {R}

20.2 Standards for Managing Passenger Queuing Areas

20.2.1 Organized queuing procedures shall be developed and formalized queuing areas shall be provided in locations where public queuing is likely to result in unsafe conditions, service stoppage, or an impediment to adjacent passenger flows. {R}

20.2.2 Designated queuing areas shall be properly sized based on anticipated passenger use in each terminal and shall be maintained to accommodate future public circulation and queuing demands. {R}

20.2.3 Public queues for a facility shall not extend beyond the tenant's designated lease area unless authorized by the Port Authority. {R}

20.2.4 The Port Authority or terminal operators shall be notified if public queues are anticipated to obstruct or are actually obstructing adjacent passenger flows in a manner that decreases public mobility or results in an unsafe condition. {R}

20.2.5 The tenant shall actively manage public queues at locations where the massing of people could result in an unsafe condition (e.g., adjacent to an escalator deboarding areas or curbside roadways) or impede primary public flow patterns. {R}

20.2.6 Public queues shall not extend or be formed outside a terminal building where shelter is not available. {H}

20.3 Stanchion Appearance and Locations

20.3.1 Placement of floor stanchions shall not interfere with public circulation, queuing or wayfinding. {R}

20.3.2 Stanchion belts should not exceed 7′ in length between posts, be less than 2″ in width, be less than 0.0275″ thick and the post should not be less than 2″ in diameter. {R}

20.3.3 Stanchion posts shall not exceed 40″ in height, the bases shall not exceed 14″ in diameter and any stanchion post weight shall not exceed 28 lbs. {R}

20.3.4 Stanchion belts and posts shall match in color, type and quality. The use of a combination of various stanchions, ropes, belts, etc. is not permitted. {R}

20.3.5 Stanchion belts or ropes should never be tied together. {R}

20.3.6 Stanchions, ropes, "tensa barriers" shall be well maintained and in good repair. {R}

20.3.7 Stanchions, ropes, "tensa barriers" shall be arranged in a neat and orderly fashion and not stored in public view. {R}

20.3.8 Stanchions, ropes, "tensa barriers" shall be clean and free of dust, tape and smudges. {R}

21.0 - Orderly Evacuation and Resumption of Services

Definition of "Emergency Situation"

a. An emergency situation is defined as any event that threatens, or has the potential to threaten, the life, health, and safety of individuals at the airport. Emergency situations include, but are not limited to, (a) fire, (b) security, (c) power outage, and (d) natural disaster.

b. Security emergencies include, but are not limited to, security breaches, threats against a specific facility or airline, acts of violence in pre- or post-security areas, bomb threats, unattended baggage or parcels and biological or chemical threats.

21.1 Airline Assistance

21.1.1 All airline employees and airline contractors shall be knowledgeable in terminal emergency and evacuation procedures.

21.1.2 All airline employees shall be familiar with airport emergency procedures.

21.1.3 In case of fire, power outage or natural disaster emergency, airline employees shall follow terminal operator and Port Authority Police instructions for emergency procedures.

21.1.4 In case of a security emergency, airline employees and contract employees shall at the direction of the Port Authority Police and the Transportation Security Administration (TSA) clear gates, boarding areas, and holding areas of all people (passengers, employees and other airport visitors) in a safe orderly, and efficient manner, and direct them to the nearest security checkpoint exit (or to the nearest emergency exit in the event of a fire emergency).

21.1.5 In case of a gate emergency involving an aircraft with passengers on board, airlines and FAA emergency procedures shall apply.

21.1.6 Airlines shall at all times have an on-duty employee designated as an "Emergency Representative" who shall communicate effectively with the Port Authority Police, the TSA, the terminal operator and customers and as applicable with Customs and Border Protection (CBP) to coordinate a safe orderly and efficient evacuation in the event of an emergency situation.

21.1.7 The Emergency Representative shall communicate and coordinate effectively with the TSA, CBP, terminal operators, and the Port Authority Police to inform airport customers of the nature of the emergency and to ensure airport customer essential needs are met.

21.1.8 After a departure emergency situation subsides, the Emergency Representative shall provide the Port Authority Police and the TSA flight departure information to effectuate an orderly and efficient re-screening of passengers according to the priority of departing flights.

21.1.9 After an arrival emergency situation subsides, the Emergency Representative shall provide the Port Authority Police, terminal operator and as applicable Custom and Border Protection, arrival information to effectuate an orderly and efficient deboarding and clearance of passengers, and what is being communicated to other airport customers waiting in the baggage claim area.

21.1.10 International arriving passengers and flight crewmembers that have been cleared through Federal Inspection Services (FIS), shall be directed to proceed with all other customers and employees when evacuating the premises, as established in the CBP Continuity of Operations Plan. (COOP).

21.1.11 International arriving passengers and flight crewmembers that have not yet been cleared through FIS, shall be evacuated in a manner established by the CBP's COOP. The Port Authority will be provided with such plans, by the CBP, on an annual basis.

21.2 Airport Tenant Responsibilities

21.2.1 All airport tenants shall be knowledgeable in terminal emergency and evacuation procedures.

21.2.2 All employees of airport tenants shall be familiar with airport emergency procedures.

21.2.3 In case of fire, power outage or natural disaster emergency, airport tenant employees shall follow Port Authority Police, or terminal operator instructions for emergency procedures.

21.2.4 In case of a security emergency situation, airport tenants shall clear their leased space of all customers and employees in a safe, orderly, and efficient manner, and direct them to nearest security checkpoint exit (or to the nearest emergency exit in the event of a fire emergency).

21.2.5 Airport tenants shall at all times have an on-duty employee designated as an "Emergency Representative" who will communicate effectively with Port Authority Police, TSA, CBP, the terminal operator and airport customers to coordinate a safe, orderly, and efficient evacuation of the airport tenant's leased space in the event of an emergency situation.

21.3 TSA Responsibilities

21.3.1 The TSA employees shall be knowledgeable in terminal emergency procedures.

21.3.2 All TSA employees shall be knowledgeable of all airport emergency procedures. Given that TSA employees may work at a number of security checkpoints throughout the Port Authority Airport system, TSA employees must be familiar with the airport emergency procedures at all terminals for each airport.

21.3.3 In case of a security emergency situation, TSA employees shall coordinate with the Port Authority Police and direct all airport customers and employees through the security checkpoint exit (or to the nearest emergency exit in the event of a fire emergency) in a safe, orderly, and efficient manner.

21.3.4 In case of fire, power outage or natural disaster emergency, the TSA shall coordinate emergency procedures with the Port Authority Police and the terminal operator to ensure an efficient and orderly evacuation and re-screening of airport customers and employees and follow departure service resumption process. (See Standard 21.8)

21.3.5 TSA employees shall communicate effectively with airlines, terminal operators, and the Port Authority Police to inform airport customers of the nature of the emergency and to ensure airport customer essential needs are met.

21.3.6 After the emergency situation subsides, TSA employees shall communicate effectively with airline Emergency Representatives, terminal operators, and the Port Authority Police to effectuate an orderly and efficient security checkpoint re-screening process according to the priority of departing flights.

21.4 Terminal Operator Responsibility

21.4.1 All terminal operator and Port Authority employees shall be knowledgeable with terminal emergency procedures.

21.4.2 All terminal operator and Port Authority employees shall be knowledgeable with airport emergency procedures relating to their terminal.

21.4.3 In case of fire emergency, power outage or natural disaster emergency, the terminal operator and Port Authority employees shall coordinate evacuation procedures with Port Authority Police, airlines, TSA, airport tenants, CBP to ensure an efficient and orderly evacuation and resumption of services.

21.4.4 In the event of extended terminal services disruption caused by fire, power outage or natural disaster, the terminal operator and the Port Authority shall implement contingency plans in coordination with Port Authority Police, TSA, airlines, CBP and airport tenants.

21.4.5 In case of a security emergency situation, terminal operator and Port Authority employees shall at the direction of the Port Authority Police direct all airport customers and employees through the security checkpoint exit (or to the nearest emergency exit in the event of a fire emergency) in a safe, orderly, and efficient manner.

21.4.6 The terminal operator or Port Authority shall at all times have an on-duty employee designated as the "Emergency Representative" who will coordinate with Port Authority Police, TSA, airline, CPB and airport tenant emergency representatives during an emergency situation.

21.4.7 The terminal operator shall make frequent public announcements using the public address system (or an alternative method if a public address system is unavailable) to inform airport customers of the nature of the emergency and the steps airport customers must take to remain safe during the emergency period.

21.4.8 When the emergency situation subsides and clearance has been given to terminal operator to re-enter the terminal, the terminal operator shall immediately inform customers of the process to return safely to the terminal areas.

21.4.9 When applicable, airlines, terminal operators, Port Authority and airport tenants shall keep airport customers and employees informed by other communication methods, including but not limited to Flight Information Display System (FIDS), website, emails and mobile phones.

21.4.10 By the end of January each year, terminal operators shall submit the most up-to-date safety and evacuation plan for the terminal to the Port Authority, including the emergency contact listing, name, phone and title.

21.4.11 Terminal operator's safety and evacuation plans shall be terminal specific to meet the needs of customers, employees, airlines and tenants operating in that facility.

21.5 Communication and Public Announcements

21.5.1 Terminal operators shall keep airport customers informed during emergency situations. Terminal operators shall maintain clear and effective communication with airport customers during emergency situations by, among other methods, frequent public announcements, FIDS and other communication methods as to the nature and seriousness of the emergency, the steps airport customers must take to get to safety, and the steps airport customers must take to reenter the building/terminal when the emergency situation subsides.

21.6 Directions and Assembly Locations

21.6.1 Terminal operators and the Port Authority shall identify all entry and exit points in the terminals, parking garages, and AirTrain stations where airport customers and employees are to assembly in case of an emergency.

21.6.2 Emergency evacuation markings are to be consistent with Port Authority sign and building code standards.

21.6.3 Airport employees shall be aware of emergency situation assembly locations as delineated in emergency evacuation plans and shall give airport customers clear and concise directions to assembly locations during emergency situations.

21.6.4 In the event of an alarm for fire, all customers and tenants must exit the terminal building as directed by the appropriate emergency response representative until the arrival of the Port Authority Police incident commander at the nearest terminal exit. It is noted that the nearest terminal exit may place passengers and employees on the tarmac and Emergency Representatives should work with the Port Authority Police to ensure that passengers and employees remain in a safe location on the airside.

21.6.5 If the nearest terminal exit places passengers and employees on public roadways, an Emergency Representative should work with the Port Authority Police to ensure the assembly areas are safe for passengers and employees to remain and allow for adequate access for emergency vehicles.

21.6.6 In the event of power outage or natural disaster requiring immediate evacuation of the terminal or a portion thereof, clear and frequent instructions shall be communicated to the customers and employees until the affected premises have been fully evacuated.

21.6.7 In the event of a security emergency, all customers and tenants must exit the sterile area. Customers and tenants may therefore remain in non-secure areas such as ticketing and domestic baggage claim areas rather than exiting the terminal building.

21.7 Departure Service Resumption Process

21.7.1 When the emergency situation subsides to the point where departure service resume, employees and departing customers must be re-screened at the security checkpoint before re-entering the sterile area of the terminal. Employees and passengers shall be re-screened n an orderly and efficient manner. Employees that are essential for service to resume shall be re-screened according to the priority of departing flights.

21.8 Departure Service Resumption Process

21.8.1 When the emergency situation subsides to the point where arrival service resumes, airline and airport tenant employees should return immediately to their workstations to expedite the processing of arriving passengers that could have been waiting for extended periods of time on an aircraft.

21.9 Passengers Needing Assistance

- Persons with Reduced Mobility are defined in Standard 19.0

21.9.1 Airport employees shall give priority assistance to persons with reduced mobility while exiting the terminal/airport during emergency situations and upon re-entry to the terminal/airport when the emergency situation subsides.

21.9.2 When required, public announcements shall be made in foreign language(s) and all uniformed airport employees should come to the assistance of Persons with Reduced Mobility in need of special assistance during the evacuation and resumption of services.

21.10 First Aid Assistance

21.10.1 Airport employees shall give priority assistance to people requiring first aid and/or medical attention outside the danger area.

21.10.2 Airport employees shall be knowledgeable of first aid stations in the terminal, and of medical facilities at the airport and shall provide appropriate assistance to airport customers needing medical attention.

22.0 - Cargo Services

In addition to the standards listed below, some elements of Ramp and Airside Areas, Standard 16.0 may apply to the Cargo Services area.

22.1 Standards of Cargo Condition

22.1.1 All cargo, both import and export, must be adequately protected from weather-related elements during the offloading process and subsequent drayage to the cargo warehouse. Plastic sheets are recommended where applicable.

22.1.2 All import cargo must be delivered to the cargo warehouse and shall not remain on the ramp areas.

22.2 Standards of Equipment Functionality

22.2.1 Aircraft handling equipment should be positioned behind designated demarcation lines and safety areas at least thirty (30) minutes prior to aircraft arrival on blocks.

22.2.2 All aircraft handling equipment should be in good working order.

22.3 Standards of Ramp Unit Load Device (ULD) Handling

22.3.1 All ULD's shall be stored off the tarmac, preferably on ULD storage racks in a designated cargo equipment area.

22.3.2 ULD's shall never be directly fork lifted at any time.

22.3.3 Slave dollies and loading vehicles and equipment shall be used when transporting ULD's.

22.4 Import Warehouse Operations

22.4.1 All cargo shall be processed and made available for customer pick-up within designated time frames but no longer than four hours.

22.4.2 All cargo shall be stored in designated areas that are monitored to ensure prevention of theft or pilferage.

22.4.3 All cargo shall be stored in designated areas that will facilitate the expeditious delivery to consignees.

22.5. Export Warehouse Operations

22.5.1 All cargo must be checked-in and verified by supervisory staff.

22.5.2 All cargo must be staged or stored n areas designated for export cargo

22.5.3 Plastic sheets shall be used for export cargo loaded on non-structured ULD's to ensure protection from weather related elements.

22.6 Dangerous Goods Handling

22.6.1 Warehouse dangerous goods areas shall be separated from other cargo handling areas.

22.6.2 Warehouse dangerous goods areas shall be clearly marked.

22.6.3 The handling of dangerous goods cargo shall be in accordance with IATA and ICAO current dangerous goods regulations.

22.6.4 Designated dangerous goods areas should have sub-areas segregated by class of dangerous goods.

22.6.5 Qualified personnel shall perform the acceptance of dangerous goods.

22.7 Valuable Cargo Handling

22.7.1 Locked vaults and similar type facilities shall be designated for high value goods.

22.7.2 Valuable cargo shall require a minimum of one (1) supervisory warehouse staff and one (1) security staff when handled for delivery, acceptance or handling.

22.7.3 Surveillance cameras or security staff shall monitor valuable cargo areas at all times.

22.7.4 Valuable cargo shall be handled in accordance with industry standards and best practices.

22.8 Vulnerable Cargo Handling

22.8.1 Locked cages and similar type facilities shall be designated for vulnerable cargo.

22.8.2 Vulnerable goods shall require a minimum of one (1) supervisory warehouse staff and one (1) security staff when handled for delivery, acceptance or handling.

22.8.3 Surveillance cameras or security staff shall monitor vulnerable goods area at all times.

22.9 Perishable Cargo Handling

22.9.1 Perishable cargo shall be handled in accordance with IATA Perishable Handling Regulations.

22.9.2 Refrigeration and climate control specifications must be maintained according to shipper or consignee requirements.

22.9.3 Perishable cargo shall be stored in designated areas of the cargo warehouse.

22.9.4 Qualified personnel shall perform the acceptance of perishable cargo.

22.10 Live Animal Handling

22.10.1 Live animals shall be handled in accordance with IATA Live Animal Handling Regulations.

22.10.2 Live animals shall be handled in designated areas of the cargo warehouse.

22.11 Import Operations

22.11.1 All documents shall be processed in a timely manner when picking up cargo but not later than fifteen (15) minutes.

22.11.2 All irregularities shall be documented.

22.12 Export Operations

22.12.1 Documentation shall be accepted and checked-in a timely manner, but not longer than fifteen (15) minutes.

22.12.2 Cargo shall be manifested according to specific instruction provided prior to flight manifesting time frames.

22.13 Cargo Public Areas

22.13.1 All public areas shall be clean, well maintained and free of unpleasant odors.

22.13.2 All public areas shall be well lit with all light fixtures in working order with no visible parts.

22.13.3 Counters shall be neat, organized and clean.

22.13.4 Floors shall be clean and free of debris.

22.14 Signs, Directions and Information

22.14.1 Handwritten signs shall not be used and all temporary signs shall be consistent with the Port Authority Aviation Signing and Wayfinding Standards.

22.14.2 Illuminated signs shall be in proper working order.

22.14.3 There shall be no unauthorized postings.

22.14.4 Airline and general tenant names shall be clearly posted and be consistent with the Port Authority Aviation Signing and Wayfinding Standards.

22.15 Signs shall clearly identify location of services provided.

22.16 All signs shall be clearly visible to customers.

22.17 Landside Parking

22.17.1 An adequate number of customers parking shall be provided based on facility specifications.

22.17.2 All designated customer parking shall be well marked.

22.17.3 Customer parking areas shall be in good condition, free of potholes and debris.

22.17.4 All designated truck parking shall be well marked.

22.17.5 Truck parking areas shall be in good condition, free of potholes and debris.

22.17.6 Truck parking shall be free of object that may impede the flow of goods into the warehouse.

22.17.7 All striping demarcations shall be visible.

22.18 Landside Truck Docks

22.18.1 All truck dock doors shall be well list with all light fixtures in good working order with no visible broken parts.

22.18.2 All truck dock doors shall be clearly marked.

22.19 Standards of Cargo Employees

In addition to the following standards, all employees shall conform to the same Employee Attitude, Appearance, Awareness and Knowledge as outlined in Standard 1.0

22.20.1 Staff shall be fully trained in the applicable ramp handling and aircraft loading processes.

22.20.2 All aircraft handling equipment must be operated n a safe and secure manner consistent with Port Authority Airport Rules and Regulations.

22.20.3 One (1) marshaller and two (2) wingwalkers shall be utilized for aircraft arrival and departure.

22.20.4 FOD checks shall be conducted thirty (30) minutes prior to aircraft arrival and thirty (30) minutes after aircraft departure.

ATTACHMENT J – TECHNOLOGY SERVICES DEPARTMENT STANDARDS AND GUIDELINES

THE PORT AUTHORITY OF NY & NJ

Standards & Guidelines

for Port Authority Technology

Technology Services Department

Version 8.3

August 30, 2011

Introduction **1**

1.0 The Port Authority Wide Area Network (PAWANET) **2**

1.1 PAWANET Overview 2
1.2 PAWANET Circuit Diagram 3
1.3 Inter-site Services Providers 3
1.4 PAWANET Functions 3
1.5 Features of PAWANET 4
1.6 Supported Protocols 4
1.7 PAWANET Switches and Routers 4
1.8 Approved Servers 5
1.9 Enterprise Addressing Scheme (including IP addressing) 5
1.10 Enterprise Network Monitoring Software 5

2.0 Network Resources **5**

2.1 Network Overview 5
2.2 Enterprise Network Architecture 6
2.2.1 Operating System and Software 7
2.2.2 Configuration 7
2.2.3 Network Resources Security 9
2.2.4 Network Access and User Account Security 10
2.2.5 Remote Access System 12
2.2.6 Network Resources Hardware Standards 13
2.3 Network Naming Conventions 14
2.3.1 Server Names 14
2.4 Directory Services and Structure 14
2.4.1 File Storage Guidelines 14
2.5 System Management 15
2.5.1 Technology Services Department and Departmental Business System Manager Responsibilities 15
2.5.2 Change Management 17
2.5.3 Turning Over a New LAN Resource to the System Administrator 18
2.6 System Backup and Recovery 18
2.6.1 Backup Logs 19
2.6.2 Backup Scheduling 19
2.7 Business Resumption Plan 19

2.8 Telecommunications Standards for Enterprise Network Resources 19
2.8.1 Closet and Telecommunications Room Access 20
2.8.2 Telecommunications Installation Contractor's Responsibilities 21
2.8.3 Electrical Requirements 21
2.8.4 Telephone Company Interface 21
2.9 Documentation 22
3.0 Virus Scanning & Management 23
3.1 Overview 23
3.2 Background 23
3.3 Standards 23
3.4 Virus Detection and Response 23
3.4.1 Preventing Virus Outbreaks 24
3.5 Virus Protection Stand Alone PCs and Laptops 25
3.6 Acquisition and Installation 25
4.0 Electronic Mail 26
4.1 E-Mail Overview 26
4.2 Policy on Use of E-Mail: Highlights 26
4.3 E-Mail Etiquette 27
4.4 E-Mail System Architecture 27
4.4.1 Public Folders in the Exchange Organization 27
4.5 E-Mail Environment: Design Considerations and Infrastructure 28
4.6 Remote Access to E-Mail 29
5.0 Intranet 30
5.1 Intranet Overview 30
5.2 Direction of eNet Development 30
5.3 eNet Software Infrastructure Standards & Guidelines 30
5.3.1 Design Guidelines 31
5.3.2 Accessibility Guidelines 34
6.0 Workstation and Workstation Operating System 35
6.1 Overview 35
6.2 Workstation Inventory 35
6.3 Workstation Operating System Standard 35
6.4 Workstation Configuration 35
6.4.1 Workstation Naming Conventions 35

6.4.2 Workstation User Accounts 35
6.4.3 Remote Workstation Management 36
6.4.4 Drive Mappings 36
6.4.5 Standard Workstation Hardware Configurations 36
6.5 Standard Department Workstation Software 36
6.5.1 Standard Workstation Software 36
6.6 Enterprise Software 36
6.6.1 PeopleSoft 37
6.6.2 SAP 37
6.6.3 Other Business Applications 37
6.7 Workstation Security 37
6.7.1 Physical Security 37
6.7.2 Logical Security 38
6.8 Customer Support Desk 38
6.8.1 Functions 38
6.8.2 Hours of Staffing 39
6.8.3 Escalation Procedures 39
6.9 Administrative Rights Procedure 39
6.10 Computing Resources Policy 40
6.11 Use of Port Authority Owned Computer Equipment at Home 40
6.12 Software Licensing Guidelines 41
7.0 Distributed Systems Environment 44
7.1 Overview 44
7.2 Microsoft Windows Servers 44
7.2.1 *Virtual Environment* 44
7.2.2 Windows Data Encryption 44
7.3 Unix 44
7.3.1 Unix Security 45
7.3.2 Backup 45
7.4 z/OS 45
7.5 Databases 45
7.6 Application Security 45
7.7 Server Physical Security 45
7.8 Load Balancing – Failover Architecture 46

8.0 Voice Network 46

8.1 Voice Network (Telephone) Services 46

8.1.1 Port Authority Telephone Network 46

8.1.2 Local Service 47

8.1.3 Long Distance 48

8.1.4 Tie Line Network 48

8.1.5 Voice Mail 49

8.1.6 Telephone Help Desk 49

8.1.7 Telephone Moves, Adds and Changes (MAC) 50

8.1.8 Installation and Use of Home Telephone Lines for PA Business 50

8.1.9 Installation of Modem Lines for PA Business 50

8.1.10 PA Calling Cards 50

8.1.11 Toll Free (800) Services 50

8.1.12 Audio Conference Call Services (Voice) 51

8.1.13 SL100 Meet-me Conference Call Service (Voice) 52

9.0 Vendor Provided Dedicated Systems 53

9.1 Overview 53

9.2 Physical Security Technology Standards 54

9.2.1 Agency Standard for Digital Video Recording and Access Control and Alarm Monitoring 54

9.3 Communications Infrastructure Standards 55

9.4 Server Infrastructure Standard 55

10.0 Wireless Technologies 57

10.1 Wireless Guidelines 57

10.1.1 Purpose and Scope 57

10.1.2 General Policy 57

10.1.3 Personal Area Networks - PAN 57

10.1.4 Wireless Local Area Networks - WLANs 57

10.1.5 Portable Electronic Devices (PEDs) – Cell Phones, PDAs, messaging devices, laptops and tablets. 64

10.1.6 Cellular and Wireless Email 65

10.1.7 Synchronization 65

10.1.8 Responsibilities of Technology Services Department 65

10.1.9 Responsibilities of Technology Services Voice Networks Group 66

10.1.10 Responsibilities of Wireless and Handheld Device Users 66
10.2 Paging Device Policy And Procedures 66
10.2.1 Policy 66
10.2.2 Procedures 67
10.3 Cellular And Nextel Phone & Wireless Modem Policy And Procedures 67
10.3.1 Policy 67
10.3.2 Procedures 68
10.4 Technology Services Personal Digital Assistant (PDA) Policy 70
10.4.1 Introduction 70
10.4.2 Hardware – Hyper Link 70
10.4.3 Software 70
10.4.4 Support 70
10.4.5 Training 71
10.4.6 Acquisition 71
10.4.7 Criteria To Qualify For A PDA Device 71
10.4.8 Personal Acquisition 71
10.4.9 Breakage And Loss 71
10.4.10 Data Security Considerations 71
10.4.11 Data Backup 72
10.4.12 Personal Digital Assistant (PDA) Policy 72
10.5 BlackBerry Device Policy & Procedure 72
10.6 BlackBerry Guidelines 73
10.6.1 Introduction 73
10.6.2 Recommendation for Essential Staff and First Responders 73
10.6.3 Support 73
10.6.4 Breakage And Loss 73
10.6.5 Data Security Considerations 73
10.6.6 Data Backup 73
Appendices 74
Appendix 2 -- Business Resumption Plan Document Format 74
Appendix 3 -- Communication Rooms/Closets Standards 76
Appendix 4 -- Cabling 77
Appendix 5 -- Port Authority Unified Wiring Plan 77
Appendix 6 -- Telephone Closet / IDF Termination Blocks 79

Appendix 7 -- Workstation Jacks.....79
Appendix 8 -- Standard Switches Inside the Department.....79
Appendix 9 -- Desktop and Lateral Cable Identification Management.....79
Appendix 10 – PA TELEPHONE NETWORK 5/08.....81
Appendix 11 -- Fiber Optic Specifications for Network Services - PAWANET....82
Appendix 12 -- Public Telephone Ordering Guidelines.....83
Appendix 13 -- PAWANET Services Connection Policy.....85
PAWANET "Rules of Connections".....87
Appendix 14 -- PAWANET Services Summary.....89

Introduction

The purpose of this document is to communicate the standards established by the Technology Services Department and provide managers and technical staff with guidance in managing the Port Authority's (PA) Information Technology (IT) resources in the most effective way. Managers and technical staff should consult this document when making decisions about how to acquire or evolve their computing systems, platforms, networks and applications. Port Authority department managers and staff need to ensure that changes in their department's Information Technology are compatible with the current Enterprise computing and telecommunications infrastructure. This is crucial to connect and exchange information with other Port Authority departments, as well as with individuals and organizations outside the Port Authority. To that end, these guidelines are intended to help departments do the following:

Implement computing and networking solutions that ensure the utmost reliability, availability and security.

Procure hardware and software that advances current and mandated business needs and enables departments to work with other departments/offices more effectively.

Easily and efficiently communicate and exchange information throughout the agency.

Achieve greater systems integration through leveraging and building upon standardized infrastructure and facilitating systems management.

Adherence to these standards ensures that IT investments achieve Enterprise connectivity, interoperability, consistency, and will enhance performance in a cost-effective way.

How to Use This Document

Throughout this document you will find cross-references, also called hyperlinks, to other documents which provide more specific and detailed information. For example, the very latest standard PC desktop and server configurations are listed on a linked page. Because the computer industry is dynamic and change is frequent, this time-sensitive information will be maintained on the PA's Intranet (eNet) so that it can be monitored and easily updated, assuring you of the most current information. This document will also be available on the eNet, so that when viewing it online, you can click on the underlined hyperlink to immediately access that information. If you are reading a paper copy of this document, you will need to access eNet to obtain the cross-referenced information.

The Technology Services Department welcomes your feedback/comments on these standards and guidelines. Please address your e-mail to: jgrant@panynj.gov.

1.0 The Port Authority Wide Area Network (PAWANET)

1.1 PAWANET Overview

The Port Authority has a modern distributed computing network, called the Port Authority Wide Area Network (PAWANET), which is managed as an Enterprise resource. It connects all the various Port Authority facilities and transportation systems using high-speed voice, data, and video lines or links.

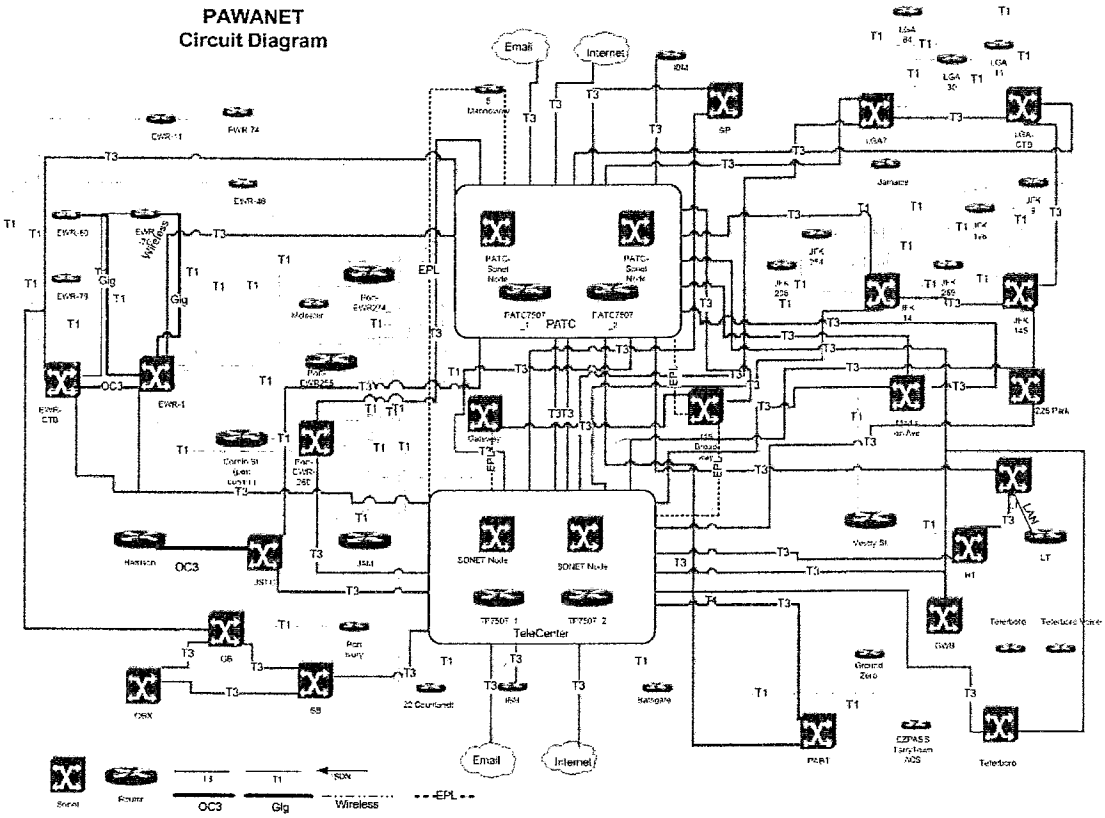
This network is crucial to all Port Authority businesses because it provides the connections for applications such as e-Mail, Internet and Intranet access, SAP, PeopleSoft, Electronic Toll Collection, CADD, Lease Image, Closed Circuit Television (CCTV) surveillance systems, and in the future, videoconferencing, and more.

PAWANET consist of a Managed Fiber Optic SONET network, provided by Verizon Select Services. This network consists of two dual OC48 SONET Rings that connect key Port Authority facilities, and intersects the Port Authority's two Data Centers. High-speed DS1, DS3, and Resilience Packet Ring (RPR) links are allocated on this network to form PAWANET's Wide Area Network (WAN) topology. Additional high-speed Ethernet Private Lines (EPL) has been deployed to support Key Port Authority's off-ring facilities.

Remote nodes are linked using high-speed dedicated communication lines. Alternate high speed dedicated communications lines and high-speed dial up communication links (ISDN Lines), provide back up paths should the primary links fail.

The network consists of state-of-the-art Cisco Systems equipment and services, such as, high performance Cisco Catalyst switches and routers. The Port Authority uses Cisco Systems SMARTnet hardware/software maintenance services, and Cisco's Technical Assistance Center (TAC) to support and maintain the network

1.2 PAWANET Circuit Diagram



1.3 Inter-site Services Providers

The Technology Services Department (TSD) has contracted with a variety of companies to provide inter-site services. Companies providing communications services for the Wide Area Network are listed below.

- AT&T Local Services
- Verizon

1.4 PAWANET Functions

Currently PAWANET provides the following functions:

Data	Supports the low and high volume transfer of data used for applications, such as SAP and PeopleSoft, and for network communications, such as e-Mail. Provides a data path for off-site, mainframe data backup of file, print and application servers. Enables the use of Storage Attached Network (SAN) for network storage of user files and routing jobs to shared network printers.
CCTV	The transfer of Closed Circuit TV (CCTV) data is supported across the entire network to provide security for the Port Authority's key facilities.

Voice	The network provides the hardware capabilities for voice and VoIP transmission.
Videoconferencing	The network switches and transmission lines are capable of handling videoconferencing to support the agency's future needs.
VOIP	Voice Over Internet Protocol (VOIP) is in the process of being implemented for the agency to replace the legacy Nortel system which currently serves the majority of Port Authority users. VOIP will be another data stream utilizing the PAWANET infrastructure.

1.5 Features of PAWANET

PAWANET provides a high performance and reliable fail-safe communications network. These are its key features:

- Alternate paths of communication
- Support of high volume traffic such as CADD, CCTV and others
- High performance Catalyst 3000, 4000 and 6500 series switches at Port Authority facilities.
- Cisco high performance 2000, 3000, 7200 and 7507 router family products with redundant power supplies.

1.6 Supported Protocols

The network supports the following network protocols, allowing dissimilar platforms to communicate within PAWANET:

TCP/IP:	Transmission Control Protocol Internet Protocol (TCP/IP) is the universal protocol that allows communications between all systems within the Port Authority's network, as well as other networks.
IPX/SPX:	This protocol allows communications between all Novell platforms.
SNA/SDLC:	This protocol allows communications between all IBM systems and other systems that support System Network Architecture (SNA)

1.7 PAWANET Switches and Routers

The current standard switches and routers used on PAWANET are:

- Cisco's 15454 High-speed SONET multiplexers connecting the Verizon's OC48 Rings to key Port Authority facilities and data centers.
- Cisco High performance 3000, 4000, and 6000 series switches
- Cisco 7200 high performance routers
  Provide high-speed connectivity and routing capabilities across the network in support of TCP/IP, IPX/SPX and bridging functions, and provides routing capabilities for Port Authority Internet access.
- Cisco 7500 series high-capacity redundant routers
  Serve as the -network backbone core router that provides high speed routing functions between Teleport, Port Authority Technical Center, and all PAWANET

connected facilities, as well as, the IBM mainframe. Also provide high-speed connection and routing capabilities to the disaster site for data recovery in case of a catastrophic event.

1.8 Approved Servers

Only IBM File & Print and Application servers may be connected to PAWANET. The link to the CTO's memo on server infrastructure standards is shown below.

Memo on Server Infrastructure Standards

This includes turnkey and distributed systems where File & Print or Application servers are being used. Any replacement File & Print or Application servers must be IBM servers. Deviation from this policy will not be allowed without prior approval of the Chief Technology Officer or their designee.

1.9 Enterprise Addressing Scheme (including IP addressing)

The Port Authority's Enterprise network is a TCP/IP Class B network allowing for a maximum of 255 subnet assignments. Subnets are assigned on a geographical basis according to the number of resources required. Workstations are configured for dynamic assignment of IP addresses via Dynamic Host Configuration Protocol (DHCP).

1.10 Enterprise Network Monitoring Software

The Port Authority continually monitors its WAN and the availability of its links. To provide for real time monitoring, the following software utilities are used:

- HP Open View Network Management software
- Cisco Works for Switched Internetworks

2.0 Network Resources

2.1 Network Overview

The Port Authority has a modern distributed computing network, which is managed as an Enterprise resource. The network connects all individual PCs, servers, printers, and other devices in a unified computing infrastructure that makes it possible for the Port Authority to conduct its business.

The Enterprise Network consists of the PAWANET (see Section 1.1) and connected Local Area Networks (LAN's). The line of demarcation between the cable and wiring which is the responsibility of the carrier and the Port Authority's area of responsibility is

usually a wiring closet. The Port Authority's Enterprise Network consists of the following components on the Port Authority side of demarcation:

- Enterprise Devices
    - Cabling
    - Routers
    - Switches
    - Wiring Closets
    - Communications Equipment Racks
    - Server Racks
    - File and Pint Servers
    - Application Servers
    - Storage Area Networks (SAN)
    - Network Printers
- LAN Devices
    - Desktop PCs
    - Workstations
    - Laptops
    - Local Printers
    - Scanners
    - Copiers
    - PC Peripherals

The purpose of the following subsections is to:

- Define the policies and standards governing Enterprise and LAN resources throughout the Port Authority.
- Delineate the duties and responsibilities of the Enterprise System Administrators, the Technology Services Department (TSD), and the Departmental System or Application Manager.

See the Guide to Systems Administration for detailed information on system requirements and procedures.

2.2 *Enterprise Network Architecture*

The Port Authority operates an extensive network of Enterprise file, print and application servers. These devices are linked to an Enterprise Wide Area Network. The flexibility provided by the use of multiple servers, server clusters and Storage Area Networks (SAN) offers users improved network response, greater reliability, increased data security and reduced operating cost. Adherence to the standards outlined in this section allows departments to manage their systems, applications and data in a way that best

meets their business needs while maintaining interoperability and safeguarding Port Authority's information assets.

2.2.1 Operating System and Software

All Enterprise file & print services in the Port Authority are based on the Novell Netware operating system. We are currently moving to a Microsoft Windows file & print environment. Microsoft Windows servers and Sun Solaris are supported as application servers when required for functionality.

In addition to the base operating system, all Enterprise servers must include or provide access to the following components:

- Virus Protection
- Network Security
- Remote Monitoring and Management
- Intrusion Detection
- Mainframe Systems Backup
- Uninterrupted Power Supply (If central UPS is not installed at the location)
- Current Service Packs and security patches

To see the current standard, click below.

PA Server

2.2.2 Configuration

All network devices--including servers, workstations, network printers, and network faxes--must use IP addresses which conform to the standards outlined in sections, 1.9 *Enterprise Addressing Scheme*, and 2.3.1, *Server Names*. System Administrators may refer to the *Guide to System Administration* for specific instructions on how to install and configure the Novell and Windows operating systems. All Novell servers must be configured using the following parameters:

- Minimum Size of DOS Partition: 5GB
- IP Protocol
- Volume Names: SYS, DATA, APPS

2.2.2.1 Drive Mapping Conventions and Organization

Mapping of workstation drive pointers to SAN or server disk volumes or folders is accomplished through the Novell NetWare Login Script. The following drive letters are reserved for Novell installations:

Pointer	Volume or Folder
H:	Novell login (first network drive)
M:	Reserved
P:	Public Applications
Q:	Installation and Upgrade Utilities

S:	Departmental shared directories and files
T:	Reserved
U:	Users Private Home Directory
Z:	Novell system files (Search mapping)

- Public (Shared) application software installed on a NetWare file and print Server, or server cluster must reside on a separate volume named "APPS".

  Example: P:\APPS

- Each software application installed on the NetWare file and print server, or server cluster, must have its own sub-folder.

  Examples: P:\APPS\EXCEL

  P\APPS\WORD

- SYS volume must be used for operating system and support software only.
- Shared Data stored on a NetWare file and print Server, or server cluster, shall reside in a volume named Data, and shall be mapped to the "S:\" drive pointer.

  Example <Server _name>:\DATA\SHARE on a single server

  <Cluster_name>:\DATA\<Department_NAME>\SHARE on a server cluster

- Each Department's SHARE folder will contain at least three sub-folders titled Org, Everyone and Projects.
- The Projects folder is provided for storage of project related files. All departmental projects will be kept in a sub-folder under the Projects folder and the folder will be named using the same name as the project. User rights will be assigned by a group having the same name as the project folder. Only staff requiring access to the project files should be granted rights to that project folder.
- Under the Projects folder will be two additional folders, one called "Active" and one called "Completed". Active projects reside in the "Active" folder.
- When staff identify a project as being completed, the project folder will be moved to the "Completed" folder and all rights, except for "Read" and "FileScan" will be removed from the folder. This will ensure that the final project documents remain unchanged, while still allowing authorized staff to review the old documents and use them as templates for new documents if desired. The "Completed" folder will be set to archive its data.
- Under the "ORG" folder will be subfolders with names corresponding to the various divisions within the department. By default, only staff within a division will have access to a division's folder. These folders are intended to hold data for a specific division that would not normally be shared departmentally. Staff from other divisions would not have access to these folders unless the division manager of the owning division gives their approval. Having folders setup by divisions will simplify the process of identifying who is responsible for the contents of a folder.
- The "S" and "U" drives should only be used to store business related files.

- The Systems Administrator, at the direction of the Director, may from time to time remove any data deemed to be non-business related.
- A folder called "Everyone" will be created in the Share folder. All staff in the department will have full access to this folder to store and retrieve files that are not related to a project or a division's day-to-day operations.
- Additional shared folders, with access restricted to only specific users, if required, will be created in the Share folder. Access will be restricted through the use of Novell Inherited Rights Filters and access will be granted through the use of groups. These groups will be named using the same name as the folder name.
- In general, rights to any folder will be granted through the use of a group having the same name as the folder. The group would have trustee rights to the folder, and users would be added to or removed from the group as needed. All rights would be granted or revoked through the use of form PA-3624A. Designated staff in each department are required to approve these requests.
- A user "U" drive will be assigned to each standard Novell account for use by each individual user to store business related data on the network. Access to the "U" drive is restricted to the account owner only. Users receive all rights to this folder except for "Access Control" and "Supervisory". Users cannot share data on their "U" drive. Files should be shared only by using the Share, ("S") drive.
- Access to a user's home directory, by anyone other than the owning user is prohibited and will be removed after notifying the end-user.
- Installation files used in the installation of desktop software must reside in a sub-folder under the "APPS" volume

  Example P:\APPS\Psoft

2.2.2.2 Connecting LAN Devices to the Enterprise Network

The Technology Services Department is responsible for connecting all LAN devices to the Enterprise Network (PAWANET) provided they meet the Port Authority's standards. The following system components must meet the standards in order to connect department devices.

Type of Device or Software

- Primary Network Operating System (NOS)
  - Application Server Operating System
  - Network Interface Card (NIC)

To see the current standard software needed for connecting LAN devices to the Enterprise Network, click below.

PA Server

2.2.3 Network Resources Security

2.2.3.1 Server Physical Security

All network equipment must be physically secured in a locked room.

2.2.3.2 Server Logical Security

To safeguard the Port Authority's Information Technology (IT) systems and data, TSD has implemented a number of processes and procedures, including the requirement that all users accessing the Port Authority's networks authenticate to the Novell NetWare Directory Service (e-Directory). The e-Directory Service is a database containing descriptions of all network devices including servers, printers, shared drives and user accounts.
In plain English, this means that by executing a login when you first power on your PC you are telling the network who you are. This is accomplished by providing your Novell NetWare Username and password. Just as you are issued an ID card for access to certain facilities, buildings or rooms you need to visit to perform your job, your Novell authentication grants you access to network resources, such as shared data volumes, software applications and network printers you use in performing your assigned tasks.

TSD, or its contracted vendor, is responsible for providing all Enterprise servers with the following protection of their logical resources:

- Guard against unauthorized access by making sure that servers cannot be booted from a floppy.
- Scan all workstations for viruses daily.
- Scan all laptops for viruses at log-in.
- Scan all incoming data from users, server peripherals, diskette, CD-ROM, tape drives, other servers, and the Internet for viruses
- Perform daily incremental backups and full backups weekly.
- Store all monthly backups off site at a secure location and secure daily and weekly backups on-site in a locked area.
- Test recovery procedures annually.
- Use system and application passwords that conform to the Technology Services Department standards.
- Configurations must conform to security parameters identified by NetVision Suite software.
- Perform deleted file purges immediately or no later than 6 days after file deletion.

Control all remote access using the Port Authority's Remote Access System.

2.2.4 Network Access and User Account Security

2.2.4.1 Account Creation

User accounts are created and managed in e-Directory for both the Novell and Windows network resources. The Novell Username must be unique. Individual user accounts are established based on a manager's approval and are inactivated and/or removed as appropriate. Documentation for the creation of user accounts and authority for access is maintained by the System Administrator.

The Novell Username is determined by combining the first initial of the user's first name and the complete last name.

Example:	**User's Name**	**Novell Login ID**
	Tony Robinson	trobinson

When the Novell Login ID is already in use, see the Guide to Systems Administration for additional examples of alternative account names to use.

2.2.4.2 Time Restrictions

Due to the fact that The Port Authority serves its clients 24 hours a day, we do not have Login Time Restrictions on our Novell File & Print servers. All staff may access their Novell account 24 X 7.

2.2.4.3 Concurrent Logins

Login sessions should be limited to one connection per user. User accounts should not have the ability to login to multiple workstations after establishing one active connection to the network.

2.2.4.4 Intruder Detection

These system-monitoring features should be active:

- Restrict the count of incorrect login attempts to three before the account is locked out.
- The time for which unsuccessful login attempts are retained to determine a possible intruder attack should be a minimum of 30 minutes before the counter is reset to zero.
- The time for which a user account remains disabled before the account can be used again should be a minimum of 30 minutes.

2.2.4.5 Passwords

All user accounts should have passwords conforming to the following standards:

- Minimum length is six (6) characters.
- Should not be easily guessed. It should not be related to one's job and should not be a word in the dictionary or a proper name.
- Should be set to expire at least every 90 days and 30 days for accounts with system or application administrator access.
- Grace Logins should be activated and limited to three.
- Users should be notified several days in advance of password expiration.
- Users should be forced to change their password on initial login and once it expires.
- Unique passwords should be required when changed. Users should be prevented from reusing a previous password for a minimum of one-year.
- Users should not be permitted to change their passwords more than once a day.
- Passwords should be encrypted in storage.
- Passwords must be entered in a non-display field with a re-enter verify function for new passwords.
- Passwords must not be available on hard copy.

- Passwords used in system startup files and login scripts must be encrypted.
- If an application uses a default password, change it on installation.
- Do not use cyclical passwords, such as the word, February, during the month of February.
- Do not reveal your password to anyone except authorized persons.
- Use both upper and lower case characters and special characters where possible.
- Change password if it has been disclosed or compromised.
- Protect by using a screen saver password with a recommended 15-minute time-out period.
- Passwords should not be the same as the user ID

Passwords are considered confidential data. They protect the Port Authority's network resources and grant system privileges and access. Disclosure may result in unauthorized access to data, system files and transactions. Passwords are also your signature and identify you as the individual who is responsible for the system activity.

2.2.4.6 Modems

Staff are prohibited from connecting dial-up modems to workstations that are simultaneously connected to PAWANET or another internal communication network unless approved by Technology Services.

Where modems have been approved, users must not leave modems connected to personal computers in autoanswer mode, such that they are able to receive in-coming dial-up calls.

2.2.5 Remote Access System

The use of local modems to establish direct dial connections to devices on the PA network is prohibited. Exceptions to this policy require the approval of the Technology Services Department's IT General Manager, Network & Operations.

The approved mechanism for remote access to the Port Authority network is through the Remote Access System (RAS). The Remote Access System utilizes an Internet-based Virtual Private Network (VPN) tunnel established over the Internet linking remote users to the Port Authority Wide Area Network (PAWANET) (remote client to PA site). It is designed to provide authorized Port Authority users with secure access to corporate applications and to files available on their departmental file servers. This access to applications and resources is delivered through a thin-client environment consisting of a farm of Citrix MetaFrame/Microsoft Terminal Services servers capable of supporting 200 or more simultaneous users each. There is no provided access to the user's office PC desktop. The system also provides access to IBM enterprise server ("mainframe") applications. Port Authority offices without direct connection to the Port Authority Wide Area Network (PAWANET) can use this system to establish remote access to corporate applications located on PAWANET.

RAS provides multiple security mechanisms to ensure that only authorized users gain access to the Port Authority's computing resources and systems. Through multiple

security steps, the user must respond to security challenges. After successful authentication verification, authorized users are provided with access to corporate applications and their departmental network resources through the thin-client environment.

To obtain Remote Access Authorization, see the *Remote Access Authorization* procedure in the public folders on the Exchange server.

The Port Authority also supports corporate site-to-site VPN connections and utilizes Cisco equipment for these connections.

2.2.6 Network Resources Hardware Standards

2.2.6.1 Standard Servers

To see the current Port Authority standards for servers, see the Technology Services Department web page on eNet, or click below.

PA Server

2.2.6.2 Printers

To see the current standard, see Technology Services Department web page on the eNet. If you are already viewing this document on the eNet, click below.

PA Printer

2.3 *Network Naming Conventions*

2.3.1 Server Names

All server names should conform to the standard 8-digit code, with the first four characters indicating the facility. Click below for a listing of facility codes.

Facility Codes

The second two characters represent the type of server, i.e. file storage, infrastructure, backup, application or database. The link below contains valid server functionality codes.

Server Functionality Codes

The final two characters contain a unique sequential two-digit identification number.

Static IP addresses for servers, printers and faxes must be within the address range of 201 to 234 of the respective subnet. All information regarding the name and address configuration should be forwarded to the Server Design Group, to ensure that duplicate names are not used.

2.4 *Directory Services and Structure*

The Port Authority uses Novell e-Directory to manage network resources and user access. Port Authority departments are designated as organizational units (OU) and servers are network objects contained within the OU.

All network printers should be created as e-Directory objects. IPrint should be utilized.

Applications are distributed using Novell's ZENworks. Applications are distributed based on the type of workstation and user definitions. Scheduling of distributions is done in conjunction with client departments.

2.4.1 File Storage Guidelines

All business related files should be saved to a shared drive or the user's home directory (U:). Non-business related files may be stored locally (C:) and backed up to removable media such as CD/DVD-ROM, etc if needed.

When saving files to network storage, whether on the U:\ drive, S:\ drive or any other network storage location, it is important to remember not to exceed a maximum of 255 characters for the file name ***and its full path.*** The length of a file name consists of: the full directory path including the server name, directory name, names of all sub-directories and the name of the file. This also includes special characters such as slashes and dots. The 255 characters limit is a known issue in both the NetWare and Windows environments as well as with data backup software.

Some of the problems that may result when full file names exceed the 255 character limit may include: inability to backup files, inability to restore files, errors when copying files or deleting files, and other problems with file utilities such as Hierarchical Storage Management (HSM), archiving and backup utilities.

To prevent the types of problems described it is highly recommended that the following guidelines be observed:

Abbreviate file and folder names to keep them as short as possible

Avoid many levels of sub-directories with long names

Don't move or copy existing directories, and the files they contain, to other directories. This only adds their names to the existing file name and path.

Avoid exotic and "wild-card" characters such as:

underscore at the beginning of directory and file names " _ "

blanks at the beginning of directory and file names

asterisk " * "

question mark "?"

semi-colon " ; "

An example of a full file name is as follows:

\\1MADCLUST\DATA\TSD\share\projects\PATH\ExpressRail\file123.doc

The format is: \\<server name>\<volume>\<department>\<directory1>\.....\<directoryX>\<file name>

In the above example the full file name is 64 characters, including spaces and all special characters.

2.5 *System Management*

All computing at the Port Authority is performed on workstations connected to PAWANET. Port Authority departments receive support for their network from the Technology Services Department and the authorized Enterprise vendor. There is a division of responsibility between Technology Services Department and those responsible for the management of departmental network resources.

The department is responsible for selecting a Business System Manager who will manage the departmental network resources. Technology Services Department will oversee the System Administrator(s). The System Administrator provides day-to-day operational support. The following chart delineates the major responsibilities of Technology Services Department System Administrators and the Departmental Business System Managers. Click below for detailed information concerning System Administrator duties:

Guide to Systems Administration

2.5.1 Technology Services Department and Departmental Business System Manager Responsibilities

Technology Services Department Responsibilities	Business System Manager Responsibilities (May be carried out by department staff, contract with TSD or third party)
Select and install: Servers Desktop PCs CAD Workstations	Select and Manage: Business Applications Software

Technology Services Department Responsibilities	Business System Manager Responsibilities (May be carried out by department staff, contract with TSD or third party)
Network & Local Printers PC Peripherals Routers and switches Cabling Wiring closet hardware	
Promulgate Port Authority Standards for, install and maintain: Workstation OS and configuration Network OS and configuration Physical and logical security for: Network Servers Workstations PC Peripheral Devices User Accounts Databases Virus Protection Back up and Recovery Hardware Software Addressing/ Naming Conventions for Network devices	**Review and Verify** Port Authority Standards for installation and maintenance of: Current Workstation OS Current Network OS Physical and logical security for: Network Servers Workstations PC Peripheral Devices User Accounts Databases Virus Protection Download and install current virus protection software and data files. Back up and Recovery Maintain tape library
Establish and monitor Performance and Capacity Standards	**Review and verify** Performance and Capacity reports
Set standards for, and provide database administration	**Monitor** database performance
Establish requirements for Business Resumption Plan	**Develop, validate and document** Business Resumption Plan **Implement** Business Resumption Plan if necessary

Technology Services Department Responsibilities	Business System Manager Responsibilities (May be carried out by department staff, contract with TSD or third party)
Conduct Change Management Meetings: Establish version control procedures Create a forum to insure good communication in the agency.	**Review and monitor** Change Management tasks: Verify version control Document changes in department devices Inform Technology Services Department of all significant changes — hardware and software.
Maintain Documentation Library containing, for example: Suppliers' manuals on all software and Hardware Configurations of all servers and workstations Physical media, such as back up tapes.	
Select, configure and deploy software distribution tools.	**Monitor and review software** distributions.
Electronic Messaging to include e-Mail, calendaring and message-enabled applications.	Supply users e-mail setup information as needed
Provide direct support to end users on the use of workstation and applications running on the department's network resources.	
Select and provide virus protection software and data files. **Maintain** a log of all virus scan activity for daily review.	Report all suspected instances of computer viruses immediately to the Customer Support Desk in accordance with established IT security procedures
	Maintain and control software licenses

Note: System Administrators do not create patches or upgrades.

To see a more detailed description of System Administrator responsibilities, see the Guide to System Administration, or click below.

Guide to Systems Administration

2.5.2 Change Management

System Administrators are responsible for reporting to the Technology Services Department all changes pertaining to:

Departmental hardware:

All network connected devices, such as:

- Printers
- Print servers
- Scanners
- Network Interface Cards

Software:

- Non-standard operating systems
- Non-standard applications

System administrators are responsible for participating in Change Management meetings or for making sure that a representative participates.

2.5.3 Turning Over a New LAN Resource to the System Administrator

Whenever a new departmental network resource goes into production, the installation team or vendor is responsible for turning over to the System Administrator of the new departmental network resource all of the items on the *Information and Documentation Transition List*. To see this list, see the Technology Services Department Web page, or click below.

Information and Documentation Transition List

2.6 System Backup and Recovery

There are two Port Authority approved standard software products used to perform scheduled server backups:

- FDR Upstream and Mainframe based tools are used to create data backups that will be stored remotely and managed automatically. The use of these backups is required to assure off-site data storage at a secure facility.
- The System Administrator is responsible for verifying that system backups, both local and remote can be used to restore the data. Tests of the ability to successfully restore from both backup systems will be performed annually. . See section 2.7 – Business Resumption Plan to establish and test recovery processes It is recommended that the test data restore be performed on a single non-critical directory only, not the entire server. Tests of the ability to restore system and application files will be performed on a non-production server in the Lab. When incremental or differential backups are routinely used, the test restore procedure should incorporate both.
- Immediately prior to performing the test restore procedure, do a special full backup on the directories being tested.
- Testing a full restore should only be performed on a non-production server.

The product used will depend on the criticality of the data and the need for redundancy. For the current standard versions click below:

PA Server

All backup media and records must be treated with the same level of security and confidentiality as the original data.

2.6.1 Backup Logs

The System Administrator will maintain the following logs for a period of two years:

- Back-up activity
- Rotation of back-ups,
- Usage/rotation of back-up media
- Off-site data storage.

2.6.2 Backup Scheduling

The System Administrator is responsible for performing back ups of data, application and system files. This must be as follows:

- Weekly full back up of each server. A full back up is a back up of all files on the server.
- Daily differential, incremental or full back up of each server or server cluster. The type of back up performed is dependent on time constraints and the amount of data to be backed up. Incremental back ups are back ups of all files changed since the last back up. Differential back ups are back ups of all files changed since the last full back up.
- A Grandfather, Father, Son (GFS) scheme based on a 33 tape rotation should be used to ensure complete back up and recovery.

2.7 Business Resumption Plan

The Departmental Business System Manager should work with Technology Services to develop a disaster recovery and contingency plan. The System Administrator should participate in the planning, design, implementation, testing, updating and documentation of the plan. Appendix 2 shows a recommended outline for such a plan. The Business Resumption Plan should be updated quarterly and tested at least annually.

2.8 Telecommunications Standards for Enterprise Network Resources

To see the standards and guidelines for the following telecommunications components, please see the Appendix.

Appendix 3 -- Standards for Setting up Closets & Communication Rooms

Appendix 4 -- Standard Cabling Schemes

Appendix 5 -- Unified Wiring Specifications

Appendix 6 -- Telephone Closet / IDF Termination Blocks

Appendix 7 -- Workstation Jacks

Appendix 8 -- Standard Switches

Appendix 9 — Workstation and Lateral Cable Identification Management

Appendix 11 – Fiber Optics Specifications for Network Services - PAWANET

2.8.1 Closet and Telecommunications Room Access

The following standards need to be followed regarding access to closets and communication rooms.

- All telecommunications rooms must be physically secured. Remote locations which are not secured by a guard or within line of sight of personnel must be secured by a card access system and/or video cameras.
- The Network Connections (NC) group is responsible for installing routers, switches (along with Cisco Staff when applied) and station drops. They also patch connections and troubleshoot LAN cabling.
- System Administrators requiring routine maintenance of data communications equipment should call the Customer Support Desk. When new devices or reconfigurations are required, the System Administrator must submit a TSD Service Request (TSR) Form.

TSD Service Request (TSR) Form

2.8.2 Telecommunications Installation Contractor's Responsibilities

1. Adherence to all of the above specifications.
2. Assurance of labor harmony by providing installation technicians whom currently maintains appropriate union membership.
3. The contractor must supply all cable, blocks, brackets, connectors, jacks, housings, face plates, special tools, etc., as necessary to perform an installation which is satisfactory to the Port Authority.
4. The contractor must label every workstation (jack faceplate) and the corresponding cross connect point (punch down block or patch panel) in accordance with the cable identification management plan, as previously described.
5. Install all Category 5e cabling in the proper manner, with the appropriate number of twists, so as to maintain Category 5e integrity and capabilities, as outlined in the TIA/EIA 568-B.2 standard.
6. The contractor must ensure that cable connections are in accordance with standard telecommunications practices and that all cabling maintains normal connectivity and continuity.
7. All materials must be agreed upon by PA Network Services prior to the start of installation.

All computer or network communication rooms and closets are to be isolated, locked, and secured. No other equipment, storage area, or smoking area are to be located in this room. Access to this room will be reserved to TSD staff and an agreed upon member of the site where the PAWANET equipment is located. This procedure is to ensure the security and the integrity of the Port Authority's computer network and its users.

2.8.3 Electrical Requirements

The following power and receptacles should be installed to support different equipment requirements such as:

- Standard 110/120 volt power receptacles
- Standard and/or NEMA 5L-30P 208/220 volt power receptacles
- Dedicated circuit breaker per AC feed, with alternate power source.
- Server rack electrical requirements are specified in the appropriate design document.

Currently, services obtained through the PA's contract are required to have the APC (American Power Conversion) UPS included in the delivered service.

2.8.4 Telephone Company Interface

The following items are needed for the telephone company interface. If your department has contracted with the Technology Services Department (TSD) to provide internal telecommunications for the department's network, TSD will provide them. If the department is designing and procuring its own network resources, then the department will be responsible for providing them, depending on the requirement of the department's network.

a) Install a dedicated wallboard for Telco demarcs

b) Standard Telco Demarcs:

- P66 Block
- Network Termination Unit (Rj48 interface) Smartjacks
- Network Termination Unit (DB15-pin female interface)
- Network Termination Unit (V.35/V.36 female interface)
- Digital Signal X-connect (DSX)
- Basic T1 CSU/DSU
- Basic DS3 handoff coax/HSSI unit
- High-speed dialup modems for network trouble-shooting when needed

2.9 Documentation

It is the responsibility of the System Administrator to establish and maintain a library of all documentation designated as standard by the Port Authority. These include archived system files and system backups. System Administrators should refer to the *Guide to System Administration* for a list of standard/required documentation.

3.0 Virus Scanning & Management

3.1 Overview

This section describes the standards and guidelines for the prevention, detection and removal of computer viruses, (malware). Its purpose is to minimize the risk and negative impact of computer virus infections in the work environment by establishing clearly defined roles, responsibilities and procedures for the effective management of computer viruses. To that end, the Technology Services Department has established a procedure with the **Customer Support Desk** to provide an expedited response for quick containment. The phone number is **212-435-7469**, and the Support Desk is staffed 24 hours a day, seven days a week.

3.2 Background

A computer virus, in its simplest form, is a software program written to alter the way a computer operates--without the permission or knowledge of the user. The virus enters a PC desktop or a departmental network server when the user executes an infected program or data file. Computer viruses can spread via removable media, or from files downloaded from online services or the Internet, or through electronic mail attachments. Multiple infections can occur on the desktop as these files are used or copied across the network.

Computer viruses can destroy or alter valuable data and program files. If not detected and eradicated, they can spread to other PC desktops causing serious disruption in business operations and considerable loss of staff time and valuable data.

3.3 Standards

Standard virus protection software must be installed on all network servers and personal computers, and updated on a regular basis. Departments are required to implement appropriate procedures to ensure adherence to this standard and to promptly report all virus incidents to the Customer Support Desk.

All users must leave the current version of virus scanning software installed on their desktops. For the current standards on virus protection software, click below:

Workstation Software for Windows XP

Workstation Software for Windows XP 64 bit

3.4 Virus Detection and Response

The Port Authority's IT support vendor is responsible for responding to all virus outbreaks, as well as eradicating them and, where possible, preventing them.

The speedy reporting of all computer viruses is essential for the protection of the information stored on Port Authority LANs. Much of that information is important to the safety of the public, as well as the day–to-day business of the PA.

If the anti-virus software has detected a virus and cleaned it, no further action is required on the end-user's part. If the virus is not cleaned, or the end-user suspects that a virus still exists, the end-user should immediately contact the Customer Support Desk, and

they will work to remove the virus. The Port Authority IT support vendor will respond quickly to all such alerts by doing the following:

Assess the risk

- Confirm the existence of a virus.
- Take appropriate measures to quarantine the virus so that it does not infect other Port Authority devices.

Notify Appropriate Parties

- Contact the originating party who introduced the virus to the Port Authority.
- If it is a new virus, contact our antivirus vendor, McAfee, for further assistance.

Remove the virus

- Work with appropriate parties until the virus is removed.

In addition, the Port Authority's IT support vendor will report on all such outbreaks on a weekly basis. The report must include:

Support Ticket Number

User Name

Virus Name

Information which was lost, (if any)

Time to correct the problem, (lost staff time)

Virus Origin, (if this can be determined; Diskette, CD, Internet)

3.4.1 Preventing Virus Outbreaks

The following tips will help end-users prevent virus outbreaks:

- Ensure that your computing devices, especially laptops, have antivirus installed and running. (McAfee displays a shield with a "V" in it, in the lower right-hand corner of the computer screen.)
- Ensure that your virus DAT files are up to date. (For McAfee, "right-click" the shield and select "About VirusScan...". DATs are updated daily. If your DATs are more than 2 two days old, update them by "right-clicking" the shield and selecting "Update Now".) Then,

contact the Customer Support Desk to determine why your DATs are not updating automatically.

- When copying data from removable media, (floppy disks, CDs, DVDs); be sure you are getting them from a trusted source. Ask if the media has already been scanned for viruses.
- When downloading data from the Internet, only do so from known / trusted sites.

3.5 Virus Protection Stand Alone PCs and Laptops

Users of stand-alone PCs and laptops are responsible for ensuring that virus protection is running and up to date on these devices. Users of such devices should contact the Customer Support Desk if they need assistance.

3.6 Acquisition and Installation

The Technology Services Department maintains current versions of standard virus protection software and virus detection files, (DATs), including configuration-specific instructions for downloading and installing the software on network servers and desktops. Staff should contact the Customer Support Desk for assistance.

4.0 Electronic Mail

4.1 E-Mail Overview

The PA's Electronic Mail System (E-Mail) is designed to facilitate Port Authority business communication among employees, job shoppers, contractors, consultants, and outside business associates. This E-Mail system is comprised of Microsoft Outlook desktop software accessing e-mail stored on Microsoft Exchange servers. This solution also includes group calendaring and workgroup collaboration.

4.2 Policy on Use of E-Mail: Highlights

The Computing Resources Policy provides guidance on the appropriate use of e-mail. This policy applies to any person who has access to the E-Mail system. For a complete copy of the policy, click on the link below.

Computing Resources Policy

Highlights of the policy are:

- The E-Mail system is not intended to transmit sensitive materials, such as personnel decisions and other similar information.
- All e-mail messages and attachments are property of the Port Authority. The system is not to be used for employee personal gain or in support of any purposes not related to Port Authority business.
- An e-mail message should not be used for disseminating information that is critical and/or needs to be retained longer than 120 days. Such information should only be transmitted as an attachment, for example a Microsoft Word document. The attachment must be filed outside the E-Mail system for retention and security in accordance with the Port Authority Records Retention Program if appropriate.
- The Port Authority reserves the right to review the contents of any e-mail communication when necessary for Port Authority business purposes.
- Employees and other users may not intentionally intercept in any way another person's e-mail messages without prior authorization.
- E-mail may not be used for the solicitation of funds or for messages that are political, harassing, threatening abusive, defamatory, obscene, religious, sexually explicit or unlawful or that infringes on copyrights. Use of e-mail for employee organization business other than communication with management representatives is also prohibited.
- Each message is automatically deleted from a user's mailbox on the Exchange server and from backup media a total of 120 days from the date of receipt or creation. It may be deleted without notice.
- E-mail messages or attachments that you delete may remain active on other recipients' accounts or on backup media, but for no more than thirty days on back up media.
- Contractors and other third-party users who are in violation of this e-mail policy may be denied access to the system and legal remedies may be pursued.

- Employees who violate the e-mail policy may be subject to disciplinary action, including dismissal from employment. In addition, misuse of e-mail may be referred for criminal prosecution.
- Passwords should be difficult to guess and changed every 90 days to ensure security of the e-mail messages. Users should not share their password with anyone else. Users are accountable for messages sent from their accounts.

4.3 E-Mail Etiquette

Since e-mail is different from paper-based messages, e-mail messages require certain conventions to ensure effective communication. For information on E-mail Etiquette click on the link below to view the document stored on eNet :

E-Mail

4.4 E-Mail System Architecture

The Port Authority's E-Mail system is hosted by AT&T Corp. who acquired USinternetworking, a managed application service provider, and consists of Microsoft Exchange servers connected to the Port Authority's enterprise network. Authorized Port Authority staff access their corporate e-mail through Microsoft Outlook desktop software on the network. The system has multiple Exchange servers containing mailboxes and Public Folders. Additional servers host Outlook Web Access, Blackberry services, and perform Internet-based e-mail services including anti-spam and anti-virus e-mail checking.

The hosted Exchange site is on a Windows resource domain with a one-way trust to the Port Authority's corporate user account Windows domain located on the Port Authority network. This Port Authority Windows domain is used for Windows authentication services when the Outlook client is opened. In addition, the Port Authority hosts DNS servers to satisfy requests from the Outlook client as needed.

High-speed, secure, and redundant network connections connect the USinternetworking data center and network to the Port Authority network.

4.4.1 Public Folders in the Exchange Organization

Public Folders on a Microsoft Exchange server provide a public forum where authorized users can share information, such as project information. In general, Public Folders should be used for dynamic--that is, frequently changing--information--or, for files or e-mails that are being worked on collaboratively by a workgroup. Static documents, such as corporate policy statements, should be placed on the corporate Intranet (eNet) and not on the Public Folders. Documents to be stored long-term should be stored outside of the E-Mail system such as on a Novell file server and in accordance with the Computing Resources policy and Records Retention program if appropriate.

All Public Folders reside on the Public Folder servers. Such Public Folders are created, and then supported, by the Technology Services Department at the request of a department. When a request is received, TSD reviews it to determine whether it is an appropriate use of a Public Folder; or, if it is not, whether some other mechanism for communication or collaboration is needed such as EmployeeNet. The criteria used for determining the appropriate use of Public Folders are as follows:

- Information must be dynamic.

- Public Folders should not be used to replace storage on a workgroup's shared network directory.

4.5 E-Mail Environment: Design Considerations and Infrastructure

The E-mail environment is further described below:

- The E-Mail system is comprised of Microsoft Outlook 2007 desktop software accessing e-mail (via MAPI mail protocol) stored on several Microsoft Exchange 2003 servers.
- E-mail is protected by TrendMicro's InterScan and ScanMail virus protection software products on the Exchange servers.
- Incoming Internet-based e-mail is also scanned for Spam and for viruses through McAfee (MX Logic), a web-based service provider.
- The servers are currently configured for the following messaging protocols:
    - MAPI (Microsoft's Messaging Mail protocol)
    - Internally for X.400 mail protocol (which Exchange servers use)
- IMAP4 and POP3 mail protocols, NNTP news protocol, and LDAP directory protocol are disabled.
- Front-end Exchange servers running TrendMicro's Internet Messaging Security System (IMSS) are being used to send and receive Internet SMTP mail. No other mail system connectors (such as Lotus Notes) are in place.
- RIM's Blackberry Enterprise Server software for Exchange provides wireless e-mail and calendar access to Blackberry wireless handheld device users.
- The two supported forms of SMTP addresses are:
    - Primary form: Flastname@panynj.gov
      FLastname where F is the first initial of the user's first name and Lastname is the last name, and FLastname conforms to the corporate standards for a unique Novell user's username (also known as Novell ID). Flastname is also used as the Alias for a user in the Global Address List. Note that an earlier format with truncating the above to a maximum of eight characters is still in use for accounts created prior to Sept. 2001 (example: Flastnam@panynj.gov).
    - Secondary form: Firstname.Lastname@panynj.gov
- Exceptions are governed by Novell directory structure and user account requirements.
- Each individual e-mail message and its file attachments has a combined limit of 10MB.
- Each regular user mailbox has the following size limits:
    - 45 MB - user receives warning notice
    - 55 MB - user is prohibited from sending
    - 85 MB - user is prohibited from sending or receiving

- When we upgrade to Exchange 2007, later this year, the mailbox storage limits will be increased as follows:
    - 80 MB – user receives warning notice
    - 90 MB – user is prohibited from sending
    - 100 MB – user is prohibited from sending or receiving
    -
- This E-Mail system also includes group calendaring and workgroup collaboration.
- Public Folders are supported based on departmental and agency-wide requirements and, in general, are used for dynamic items for a form of workgroup collaboration. Static documents like corporate policy statements are placed on the corporate intranet (EmployeeNet) and not on the Public Folders. Documents requiring long-term storage are stored elsewhere such as on Novell file servers.

4.6 Remote Access to E-Mail

We provide a secure Internet-based web browser access to corporate e-mail utilizing Microsoft's Outlook Web Access (https://email.panynj.gov). In addition, we have wireless e-mail access utilizing RIM's Blackberry Enterprise Server and Blackberry handheld devices.

Also, remote access to the Port Authority E-Mail system is available through the Agency's Remote Access System. Please refer to the section on Remote Access System in this document.

5.0 Intranet

5.1 Intranet Overview

The Port Authority EmployeeNet (eNet) is intended to provide timely information and resources to employees via the web browser on their desktops. eNet is a decentralized collection of web pages, data lookup services and applications that are managed as if they were a centralized enterprise resource. It is accessible to all personal computer workstations on the Port Authority Wide-Area Network (PAWANET). eNet is housed on servers at the Teleport.

Examples of business information hosted on eNet include:

- Departmental Websites
- Directories
- Corporate Announcements
- Reference Materials
- Document Collections
- Library Services
- News Displays
- Enterprise and Departmental Applications

5.2 Direction of eNet Development

eNet is intended to provide a convenient, timely and accurate source of information for Port Authority employees as well as providing access to enterprise and departmental applications. The owner of content on eNet is responsible for authorizing its publication, its accuracy and timeliness. Technology Services provides a common infrastructure and technical support for those departments that electronically publish agency information or make available electronic resources. Infrastructure standards and guidelines are recommended to ensure compatibility and facilitate maintenance. Departments requesting specific applications should discuss their requirements with eNet staff to determine a solution that best meets the department's business needs.

5.3 eNet Software Infrastructure Standards & Guidelines

Category	Software Name	Minimum Version
Browser:	Microsoft Internet Explorer	7.0
Browser Plug-in:	Windows Media Player	10.0
	Adobe Acrobat Reader	9.0

Category	Software Name	Minimum Version
	Macromedia Shockwave Player	9.0
Web Server Software:	Sun One Web Server	6.1
	Microsoft IIS	5.0
Media Server Software	Microsoft Media Server	9.0
Application Server Software:	Macromedia ColdFusion MX	7.0
Development and Design Tools:	Macromedia Dreamweaver MX	9.0
	Macromedia Fireworks MX	9.0
	Macromedia Flash MX	9.0
	Adobe Photoshop	9.0
Database	Oracle Database	9i
	Microsoft Access	2007
Programming Language/Scripts	ColdFusion MX Java PERL for Windows JavaScript	7.0 2.0 5.0 1.0
Search Engine Software:	UltraSeek	5.7
Bulletin Board/Discussion:	Chatspace WebBoard	6.0
Web Performance Monitoring:	WebTrends Marketing Lab 2	2.0
Content Management:	Stellent	7.5

5.3.1 Design Guidelines

We have developed the following guidelines to ensure that all web pages on eNet have a consistent look, feel and navigation scheme, while providing creative flexibility.

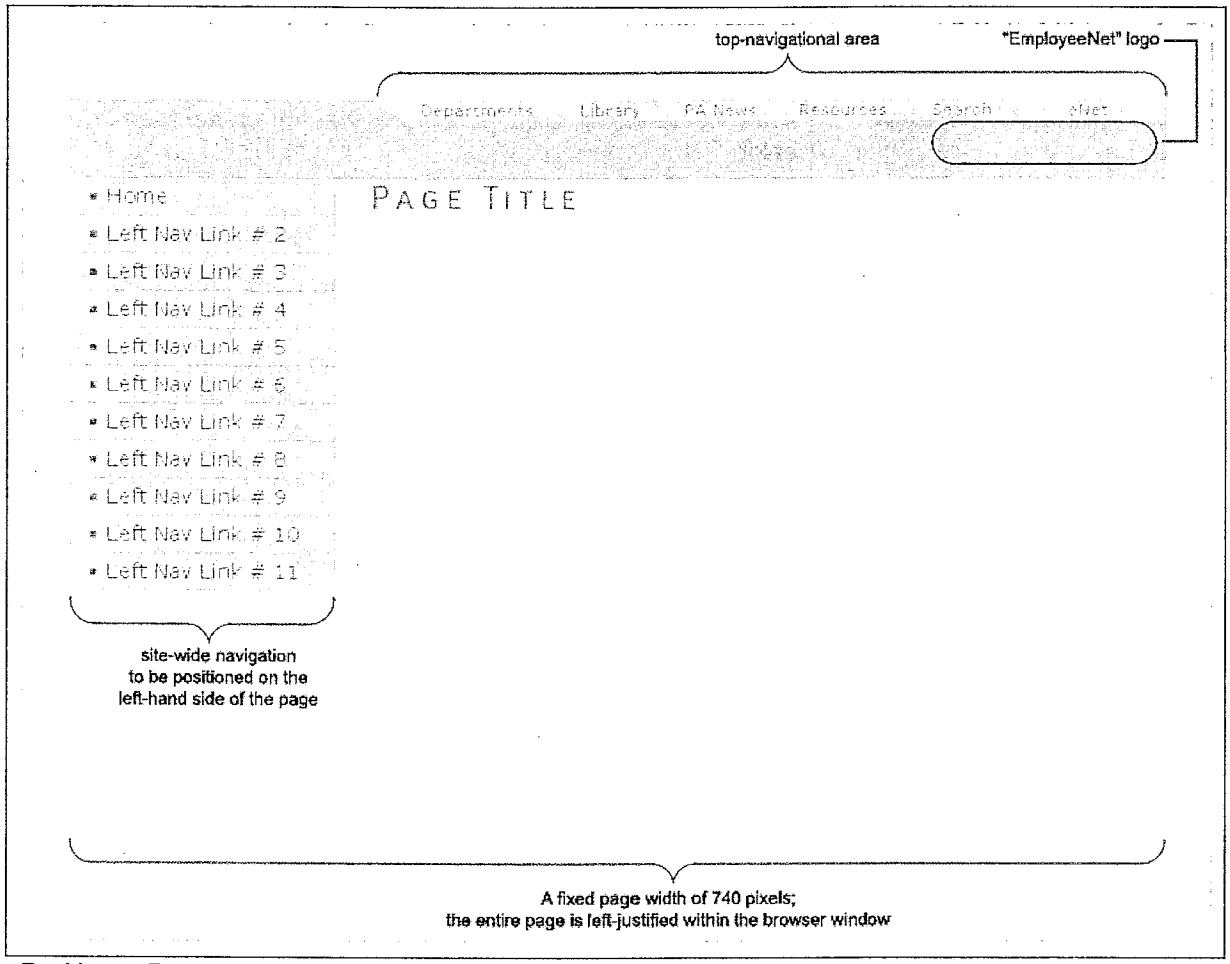
Departmental Web Site Standards and Guidelines

Prescribed standards are assigned to only the following items:

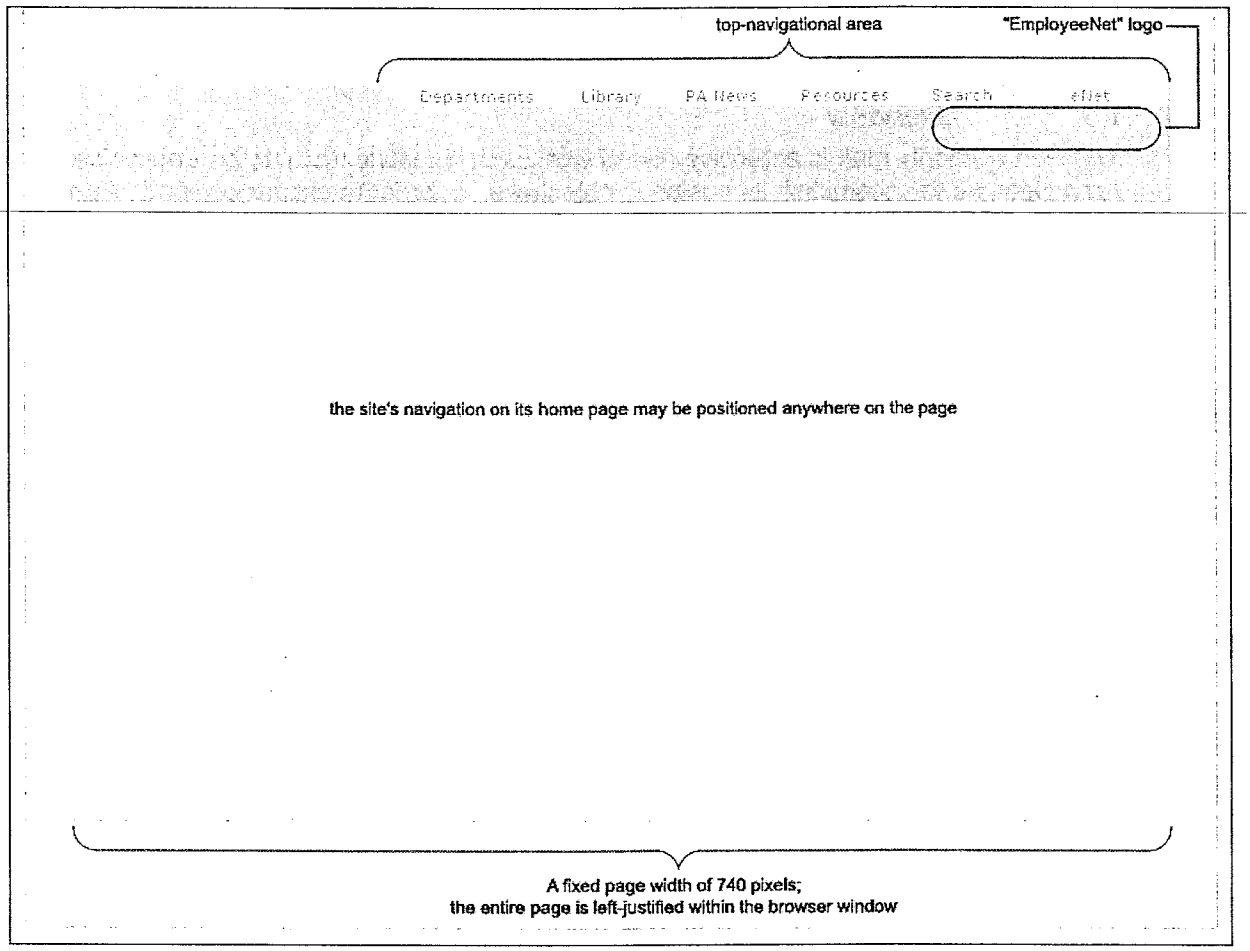
Page Width:	A fixed page width of 740 pixels
Page Justification:	The entire page is left-justified within the browser window
Global Navigation:	A top-navigational area, which provides for global links within eNet
eNet Logo:	The top-navigational area includes an accompanying "EmployeeNet" logo whose position is fixed
Resolution:	Pages will be designed for optimal viewing at the 800x600 setting.
Site Navigation:	Site-wide navigation shall be positioned on the left-hand side of each page, except for the home page, where navigational links may be positioned anywhere on the page. All efforts should be made to present the entire navigational scheme without the need to scroll. Positioning of each navigational link must be consistent throughout the entire site.
Masthead - Heading and Subheading:	The design for the masthead area, which included the page heading and sub-heading, shall be flexible and will be developed with the customer department.
Body:	The design for the body area shall be flexible and will be developed with the customer department.

The Departmental Web Site Standards are Illustrated Below:

A. Basic Page


top-navigational area
"EmployeeNet" logo
Departments
Library
PA News
Resources
Search
eNet
PAGE TITLE
Home
Left Nav Link # 2
Left Nav Link # 3
Left Nav Link # 4
Left Nav Link # 5
Left Nav Link # 6
Left Nav Link # 7
Left Nav Link # 8
Left Nav Link # 9
Left Nav Link # 10
Left Nav Link # 11
site-wide navigation
to be positioned on the
left-hand side of the page
A fixed page width of 740 pixels;
the entire page is left-justified within the browser window

B. Home Page



5.3.2 Accessibility Guidelines

TSD's eBusiness Unit is committed to making all eNet content accessible to persons with disabilities. In order to ensure that all eNet web content is in compliance with accessibility guidelines and applicable legal requirements, contact the Webmaster via email at webmaster@panynj.gov, or call 212-435-3294.

6.0 Workstation and Workstation Operating System

6.1 Overview

The Port Authority makes extensive use of workstations networked into an Enterprise Wide Area Network to accomplish its business objectives. In order to ensure compatibility with the agency's Enterprise network and to make optimal use of its resources, this section defines the standards governing workstations and their configuration and use.

6.2 Workstation Inventory

All computer related hardware, including printers must be maintained in the Port Authority's (PA) PC inventory. Tivoli Asset Management for IT (TAMIT) is the system of record for all managed PC assets within the PA. The data obtained from this system is used for PC inventory reconciliation purposes and report generation. Users requesting changes to their PC inventory – including the decommissioning of assets, reassignment of equipment to another person within the same department/organizational unit, etc - should contact their Departmental IT Coordinator. The Departmental IT Coordinator should send the request to: jgrant@panynj.gov for processing. This e-Mail notification should include, at a minimum; the Serial Number of the PC, the user name, department number, organizational unit number and the type of change required. This information must be received by the 20th of each month (or previous business day) to be reflected in the subsequent month's report.

6.3 Workstation Operating System Standard

The Port Authority's standard operating system for workstations is Microsoft's Windows XP Professional. The current versions of workstation software for Windows XP are contained in the links below:

Workstation Software for Windows XP

Workstation Software for Windows XP 64 bit

6.4 Workstation Configuration

6.4.1 Workstation Naming Conventions

All departmental workstations must contain a unique computer name which is the machine's serial number.

Example: Workstation name: 23AAH86

System Administrators are responsible for naming workstations and maintaining an up-to-date inventory of equipment and names used.

6.4.2 Workstation User Accounts

Windows workstations must have user accounts that correspond to the user's network user identification. All workstations should include at least two login accounts, the local Administrator account and at least one user account. The local Administrator account should be used only by the System Administrator for workstation installations and maintenance.

6.4.3 Remote Workstation Management

The Port Authority also distributes software applications and upgrades via Novell's ZENworks. Each workstation should have Novell's Workstation Management module installed as part of the NetWare workstation client. This will enable remote distribution and updates of software, hardware inventory and workstation troubleshooting.

6.4.4 Drive Mappings

Drive mappings for workstations should be accomplished only through the Novell login script and should conform to the standard outlined. Locally configured drive mappings to network volumes are discouraged and should not be used. See Section 2.2.2.1 for drive mapping conventions.

6.4.5 Standard Workstation Hardware Configurations

There are standard configurations established for workstations and laptops. The standards specify the product approved for the following devices: processor, memory, storage, CD/DVD-ROM/multimedia and monitor. The current workstation standard can be accessed using the link below:

Workstation

6.5 Standard Department Workstation Software

The following software is the standard Port Authority software for departmental workstations. New computer installations should conform to the existing standard. Previous installations may use the alternate standard until they are replaced or upgraded.

6.5.1 Standard Workstation Software

Windows XP, Professional Edition

Novell NetWare Client

Novell LAN Workplace Pro

McAfee Antivirus

Internet Explorer

Microsoft Office Professional

WinZip

Because technology is rapidly changing, the links below should be consulted to obtain the most recent versions of standard software.

Workstation Software for Windows XP

Workstation Software for Windows XP 64 bit

Approved and Supported Software

6.6 Enterprise Software

The sections below describe the standard Enterprise software.

6.6.1 PeopleSoft

Users requiring access to the Port Authority's Human Resources – Payroll System (PeopleSoft) must enter the link to the PeopleSoft application in their browser.

6.6.2 SAP

Users requiring access to the Port Authority's Financial and Procurement system (SAP) must have the current client installed on their workstation. System Administrators are responsible for installing appropriate components on the user's workstation as well as maintaining current application files on the network server for use. System Administrators must also work with the Customer Support Desk to install and configure IP addressable printers for use with SAP.

6.6.3 Other Business Applications

Other Enterprise applications are deployed on occasion to user workstations. This includes systems like the Business Expenses system, (BEAM) and BudgetPro. System Administrators are responsible for deploying the workstation clients and network server software according to standards and guidelines provided by the Technology Services Department.

For the current list of Enterprise applications, click on the link below:

Enterprise Applications

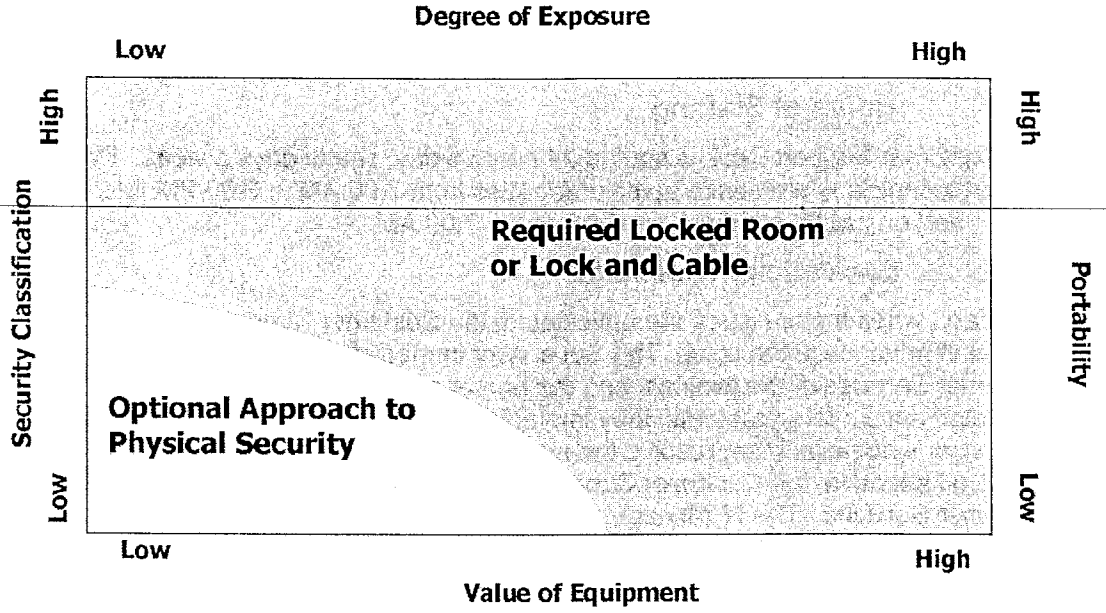
6.7 Workstation Security

Workstation users and their managers are responsible for the security of computer equipment and safeguarding critical corporate data and access to Port Authority network resources. This includes both the physical securing of equipment as well as logical safeguarding equipment and data.

6.7.1 Physical Security

The method of control should be based on the value of the equipment, the sensitivity of the data, its portability and the degree of exposure to theft. The department's Business Systems Manager should make the appropriate determination of physical security required based on their best business judgment. In addition, it is recommended that workstations be assigned a coded theft recovery ID.

The graph below provides general guidance to Business Systems Managers in determining the level of physical security required.



6.7.2 Logical Security

Port Authority departments are responsible for providing for the security of computer resources and devices:

- Workstations should be protected with a boot-up password during power on.
- Screen saver passwords should be implemented with a maximum of a fifteen (15) minute time-out.
- All critical data should be backed up nightly onto either external media or a network drive.

6.8 Customer Support Desk

6.8.1 Functions

The Customer Support Desk's primary role is to provide assistance, troubleshooting, and first resolution of the problem. When necessary, problems are referred to the appropriate party. Customer Support Desk Agents are equipped to answer questions pertaining to vendor-packaged software, hardware problems, resetting of passwords, etc. Incoming calls are evaluated and a determination made as to whether the call can be handled by Customer Support Desk Agents or referred. Customer Support Desk staff maintains records and collects information, including listings of appropriate contacts, to ensure that all calls are handled properly.

Using problem ticketing and referral software, each call is assigned a problem number, and then forwarded to one of the following: the System Administrator, a desktop technician, a Port Authority staff member responsible for that particular problem, or an outside contractor. A ticket is opened and an email submitted with the ticket information to the customer. When the problem is fixed, the Customer Support Desk Agent closes the trouble ticket and a closure email is also submitted to the customer. When special issues arise within the Agency, Customer Support Desk staff is alerted. They plan a strategy to resolve the problem and handle incoming calls related to the issue. Reports of outstanding ticketed

problems are generated daily by the Customer Support Desk ticketing system for management review.

6.8.2 Hours of Staffing

The Customer Support Desk is staffed 24 hours a day, seven days a week. Desktop support technicians are onsite at major facilities from 7:00 AM to 6:00 PM, Monday through Friday, and on call as needed from 6:00 PM to 7:00 AM.

6.8.3 Escalation Procedures

Generally, when major issues are anticipated, the Customer Support Desk Supervisor is notified in advance of the issue. The Supervisor immediately alerts the IT Manager Customer Services of the problem and the proper response. When the Customer Support Desk staff encounters problems, they immediately notify the Customer Support Desk Supervisor who helps them resolve the problem. If the issue is urgent and requires additional attention, the Customer Support Desk Supervisor notifies the IT Manager Customer Services. The IT Manager Customer Services then escalates to the Assistant Director, Technology Infrastructure and others, as appropriate.

6.9 Administrative Rights Procedure

Technology Infrastructure & Service Delivery (TISD):

A PA3624A form is submitted to the TISD Customer Services Group.

The form is reviewed for accuracy and sent via email to the TISD-AD for approval.

TISD AD reviews and approves request with start and end dates.

If no start and end date, the form is reviewed with the CTO for approval.

Pomeroy:

Request for administrative rights received on approved PA3624A form from TISD Customer Services Group.

For Server:

Email is sent to the Server Team with approved PA3624A form attached.

Administrative Rights spreadsheet is updated with the following information: Ticket #, Date Opened, Department, Last Name, First Name, Description of Request, Date Completed, and Time Limit.

If no time limit specified: Marked on spreadsheet as "NO TIME LIMIT SPECIFIED"

Time limit specified: Noted in spreadsheet and marked on calendar to send removal request to server team on the day of removal.

Email is sent to End User 3 days prior, notifying them of impending removal of rights on server.

On day of removal: Email is sent to the Server team to remove rights.

Rights removed by Server Team, confirmed via email.

Spreadsheet is updated.

For PC:

PA3624A form is processed with the Support Desk team to grant administrative rights to End User until specified date.

Administrative rights spreadsheet is updated with the following information: Ticket #, Date Opened, Department, Last Name, First Name, Description of Request, Date Completed, and Time Limit.

~~If no time limit specified: Marked on spreadsheet as "NO TIME LIMIT SPECIFIED"~~

Time limit specified: Noted in spreadsheet and marked on calendar to contact the End User on the day of removal.

Email is sent to End User 3 days prior, notifying them of impending removal of rights on PC.

On day of removal: Systems Administrator contacts End User via phone and/or email to remove administrative rights.

Rights removed by Systems Administrator.

Spreadsheet is updated.

TISD Assistant Director & CTO:

Review Administrative Rights spreadsheets once a month.

6.10 Computing Resources Policy

Computing resources are intended solely for the Port Authority's business. Resources are not intended for personal gain or in support of any purposes not related to the Port Authority's business. The Port Authority's policy on computing resources is provided at the link below.

Computing Resources Policy

6.11 Use of Port Authority Owned Computer Equipment at Home

The Port Authority's computer equipment may be authorized where the benefit to the organization can be clearly demonstrated and the employee's intended use cannot be accomplished in the workplace during normal business hours. The Port Authority's policy on computer equipment at home is provided at the link below.

Port Authority-Owned Computer Equipment at Home

To safeguard the Port Authority's equipment and data, all authorized users must adhere to all applicable standards as if the equipment was in use at a Port Authority site. This includes physical security of equipment and virus scanning. In addition, where persistent Internet connections are in place, an approved firewall configuration and software must be in place.

6.12 *Software Licensing Guidelines*

SOFTWARE LICENSE GUIDELINES

All software installed or running on Port Authority equipment must be licensed with a proof of purchase available for verification. Employees, Consultants or Vendors of the Port Authority must not install, upload, download, or use any unlicensed and unapproved software. Employees, Consultants or Vendors who acquire or use unlicensed copies of computer software are subject to disciplinary action up to and including suspension or dismissal. Copyrighted and licensed software may not be copied or duplicated, or installed on non-agency computers, unless such use is permitted by the software's license agreement.

The proper licensing of software is both a legal requirement and an ethical imperative. Software vendors and industry watchdog organizations regularly survey organizations for software license compliance and can assess substantive penalties for noncompliance.

Using non-licensed (copied or counterfeit) software has other risks:

- Greater exposure to viruses and corrupt or defective software.
- Inadequate or non-existent documentation and warranties
- Lack of technical support for the software
- Ineligibility for software upgrades and fixes

We must manage our software assets in a way that respects copyrights and software licenses, in order to protect confidential information and provide maximum benefit to the Agency, as well as to ensure the ongoing maintenance and operation of a safe computing environment while avoiding penalties and monetary fines.

GENERAL RESPONSIBILITIES FOR MANAGING SOFTWARE LICENSES

Procurement and Technology Services Department (TSD) will continue to work closely together to ensure that enterprise software supported by TSD, purchased through an Agency-wide agreement, and software purchased by Departments directly through

Procurement is licensed appropriately. The Audit Department will periodically perform audits in the area of software license compliance.

Appropriate documentation required to ensure software license compliance must include:

- software inventories with user counts or installation counts (including user name and machine name as appropriate)
- valid license agreements/license confirmations
- proof of purchase/email confirmation of purchase

These documents must be kept up to date and must be readily available for audit verification.

For enterprise software with agency agreements, TSD will oversee the management of these products to ensure the usage of software is within the contractual and license requirements. TSD will be responsible for addressing the documentation requirements listed above for these software products. The use of these licenses will be monitored and reviewed on an annual basis. The current list of enterprise software includes:

AutoCAD

BudgetPRO

Cognos Client Software

Livelink

PeopleSoft

Primavera

SAP

Schedulesoft

TRIM

BlackBerry

HIDS

Lumension (Patchlink)

McAfee Virus Scan

Microsoft Office 2007

Microsoft Server

MS SQL

Oracle

Record Now/Roxio

WinZip

For all other software, each department, through their business managers and IT coordinators, are responsible for assuring that software running on all computers utilized by that department's employees, vendors and contractors is appropriately licensed. The Department is responsible for maintaining and producing the required documentation listed above for this software. Departments should validate software in use against their inventory listing and purchases on a regular basis. These documents must be kept up to date and made readily available for audit verification.

Only the system administrators designated by the Technology Services Department for installation and maintenance will perform the installation of all computer software. Individuals are prohibited from installing free-ware or any software on their computers.

In situations where the presence of a given software application on an Agency computer represents a violation of copyright, license agreement, or a violation of security, privacy, or other Agency policy, remedies may include removal of the software application or, in some cases, complete review of the system on which the software is installed.

PURCHASING DESKTOP SOFTWARE

Before requesting purchase or installation of any software, the requestor should check the list of approved software available on the TSD ENET web page. This web page also provides a mechanism for requesting the review/approval of software not already on the list. Only software on the approved software list may be installed on Agency computers. This includes free downloadable utilities, browser plug-ins, freeware or shareware. No employee shall download such software to his or her computer. Only the system administrators designated by the Technology Services Department for installation and maintenance will perform the installation of all computer software, including free software.

As of July 2011, the purchase of desktop software has been centralized within TSD and is initiated by filling out a "Desktop Software Request" form #3694, available on ENET. You will be notified if your request is approved and you will also receive the license-key information. You will not receive any software media(CD/DVD). When you receive your license-key information, you should contact the Support Desk (10-7469) to arrange for installation of the software. You must provide the system administrators designated by the Technology Services Department with the valid license-key information and confirmation email to complete the install.

As stated in the General Responsibilities for Software Licenses, you should retain all information associated with the software licenses purchase. Department business manager and IT coordinators should also be provided with copies of all license information that you receive when purchasing software licenses.

7.0 Distributed Systems Environment

7.1 Overview

A number of department and enterprise servers provide critical application and system services. Different operating systems and configurations may be required for specific applications. This section provides information on the standards and guidelines for supported systems within the Port Authority.

7.2 Microsoft Windows Servers

The standard for general purpose application servers and File and Print Computing is IBM servers. Microsoft Windows 2003 & 2008 Server (Standard and Enterprise) are supported Operating Systems for application servers.

7.2.1 Virtual Environment

The standard for Virtualization Computing is both IBM and NEC FT host servers. The Port Authority will provide a VMware ESX-based Guest Virtual Machine (VM) to operate all Contractor-provided applications software on one of the above host computing platforms depending on the critical nature of the application.

All applications software shall be capable of operating in a virtual environment under VMware ESX server and shall operate in a VMware ESX-based Guest Virtual Machine (VM) on a 'shared' host computing platform for Contractor application, unless performance requirements mandate a dedicated ESX host.

7.2.2 Windows Data Encryption

For those applications that require additional data security measures, TSD offers additional tools that provide encryption services to protect the data stored in the application's database, even from authorized individuals that have physical access to the applications and database servers but not the decryption key. Prior to implementation, the Business System Manager should consult with the Technology Services Department to implement the Encrypting File System feature on Windows XP, 2003 and 2008 Servers (See http://technet.microsoft.com/en-us/library/cc700811.aspx).

7.3 Unix

Sun's Solaris is the currently supported UNIX operating system for infrastructure and corporate servers.

7.3.1 Unix Security

Unix servers must be physically and logically secured from unauthorized access. The following document should be used to secure your Sun Solaris server. Click on the link below to view the document:

Unix System Security Policy

7.3.2 Backup

Critical system backup must be performed regularly (daily and/or weekly) utilizing our centralized backup strategy and associated tools. Extra copy of backup should be kept offsite for disaster recovery purposes if required.

7.4 z/OS

z/OS (currently release 1.5) is the IBM-supplied operating system on the IBM 2096-R07. This hardware/software supports multiple users and multiple applications. Provided on this platform for transaction-processing applications are TSO/E, ISPF, and CICS. The database is DB2, although other file structures are also supported.

7.5 Databases

Oracle 10.2.0.4 or higher and MS/SQL 2005 Server or higher are the supported database platforms for Port Authority systems. Auditing trail must be enabled for all database accounts with administrator privileges.

7.6 Application Security

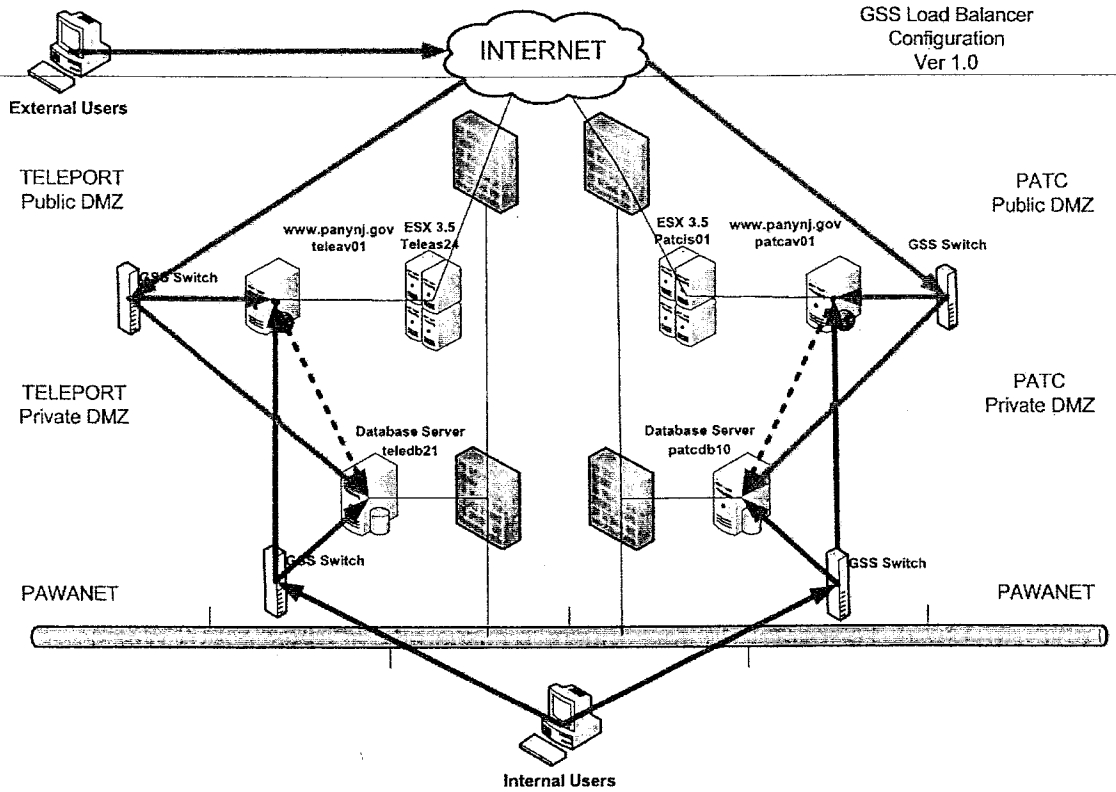
Depending on the application residing on the server, security may be administered at the application, database, module, screen, data field, and/or transaction level in addition to network authentication. Prior to implementation, the departmental manager who owns the application (Business System Manager) should review the capabilities of the application and consult with Technology Services Department staff to ensure implementation of the appropriate security levels. When in production, the administrator responsible for day-to-day administration of the application (Application Administrator) is responsible for maintaining the selected security profiles. At a minimum, all applications must require authentication to Novell Directory Services by way of a network login.

7.7 Server Physical Security

All servers and communication equipment must be located in locked rooms or secured with a cable and lock with the keyboard secured to prevent tampering and unauthorized usage. The Business System Manager is responsible for determining the appropriate access control method (receptionist, metal key lock, magnetic card door locks, etc.) He/she must also maintain a list of persons authorized to enter secured areas. Technology Services Department staff is available to provide technical assistance in making this determination.

7.8 Load Balancing – Failover Architecture

Depending on the requirements of the application, load balancing and failover architectures are supported. Below is a typical diagram of the load balancing/failover architecture.



There are a total of four load balancers, two are used for internal users and the other two are used for external users.
Cisco GSS devices support load balancing or failover configuration

8.0 Voice Network

8.1 Voice Network (Telephone) Services

8.1.1 Port Authority Telephone Network

Most of the Port Authority's telephone services are provided by a Nortel SL100 (CS2100) Private Branch Exchange (PBX) network (approx. 11, 000 lines) with a host switch at **JFK International Airport** (JFK) and remote switches at **Newark International Airport** (EWR), **LaGuardia Airport** (LGA), the **George Washington Bridge and Bus Station** (GWB/BS), **Lincoln Tunnel** (LT), **PATH /Journal Square Transportation Center** (PATH/JSTC), **PA Bus Terminal (PABT), Gateway Plaza** in Newark, NJ, **225/233 Park Ave South which serves 115 Broadway and the WTC site, 1 Madison Ave.** and the **NJ Leased Properties (NJLP)** which serves the PA Technical Center (PATC), the Jersey Ave. Maintenance Facility (JAMS), and the Holland Tunnel. Additional networked PBXs include a Nortel Meridian One PBX (130 lines) with Call Pilot serving **Port Newark** and a Nortel CS1000M switch (250 lines) serving the **Staten**

Island Bridges, with voice mail off the Call Pilot at JFK. **The PA Tech Center** also has a Meridian 1 System (300 lines) with Call Pilot for the Public Safety headquarters operation. Several of the above remote locations may also have Nortel adjuncts, such as 9150 or Norstar systems for secondary sites or special applications. Additionally, there are other PA sites (e.g., Brooklyn Piers, EWR Redevelopment, Harrison Car Shop, and Stewart International Airport) that have PBXs or service from other vendors that are maintained by the facility under separate maintenance contracts. See Appendix 10 — Voice Network Diagram.

The SL100 remote switches are tied to the JFK host via Telco T-1 links, which serve as intermachine trunks. Most of these have been transitioned to our new Sonet network from Verizon. . If the intermachine trunks are lost, the remote switches function independently in Emergency Stand Alone (ESA) mode, but only with basic "Plain Old Telephone (POTs)" features (i.e., the more sophisticated features from the host switch are not available.)

Voice Over Internet Protocol (VOIP) is in the process of being implemented at a number of Port Authority facilities. VOIP is based upon a Cisco product line of Call Manager Appliances which also include Voice Mail, Call Center, Emergency Stand Alone, along with other features and functionality that will be introduced as the installed base of VOIP phones increases. As of the 2nd Quarter of 2010, VOIP has been implemented at: Teterboro Airport, Telecenter, Journal Square Transportation Center, PATH Waldo Yards, Lincoln Tunnel, George Washington Bridge, Lincoln Tunnel, and selected buildings at Newark Liberty International Airport and JFK International Airport. Work is continuing at PATH, GWB and LT to convert Analog and Customer Service phones to IP, while VOIP implementation for Harrison Car Shop and LaGuardia Airport is in its final stages. To date, approximately 1000 lines have been converted to VOIP.

This section will be updated on a quarterly basis to track the VOIP deployment.

As of August 1, 2008, AT&T is the vendor that maintains the Port Authority's telephone network. .

Note: Most facilities also utilize some auxiliary business Centrex lines or private lines supplied directly from Verizon. These auxiliary lines often serve as back-ups to the above PBX systems. They are typically ordered from Verizon directly by the facility.

8.1.2 Local Service

At most Port Authority sites, Verizon provides local service. However, we utilize local service from AT&T Local Services at several New York sites. AT&T Local Services handles outgoing service on the JFK, LGA and PABT switches and both incoming and outgoing on the 225 Park Avenue South and 1 Madison systems.

8.1.3 Long Distance

The Authority's primary long distance carrier is currently AT&T under the NY State contract. Dedicated service is aggregated at the host PBX, where the SL100 routes long distance calls over the dedicated T-1's as a first choice: if these T-1's fail, the SL100 will route the calls over "PIC'd" service to Verizon, thus providing a redundant path and service for all SL100 long distance traffic.

8.1.4 Tie Line Network

Most facilities enjoy the convenience of our corporate dialing plan, which typically consists of a 2-digit access (tie line) code, followed by the 4-digit end user extension. This is done by connecting our main SL100 telephone hub at JFK to facilities via the intermachine links or tie lines that are leased from the local telephone company. Moreover, we avoid the usage charges associated with making intra-Agency calls over the public switched network.

Port Authority Access (Tie Line) Codes

03 - Stewart International Airport (Follow with 3-digit Stewart extension number)*

04 - Gateway

06 - Brooklyn Piers**

07 - Port Newark/Elizabeth

08 - Teleport Office Park***

10 - Park Avenue South, One Madison Avenue, 115 Broadway, WTC Command Post PAPD

11 - PATC, JAMS (NJLP), Public Safety at PATC and the Holland Tunnel

12 - JSTC/HCMF

13 - LGA

14 - EWR, 5 Marine View Plaza

15 - JFK, Bldg. 9, Vertical Control Bldg.

16 - Lincoln Tunnel, Teterboro Airport (Mgr.'s Office/REO)

17 - GWB/GWBBS

18 - Staten Island Bridges

19 - Port Authority Bus Terminal

**Users at Stewart International airport must dial "8" button in advance of the tie line access code. Note: When dialing Stewart using access code "03" from other PA facilities, you will experience 5-6 seconds of silence before you hear the Stewart greeting and can enter the desired Stewart 3-digit extension.*

***Users at Brooklyn Piers must use their access button in advance of the tie line access code.*

****Users at Teleport Office Park must dial "606" in advance of the tie line access code.*

8.1.5 Voice Mail

The primary voice mail system that serves the SL100 system is a Nortel Call Pilot system. It is located at JFK and serves approximately 4300 mailboxes. Independent Call Pilot systems that are networked to JFK's Call Pilot serve Port Newark and Public Safety at PATC (3rd floor). SIB obtains its voice mail from the main JFK host. Other vendor-specific voice mail systems that serve the non-Nortel sites include a Lucent Audix system at Harrison Car Shop and a Toshiba voice mail system at Brooklyn Piers.

Voice mailbox access is restricted by a unique password entered via the touchtone pad. Passwords must be changed every 90 days and must adhere to the password standard outlined in Section 2.2.4.5. Users should call the Telephone Help Desk at 212-435-4357 (HELP) for assistance with resetting passwords.

As indicated in Section 8.1.1, where VOIP has been deployed, Voice Mail is now provided via the Cisco based Unity Voice Mail system.

8.1.6 Telephone Help Desk

All trouble calls for lines and telephones on the PA telephone network should be directed to the **Telephone Help Desk at 435-4357 (HELP).** Outside of normal business hours, the call is forwarded to the AT&T 24X7 Help Desk for repair on the next business day. Phone numbers on each facility's Critical Line List will have a 1-hour response time. Note: Extra charges will apply if the line/phone you are reporting is not on your facility's Critical Line List, so use judgment if requesting to override the Critical Line List for an immediate repair. Telco lines that are billed directly to the facilities should be reported directly to Verizon, as follows:

- **Verizon NY Repairs**: 866-804-2640

  Verizon NJ Repairs: 800-540-6960

Note: on an interim basis, trouble calls for VOIP will also go the Telephone Help Desk. Operational procedures are being worked to migrate VOIP Help Desk functions to the

Customer Support Desk and additional information will be forthcoming when those arrangements have been finalized.

8.1.7 Telephone Moves, Adds and Changes (MAC)

Orders for new or modified SL100 and Meridian One telephone network services are coordinated by the Voice Networks Telephone Help Desk at 212-435-3257 (HELP) using the attached form (Form PA3753 on ENET.)

SL100

8.1.8 Installation and Use of Home Telephone Lines for PA Business

Installation of a local "Telco" line from Verizon in the home for PA business purposes can be arranged via a request by the Department Director and approval by the Chief Administrative Officer (See AP30-4.01-Telephone Charges). Contact Will Lassalle at 212-435-3221.

8.1.9 Installation of Modem Lines for PA Business

Installation of modem lines in the office is discouraged due to network security issues, but if a PA business reason justifies a modem line, the attached form must be completed (in addition to the SL100 Telephone Service Request form referenced in Section 8.1.7). Contact Will Lassalle at 212-435-3221.

Request for Modem

8.1.10 PA Calling Cards

AT&T calling cards for PA business use may be obtained by submitting a request to the Manager, Voice and Data Networks that explains the intended use and business justification for the card and signed by the requesting unit manager. Contact Will Lassalle at 212-435-3221.

8.1.11 Toll Free (800) Services

Toll Free Services can be obtained via dedicated Megacom circuits or Readyline Service, where AT&T redirects calls from your Toll Free number to an existing local line. To obtain assistance with arranging for Toll Free service, call Will Lassalle at 212-435-3221.

8.1.12 Audio Conference Call Services (Voice)

To take advantage of AT&T's discounted New York State/City rates for Conference Call Services to the Port Authority,

New Users must call:

Robert G Taylor

AT&T Operations, Inc.

toll free 888-478-0374

efax 512-646-3696

Existing Accounts may call:AT&T Teleconference Center at 1-888-NYS-CONF (888-697-2663) (or, use your dedicated dial-in number to set up AT&T Reservationless conference call anytime – day or night – without making a reservation in advance!)

Instructions for New Users/Accounts:

Coordinators can begin the process of establishing a new TeleConference account by simply emailing the above Sales Consultant with the following information **5 days in advance of your first conference call**:

- Verify you are with New York City account: 12516422 (Note: The PA obtains the discounted service under this NYC account.)
- Bill Name (PORT AUTHORITY, plus Dept. Abbr., plus Unit Name)
- Host Name
- Host Phone Number
- Email Address
- Billing Address
- Cost Center (3-digit unit code, plus 3 digit program/facility code; Examples. 123G01 or 123A04)

When processing new accounts, the Sales Consultant will set up:

- A "**Billing Site**" account for each PA Unit based on your Cost Center code (3-digit Org. code, plus 3-digit Program or Facility code – Examples 123GO1 or 123A04) that will be used to pay for the service.
- A TeleConference "**Folder ID**" will also be created to identify each host (specific user); Folders sit under the umbrella of each Unit's Billing Site account.

Once a Billing Site has been established, your Sales Consultant will have a Reservationless Folder ID created on your behalf. AT&T Reservationless Service provides the host with dedicated dial-in numbers and access and host codes. This enables the host to make conference calls without making a reservation in advance!

IMPORTANT: Each Unit is responsible for their own conference call account administration and billing obligations!

Please click here for more information on AT&T conference call services.

For AT&T discounted rates, open this attachment:

ATT Discounted Rates

8.1.13 SL100 Meet-me Conference Call Service (Voice)

PA staff can utilize a basic Meet-Me Conference Call service from our SL100 system that allows staff to reserve a special "435" number that allows up to 30 conference attendees (internal or external) to participate in a conference call. Each attendee dials in at the time predetermined by the organizer. The first party to call the number will continue to hear the line ring until a second party joins the call. Note: This is not a secure conference bridge, so anyone can dial in at any time. If you need a secure conference, use the AT&T service described in 8.1.13. Contact the Telephone Help Desk at 212-435-4357 to schedule an SL100 Meet-Me Conference Call.

Revised 12/22/08

9.0 Vendor Provided Dedicated Systems

9.1 Overview

Vendor Provided Dedicated Systems refers to the Information Technology software, hardware and infrastructure furnished and installed through a contract with an external provider. Generally, this refers to systems that are designed to support a large Capital Project, where the Information Technology Systems are either provided based upon detailed functional and technical requirements as outlined in a Request For Proposal (RFP); or, are an integral part of a detailed design and set of specifications prepared by an outside Engineering firm in the preparation of "Low Bid" contracts. These Capital Projects are usually large scale, multi-year engagements, requiring specialized technical and management staff, as well as, Systems Integration support. These projects normally have significant construction components and require the coordination, design and support from many diverse Engineering and Technology disciplines

The uniqueness of the Capital Projects is further reflected in the organizational structure within the Port Authority. Typically, a Line Department identifies a specific need that will require a Capital Project. The Line Department identifies the functional and operational requirements of the endeavor and solicits Project funds to support the initiative. On all technology related projects a representative from the Technology Services Department (TSD) provides a single point of contact for technology oversight, accountability, adhering to Standards and systems integration, which is required under the Roles and Responsibilities of the Chief Technology Officer (CTO) and is expected by our client departments. The Line Department or their representative shall submit a Technology Service Request (TSR) via the online form PA 3937 found on eNet, to solicit TSD support on these projects.

To ensure a successful project, and honor our responsibility to our customers and the Agency, one of the steps undertaken by TSD is to provide guidance with, and focus attention on, adherence to and compliance with the Port Authority Technology Standards and Guidelines. By following the Standards and Guidelines, it enables the Port Authority to leverage the large discounts negotiated in the various requirements contracts, ensures that the equipment can be gracefully integrated with other existing systems, and ensures that long term maintenance and systems administration contracts will be focused on the same product lines. Ensuring that the relevant sections of the Standards and Guidelines are included in either the basic design of a low bid contract or as requirements in an RFP is the first step. Responses to RFP's should be reviewed for their compliance with the Standards and Guidelines. Deployment, integration and testing should be monitored by TSD to ensure that equipment or infrastructure is not duplicated, that the integration and migration plan will not adversely impact existing systems, and to integrate new systems under existing maintenance contracts where applicable.

In cases where a specific vendor or system is so specialized that it normally does not adhere to the hardware, software, infrastructure and operations guidelines of the

Standards and Guidelines, the vendor should be directed to work with TSD in exploring all options, and if an exception is deemed required, the vendor should work with TSD to prepare the necessary Business Case to receive written concurrence from the Chief Technology Officer for this deviation from the Port Authority Technology Standards and Guidelines.

9.2 Physical Security Technology Standards

9.2.1 Agency Standard for Digital Video Recording and Access Control and Alarm Monitoring

Based upon the Agency's investment in and positive experience with Lenel's access control and alarm monitoring and Loronix's CCTV and Digital Video recording technologies, these product sets are the Agency's standard (please see below a description of when these standards apply).

The Port Authority has long recognized the need for a corporate architecture for its security systems that would allow us to integrate compatible technologies agency-wide. September 11th reinforced the need to maximize the Port Authority's investment while providing for redundancy. Using these standards will improve the Agency's security posture and will permit us to leverage additional operations and business benefits while keeping our operations resources, maintenance and support costs at a minimum.

A standard will also improve:

- The capabilities of an Emergency Operations Center and other facilities;
- The operational and cost-effectiveness of adding a variety of modular features to the core systems, such as paging, e-mail, fire systems, facility management, etc.;
- Alarm notification, response, and acknowledgement;
- Operational flexibility for facility and Public Safety staff;
- Access to and the sharing of information;
- Single learning curve;
- Minimization of maintenance and system administration costs.

Guidelines for using the Loronix standard include:

1. If the camera system needs to be recorded
2. When an upgraded or new system is being installed at a PA facility or at a tenant facility monitored or reviewed by Agency personnel or contractors
3. When rule based intelligence is to be added like motion detection and other related algorithm processes
4. If WEB based video needs to be made available
5. When monitoring at remote locations is needed to view on site operations and archived events via the corporate WAN
6. When live monitoring is required.
7. When distributed recording is required i.e. at multiple locations, concurrently

8. When network transport (communication) medium has limited bandwidth and the video needs to be sent to designated workstations on the network. Discuss bandwidth issues with Technology Services Department before proposing alternate solutions
9. On all new projects where Loronix is the site base system now.
10. When the OEM department needs override capabilities in the event of an incident.

Guidelines for using the Lenel standard include:

1. On all new or upgrade projects that need card access and / or alarm monitoring
2. On projects that will have security that needs to be monitored by PA personnel or contractors (airports are monitored by contractors)
3. On all new projects where Lenel is the site base system now
4. Where access is required to work with ID cards that exist and are compatible with Lenel
5. When the OEM department needs override capabilities in the event of an incident.

9.3 Communications Infrastructure Standards

The Port Authority Standard for Communications Infrastructure is Cisco. The link to the CTO's memo on communications infrastructure standards is shown below.

Memo on Communications Infrastructure Standards

This applies to all future systems, as well as, upgrades to existing systems. This standard ensures the interoperability of all deployed systems and permits the full integration of systems into PAWANET. In addition, all Cisco equipment either designed in a low bid contract or specified in an RFP should be purchased through the Cisco Requirements contract, which is administered by TSD and permits the Agency to purchase equipment, maintenance and support services under the high discounts negotiated in the Requirements Contract.

This standard applies but is not limited to; Layer 2 and 3 Ethernet switches, Routers, Wireless Access Points (WAP), Mobile Access Routers (MAR), GIG E (Gigabit Ethernet) switching and networking and SONET (Synchronous Optical NETwork) equipment.

Deviation from this standard requires the written consent of the Chief Technology Officer.

9.4 Server Infrastructure Standard

The Port Authority's standard platform for File & Print and Application servers is IBM. The link to the CTO's memo on server infrastructure standards is shown below.

Memo on Server Infrastructure Standards

Technology Services has contracted discounted pricing with IBM for its servers and hardware support. In order for the agency to take full advantage of these savings, any new Application servers or File & Print servers must be built using IBM hardware. This includes turnkey and distributed systems where File & Print or Application servers are specified in the design. Any replacement File & Print or Application servers must be IBM servers. Deviation from this policy will not be allowed without prior approval of the Chief Technology Officer or his designee.

10.0 Wireless Technologies

10.1 Wireless Guidelines

10.1.1 Purpose and Scope

Applies to: all wireless devices and technologies including voice and data capabilities that store, process, transmit or access data.

Includes but is not limited to commercial and unlicensed wireless networks and laptops, cellular devices, scanning devices, messaging devices (2-waypagers and email devices) and PDAs.

10.1.2 General Policy

Employees will only use PA owned wireless devices to store, process, transmit or access PA data.

The following must be considered:

Wireless Technologies Vulnerabilities Protection

Minimum Requirements

Identification and authentication at both the device and network level.

Confidentiality encryption of data transmitted is required.

Data end-to-end over an assured channel (a communication link with security protocol such as Secured Sockets Layer).

At the device level, implement file system encryption where applicable.

Devices should not be connected to PA systems for data synchronization, data transfer, or any other purpose without virus protection, mobile code restrictions (executable information delivered to information system and directly executed on any architecture that has appropriate host execution environment) and other preventative measures.

10.1.3 Personal Area Networks - PAN

PAN technologies should not be used for transmitting information without encryption.

Bluetooth security alone is unacceptable because it is not encrypted and does not use Federal Information Processing Standardization (FIPS) 140-1/2.

Wireless devices should be procured without Bluetooth embedded transmitters, when not possible transmitter should be disabled

10.1.4 Wireless Local Area Networks - WLANs

I- OVERVIEW

Business requirements have arisen throughout various Port Authority locations for the improved use of Wireless LAN technology to facilitate local user mobility. Research has been done on the different technologies supported via Cisco as opposed to various wireless vendors in an attempt to produce a standard that will provide the agency with a secure, robust and scalable solution as WLAN's continue to grow within the agency.

This document from the desk of TSD's Senior Network Specialist is targeted for an agency wide audience of network designing and implementations for deploying wireless LANs within the agency.

In summary, the current Port Authority Wireless Lan standards are based upon IEEE 802.11n draft 2.0 technologies. (802.11n is backwards-compatible with existing 802.11a/b/g network adapters.)

The physical infrastructure is now based upon a centralized WLAN architecture that relies upon **Cisco** wireless **bridges**, **access points**, **mesh routers** and newly implemented **controllers**. WLAN's should be standardizing on the 4404 and 4402 controllers at this time as described further in this document.

Wireless LAN technology is continually developing with rapidly evolving industry standards, government regulations, and vendor products. As a result, the WLAN Standard presented in this document will likely be superseded in the future as the technology and products change.

II- SCOPE

The scope of this document shall present some standards for the Agency Wireless LAN and the specification of all devices and configurations.

III- PRINCIPLES

At the highest level, the principles for the Wireless Standard are based upon the following attributes:

- **Security .. use of strong encryption ... e.g. WPA-TKIP / WPA2- AES, for use as authentication of all traffic on a port-to-port basis, with the use of credentials stored on a back-end RADIUS server utilizing key distribution.**
- **Scalability** .. with LWAPP access points & use of LWAPP tunnels
- **Reliability** .. via authentication of users to the networking enterprise mode.
- **Manageability** .. via secured ports and VPN / FW access.

IV- OWNERSHIP

This document is under the ownership of Bill McPherson the Port Authority's IT Senior Network Specialist.

V- COMPLIANCE, REQUIREMENTS

All specifications defined in this document may be effective upon approval of and complete concurrence with TSD's CTO & Senior IT Architecture, to update wireless standards and policies as per IEEE and Wi-Fi Alliance std.

VI- DEVICE SPECIFICATIONS

The following sections will detail the various hardware components, and related firmware versions, that are specified for use in the Port Authority's WLAN solution.

6.1 Access Point Standard

Standards Details:

- **1250** AP's are the agency standard for WLAN deployment. These AP's have 802.11n 2.0 radios. Backward compatible to 802.11 a/b/g. 1242 for light-weight AP's for WLAN controller.
- 1310 AP/ Bridge is certified for use in unique situations where both internal and external antennae are supported. The major distinction is that of a more rugged chassis designed for higher-stress outdoor-type conditions. 3250 mobile routers for mesh deployments.
- Physically the device models (1242 & 1230) by

  default when AP connects to controller automatically becomes an access point.
- All autonomous, IOS APs must be upgraded to LWAPP, Note: LWAPP

  Upgrade requires AP to run at least IOS version 12.3.7. WAP2 with AES / CCMP for unique authentication deployments.

- **AP 350 is no longer supported.**

- **AP Standard Summary**:

  a. Two cables per pull during wiring for wired to wireless.

  b. AP's & controller placements via RF propagation results.

  c. PA supported standard AP's:

  - v4.0.217.0 or above
  - 1242 & 1310 usage were spectrum analyzer testing warrents.
  - 1200 IOS AP must be LWAPP capatible.

d. AP fallback enabled

e. 3 SSIDs-each on separate VLAN's as per radio configurations.

Note: "guest" SSIDs must anchor on management string.

f. 15 users per AP

g. AP ratio-4:1

h. Auto RF channel changes via configuration settings. Roaming rule consideration for extended service area (ESA), prevents interference between two overlapping APs with the same SSID. These types of APs must be configured on different channels or frequency ranges that do not overlap. This process will prevent co-channel interference.

i. DTIM=2

j. 800 APs per Mobility Group (or 8 '4404' controllers per mobility group)

k. Use DNS to 'load-balance' AP' connections between controllers in same mobility group.

l. If wireless is primary connection-'load-balance' AP' cabling connection to two different network switches

6.2 Antennae Standard

Cisco's AP1310 have both internal & external antennae while AP1242 have external antennae.

1200 AP series with multiple antennae supporting 2.4 & 5 GHz bands.

6.3 WLAN Controller Standard

The Cisco 4400 Series Wireless LAN Controllers is available in two models (4404, 4402) depending upon the number of AP's to be supported at each location. When roaming via settings on a controller for clients, the primary interest must be mobility group deployment. Mobility domains are for extended controllers ONLY.

4404 Controller Standard

* 4 front Distribution System ports (gig only). Has fiber connections but can use SFP connector if copper is required.

* Dual power supplies

* One single out-of-band management service port

* Handles to 100 AP's

4402 Controller

(2 front Distribution system ports (gig only). Has fiber connections but can use SFP connector if copper is required)

- Dual power supplies
- One single out-of –band management service port
- Handles 12, 25, and 50 AP's

Controller Standards Summary:

- **4404-100 v4.0.217.0 (supports up 100 APs)**
- **4402-12 v4.0.217.0 (supports 12, 25 or 50 APs)**
- **Ports must be hard-coded to 1000-duplex**
- **Controller's location (connection):**

:

Controllers must connect to user block aggregation router

i For sites with multiple core routers, connect each additional Controller to DIFFERENT user block aggregation router on DIFFERENT core.

ii. For sites without multiple core routers, connect each additional controller to DIFFERENT user block aggregation router.

iii For sites without aggregation routers or gig ports access switch, a Catalyst 4948 **(WS-C4948-S)** can be purchased to accommodate wireless controller.

For both 4404 and 4402, physical connections must include ports #1 & #2 in LAG (Link Aggregation) mode.

Data Site (dedicated) controllers:

1. Each location must have their own centralized WLAN controllers
2. **Two 4404-100** controllers (one in each WLAN) must be designated as failover for sites with **one** local controllers. APs connect directly to their local controller as their primary connection. For secondary & tertiary controllers-point APs to WLAN controllers.
3. **Two 4404-100 controllers** (one in each WLAN) will be designated for sites **without** any controllers. APs connect directly to these controllers as their primary, secondary and tertiary connections for failover

4. **Two 4402-12** controllers for guest access in DMZ

   4404 and 4402 controllers, "service" and "virtual" ports are not used

   3 SSIDs per controller with each SSID having independent security and QoS policy (e.g., **SSID #1 WLAN; SSID #2 QUEST-VPN; SSID #3 QUEST-PROXY**).

   8 Controllers per Mobility group

5. **Note:** There is a 24 controller's limitation per mobility group but to limit the chattiness of mobility messages between controllers belonging to same mobility group, there should be only 8 controllers per mobility group. Create new mobility group for 9th or more controllers

   Management and AP-Manger interfaces reside on same VLAN. Mainain range of encryption cipher suites with algorithms under SSLv2 or SSLv3. Maintain authentication framework with Extensible Authentication Protocol (EAP). Disable all unnecessary services that the controlled AP's are shipped with. Add controllers to WCS (Wireless Control System)for management.

VII CONTROLLER PLACEMENT

Following is a guideline for controller placements. Controller's placement depends on a few important criteria such as size, WAN latency, local resources, mobility, scalability, cost and redundancy. Four separate scenarios are defined to meet these different requirements. PA considers these four placement types ...

Single local controller

Two or more local controllers

No local controller

Guest controllers

VIII OVERVIEW FOR NETWORK & SUBNETTING

- No Multicast on wireless
- Radius ACS v3.2 or higher
- 802.11 family of specifications developed by IEEE for wireless LAN technology.
- IP Lease = 1 hour as per static IP wireless device assignments.
- **DHCP server** for non-static IP wireless devices.
- MANAGEMENT VLAN ... Each controller needs 2 IP addresses for management and AP management interfaces. Two IP addresses must be on same VLAN
- USER VLANs

6. For sites with 10 or more APs on each controller use **/24 (510 IPs) for each SSID**
7. Each SSID is on different VLAN
8. Increase subnet size if more IPs are needed later for LWAPP.
9. **Note**: For non-FW controllers, there's **no need** for quest VLANs. Guests are terminated at quest controllers. It is at guest-LWAPP controllers that IP addresses for clients are handed out. The only VLAN needed at non-FW controllers is for SSID WLAN.
10. For sites with less than 10 APs for each controller, use /26 (62 IP) for each SSID

THIS DOCUMENT IS FOR BEST PRACTICES WITH WIRELESS HARDWARE IMPLEMENTATION AGENCY-WIDE SITE DEPLOYMENTS ... NOT FOR WIRELESS DEVICE CONFIGURATION PRACTICES.

Appendix A

WLAN Best Practices Add-ons :

1. Ensure that the PA maintains an up-to-date wireless hardware inventory.
2. Identify rogue wireless devices via wireless intrusion prevention systems (IPS)
3. Enable automatic alerts on the wireless IPS
4. Perform stateful inspection of connections.
5. Augment the firewall with a wireless IPS
6. Mount AP in location that do not permit easy physical access
7. Secure handheld devices with strong passwords
8. Enable WPA and WPA2 under ENTERPRISE mode
9. Synchronize the AP's clocks to match networking equipment.
10. Manage remote physical locations of all access points which support an isolated network that needs access to PAWANET for server farms and internet access. Deploying the use of WGB (autonomous workgroup bridging) topology with IOS AP version 12.4(3G)JA.
11. Maintain cryptographic strength range from 128-bits to 256-bits with matching symmetric algorithms AES-128 to AES-256

Appendix B

Wireless Control System (WCS):

1. Single license
2. Secure "WIRELESS LOCATION APPLIANCE" with real-time client tracking & RF fingerprinting
3. Secure Windows-Based deployment as minimum, for example, windows server 2003; intel dual-core; 3.2 GHz; 4-GB RAM; 80-GB hard drive; IPS devices; IOS firewall routing; HTTP port 80; HTTPS port 443.
4. Multi-homed server (i.e., two NIC cards)
5. Secure WCS and IIS (i.e ,internet information service), installation sequence
6. Create configuration group (config. multiple controllers)
7. Secure auto provisioning with filtering
8. Secure WCS with RF modeling for heat map planning
9. Secure 15 second alarm summary refresh

10.1.5 Portable Electronic Devices (PEDs) – Cell Phones, PDAs, messaging devices, laptops and tablets.

If a device receives information via a wireless technology, and that device allows that information to be placed directly into the corporate network at the workstation level, then all perimeters and host-based security devices have been bypassed. Therefore the following procedures apply:

PEDs connected directly to a PA wired network via a hot sync connection to a workstation shall not be permitted to operate wirelessly at the same time. Wireless solutions could create backgrounds into corporate networks.

IR, Bluetooth and 802.11 peer to peer should be set to "off" as the default setting. Mobile code should be downloaded only from trusted sources over assured channels.

Anti-virus software should be on devices and workstations that are used to synchronize/transmit data, if available. Where not available on a device, you need to disable the synchronization capability or provide server or workstation based handheld anti-virus protection.

PEDs are easily lost or stolen therefore approved file system/data store encryption software should be installed.

PEDs need to be capable of being erased or overwritten to protect data. If the device is no longer needed and cannot be erased or overwritten,it must be physically destroyed.

10.1.6 Cellular and Wireless Email

Cellular and wireless email devices are subject to several vulnerabilities (e.g. interception, scanning, remote command to transmit mode, etc). Therefore the following procedures apply:

These devices are not to be allowed into an area where classified information is being discussed unless it is rendered completely inoperable.

Must have end-to-end encryption.

PC based redirectors are not allowed as it requires the PC to be active at all times only server based redirectors should be used.

Electromagnetic sensing shall be periodically performed to detect unauthorized LANs, Bluetooth transmitters etc.

10.1.7 Synchronization

Some synchronism systems will operate even if the workstation is locked and the wireless or handheld device is not registered with the sync application on the workstation. As long as the workstation is on, the user is logged on, the data application client (e.g. MS Outlook) is active, and the "hot sync" cable is attached to the workstation; any person can place a compatible wireless or handheld device in the "hot sync" cradle and download data. Therefore the following procedures apply:

"Hot sync" cable or cradle has significant security risks, therefore perform "hot sync", then remove immediately once "hot sync" operation is complete.

Secure "hot sync" cables and cradles.

Use only PA approved third party sync access control software installed on all workstations.

PA owned devices may only be synchronized with PA owned computer systems

10.1.8 Responsibilities of Technology Services Department

Monitor and provide oversight of all PA wireless activities, insure interoperability of wireless capabilities across the agency.

Develop appropriate technical standards and guidelines for secure wireless and handheld solutions.

Establish a formal coordination process to ensure protection of PA information with PA information systems employing wireless technologies.

Review and evaluate wireless technologies, products, solutions that meet PA requirements.

Identify approved monitoring mechanisms for wireless devices to ensure compliance with policy.

Periodically review approved wireless technology standards and procedures to ensure products and solutions remain compliant.

Support risk management activities associated with evaluating wireless services

Act as central coordination point and final approval authority for any exceptions to this policy.

Define or approve acceptable wireless devices, products, services and usage.

Provide immediate consultation to PA units.

10.1.9 Responsibilities of Technology Services Voice Networks Group

Adhere to wireless procedures and standards, establish procedure for reviewing and approving requests for using wireless devices to store, process, or transmit information.

Establish procedures for periodically reviewing approved wireless devices and services to ensure that the business requirement for device/service/system is still valid and meet current PA guidance.

Establish procedures for inventory and control of wireless devices and equipment.

Establish procedures and implementation plans for auditing wireless connections to the network.

Provide user training.

10.1.10 Responsibilities of Wireless and Handheld Device Users

Coordinate all requests through Technology Services Department...

Read and follow standards and guidelines.

Access information systems using only approved wireless hardware, software, solutions and connections.

Take appropriate measures to protect information, network access, passwords and equipment.

Use approved password policy and bypass automatic password saving features.

Use extreme caution when accessing PA information in open areas where non-authorized persons may see PA info (airport lounge, hotel lobby).

Protect PA equipment and information from loss or theft at all times, especially when traveling.

Keep current anti-virus software on devices.

Use appropriate Internet behavior (e.g. approved downloads).

Exercise good judgments in efficient cooperative uses of these resources and comply with current and future standards of acceptable use and conduct at all times.

Report any misuse of wireless devices, services or systems to management.

10.2 Paging Device Policy And Procedures

10.2.1 Policy

The Port Authority obtains its paging services under governmental contracts. All orders for paging service or equipment must be placed under these contracts. If the contract service provider cannot meet the paging requirements, a memorandum requesting approval to obtain paging service outside of the contracts must be sent to the Chief Technology Officer. If approved, the requesting department is responsible for obtaining necessary authorizations and preparing a contract and/or purchase order.

10.2.2 Procedures

Specific models of paging devices and service pricing plans have been selected by Technology Services Networks Division, E-Mail Group, as agency standard models and plans, and will be used for all staff. The E-Mail Group will review all requests for alternate models or plans to ensure that the request is appropriate for the work need indicated.

All requests for paging devices should be sent via e-mail to Marion Resnick, E-Mail Group, mresnick@panynj.gov using the unified Wireless Device Approval form available by clicking on the link below:

Wireless Device Approval Form PA 3943

The request must be approved by the department director. Concurrence via e-mail is acceptable. Once the request form is reviewed, it will be forwarded to the service provider who will deliver the paging device directly to the requestor.

All service and equipment problems should be reported to Marion Resnick, E-Mail Group, ONEMAD 152TSD (for PA mail) or call 212-435-3251.

The service provider will send all invoices directly to the customer department. Each customer department will be responsible for reviewing, approving and processing the payment of the invoices. Each department is required to maintain an inventory list of assigned paging devices for use in verifying the invoice. Inconsistencies should be reported to the service provider for resolution.

Responsibility for keeping accounts current with the service provider will rest with the customer department. Prompt payment of invoices is critical as delinquency may result in termination of service.

Annually, the E-Mail Group will send each department director and their respective Chief, a listing of assigned paging devices for review. Each department must review the list, perform a physical inventory and reconcile any discrepancies. The reviewed inventory list must be returned to the E-Mail Group for update of the master list.

When the use of a paging device is no longer required, or upon termination of employment, the paging device is to be returned by the department to the service provider, and the completed Pager Change Form requesting the disconnection (available on ENET) is sent to Marion Resnick, the E-Mail Group. Please click on the link below for the form:

Pager Change Form

Staff below director level are allowed only one of the following devices, cellular phone, Nextel radio/phone or pager, unless approved in writing by the department director. BlackBerry devices are excluded from this restriction.

10.3 Cellular And Nextel Phone & Wireless Modem Policy And Procedures

10.3.1 Policy

The Port Authority obtains cellular and Nextel radio/cellular service under governmental contracts. All orders for cellular service or equipment must be placed under these contracts. If the contract service provider cannot meet the requirements, a

memorandum requesting approval to obtain cellular service outside of the contracts must be sent to the Chief Technology Officer.

If approved, the requesting department is responsible for obtaining necessary authorizations and preparing a contract and/or purchase order.

10.3.2 Procedures

Specific models of cellular phones, wireless modems and service pricing plans have been selected by Technology Services, Voice Networks/Wireless, as agency standard models and plans and will be used for all staff. Voice Networks/Wireless will review all requests for alternate models or plans to ensure the model or plan requested is appropriate for the work need indicated.

All requests for cellular telephones, wireless modems and Nextel radio/cellular phones should be sent to Voice Networks/Wireless, One Madison Avenue, 7th floor, New York, NY, 10010, (212-435-8227 fax 212-435-3363), using PA form 3943, available online on Enet. The requesting director is responsible for determining whether there is sufficient business reason to authorize use of a cellular phone or wireless modem.

The request will be reviewed to ensure that a cellular telephone, wireless modem or Nextel radio/cellular phone is the best solution for the department's communications needs and that it meets the above criteria. Nextel should be considered only where substantial use of radio service is needed. Once approved the order will be sent to the contractor.

Once the order has been processed the contractor will ship the cellular telephone, wireless modem or Nextel radio/cellular phone to the customer.

When required, the installation of any cellular or Nextel telephone equipment in a PA vehicle, can be requested from Voice Networks/Wireless, and will be coordinated with the Central Automotive Division. Staff is advised that using a cellular or Nextel radio/cellular telephone while driving is dangerous and is restricted by law in both the states of New York and New Jersey.

Voice Networks/Wireless will arrange with the cellular or Nextel network service provider for the initial telephone number or wireless data service. Any subsequent number changes and/or disconnects will be processed by Voice Networks/Wireless upon receipt of a written request.

All charges for Verizon Wireless, ATT Wireless cellular service and Nextel radio/cellular service- including usage and equipment- are included on a consolidated invoice, which is processed under SAP by Voice Networks/Wireless. Courtesy statements are sent directly to the customer for review. Employees are responsible for reimbursement to the Port Authority for non-business calls (See AP 30-4.01, Non-Work Related Telephone Charges).

Annually, Voice Networks/Wireless sends each department director and their respective chief, a listing of assigned cellular, Nextel radio/cellular phones and modems for review (this listing can be provided to departments more frequently if required). Each department must review the list, perform a physical inventory and reconcile any discrepancies. The reviewed inventory list must be returned to Voice Networks/Wireless for update of the master list.

All service and equipment problems should be reported to Voice Networks/Wireless, One Madison Avenue, 7th floor, New York, NY 10010, 212.435.8227.

Staff below director level is allowed only one of the following devices, cellular phone, Nextel radio/phone or pager, unless approved in writing by the department director including specific business need for multiple devices. Blackberry devices are excluded from this restriction.

When the use of a cellular telephone, Nextel radio/cellular phone or wireless modem is no longer required, or upon termination of employment, the department must notify Voice Networks/Wireless which will issue the disconnect notice. The department is responsible for proper disposition of the cellular/radio equipment.

In accordance with PA environmental policies, all wireless equipment that is no longer needed must be returned to the vendor for appropriate handling and recycling.

All wireless phones and accessories that are old or not being used remain the property of the owner's department. Equipment in very good condition may be kept as spares. If the device is not needed or is not in good condition, select the appropriate procedure listed below for disposal. Contact Chuck Levinson via email or at 212-435-8227 to discuss disposal. Do **not** send devices to the Technology Services Department, unless you have received approval to do so.

For large numbers of wireless phones, fill out a Property Disposition Report, noting that you will be sending the unused phones back to the vendor for recycling. PA form 2331A -Property Disposition Report is available on eNet.

Send the Property Disposition Report form only to Margaret D'Emic in Procurement.

Nextel equipment must be sent to Michael Mistretta, Nextel, 59 Maiden Lane, 21st Floor, New York, NY 10038. Send only when you have a full box of phones. Accessories may also be returned to the above location, but must be packaged separately.

Verizon Wireless and other cellular equipment must be sent to a Verizon Wireless Warehouse, using labels provided by Voice Networks/Wireless. Contact Chuck Levinson, Technology Services Department, One Madison Ave. 7th floor, via email at clevinso@panynj.gov or call 212-435-8227.

Please include a note listing the contents (number of phones, etc.), indicate they came from our agency and the date and send a copy to Chuck Levinson, Technology Services Department, One Madison Ave. 7th floor.

Users should delete all stored numbers, names, caller ID lists and messages prior to returning equipment to the vendors. Use the phone menu or check the operating manual for instructions on how to do a "Master Clear" or "Reset" or "Erase". These are usually found in the "security" section and require the use of an access code, which is usually set to all zeros.

We suggest administrators verify that all stored information is erased on receipt of the equipment since it may be hard to do so after they are collected.

Assistance is also available by contacting the vendors' customer service support lines at the numbers listed below:

Sprint/Nextel: 800-390-7545

Verizon Wireless: 800-922-0204.

10.4 Technology Services Personal Digital Assistant (PDA) Policy

10.4.1 Introduction

Personal Digital Assistants (PDAs) are a class of handheld computers that currently offer limited functionality with compact size and portability. PDAs are designed to replace the paper organizer; functionality typically includes maintaining a date book, address list, to-do lists, email, etc. Additional functionality such as Word and Excel are already included in many PDAs, with further enhancements predicted.

In order to better serve the PA, and to limit the expense of supporting a wide variety of PDA hardware and software, Technology Services will support the use of the Windows based devices.

With a PDA, a user can maintain their calendar, address book, to-do list, and e-mail on a platform that is very portable and easy to use. Integration with Outlook makes it possible for users to keep identical, synchronized copies of data on both the desktop application and the PDA.

Any questions related to this policy should be directed to the Customer Support Desk at 212-435-7469.

10.4.2 Hardware – Hyper Link

Specific manufacturers listed below and other models using the current Windows Pocket PC 2002 or more recent versions of Windows operating system are supported.

Compaq/HP

The list of supported hardware will be updated from time to time to reflect current standards.

10.4.3 Software

All versions of the Windows Pocket PC 2002 (Operating System) or more recent Windows versions are supported.

Microsoft ActiveSync

The list of supported software will be updated from time to time to reflect current standards.

Any software found to interfere with normal operation must be uninstalled in order to receive support from Technology Services.

10.4.4 Support

Support for PDA hardware and software is provided by Technology Services through the Customer Support Desk. TSD will support the physical hardware connection (PDA cradle to PC) and software to support this connection. No software can be added to company owned PDA devices without TSD's assistance and director approval.

10.4.5 Training

Training will be available covering basic PDA use and integration with Outlook at the time of installation of the equipment. Training classes for the PDA units may be provided in the future depending on user demands.

10.4.6 Acquisition

The PA will purchase PDA units for employees with a business need for the PDA device. Employees are responsible for obtaining management approval. TSD also recommends that a protective case (preferably a zippered case) be purchased to reduce damage to the units.

Since the PA owns the device, if an employee leaves the PA the device is returned to the director's office of their department.

10.4.7 Criteria To Qualify For A PDA Device

It is recommended that the purchase of PDA devices be limited to employees who:

Have heavy meeting schedules

Travel frequently

Do not have access to their desktop computers for at least two entire workdays 12 hours per week

PDA requests must be approved by a director or above. After a director grants approval, the unit will be ordered and installed by Technology Services personnel.

10.4.8 Personal Acquisition

Employees, who purchase their own PDA devices, will not be allowed to connect to the PA corporate network or equipment, unless approved by Technology Services.

Customer Support Desk personnel will support all PA owned and authorized PDA devices.

10.4.9 Breakage And Loss

Be aware that the touch-sensitive screen used on a PDA device is very fragile. Dropping a PDA device from the height of a desktop, or applying too much pressure on the screen itself, often results in breakage of the glass. Once this happens, the PDA device is unusable. If a PDA screen is broken, it will be up to the user department to justify the cost of a replacement unit.

If a PDA device is lost, the employee is responsible for replacing it. As with all PA equipment, PDAs should be used for business purposes only.

10.4.10 Data Security Considerations

Since in most cases the data residing on a PDA device is not encrypted or password-protected, data can be easily browsed by anyone having possession of the device. Users should carefully consider what type of information they store on their PDA. Extreme caution should be taken when using company confidential data on the PDA units.

At the present time, Technology Services is researching options for encrypting PDA data using a third-party application. Until a solution is found, great care should be taken to ensure that important or confidential information doesn't end up in the wrong hands.

10.4.11 Data Backup

Though it doesn't happen often, it is possible to lose, damage or duplicate the data that resides in the PDA and PC applications. Technology Services will provide assistance in attempting to recover files or data from data corruption.

10.4.12 Personal Digital Assistant (PDA) Policy

Instructions:

Send a copy of this completed form to Technology Services.

I have read, and agree to abide by, the terms of the Technology Services Personal Digital Assistant Policy.

Signature _____

Printed Name _____

Date _____

Approved By:

Director _____

Date _____

10.5 BlackBerry Device Policy & Procedure

The Port Authority provides corporate wireless e-mail services using the BlackBerry device from RIM.

To obtain a BlackBerry, you must have the approval of the department director using the Wireless Device Approval form PA 3943 which is available on eNet or by using the link below. It must be completed in its entirety including the appropriate account code.

The BlackBerry is a palm-sized device designed to synchronize with Outlook and other e-mail systems. The monthly cost for BlackBerry data service is approximately $41 plus fees. Voice service through Verizon costs an additional $30 per month. If radio service is required through Nextel, the cost would be $40 for the voice/radio service. With a BlackBerry device, one can read, compose and respond to e-mail messages and meeting requests, which are transmitted through the Port Authority's E-Mail System. The BlackBerry contains the user's synchronized Outlook "Contacts" address book, Outlook Calendar, memo pad and task list as well as a calculator and an Internet browser.

Forward the completed form to an authorized approver for their concurrence. He or she will then forward it via e-mail to Marion Resnick, Technology Services Department. If you have any questions regarding a BlackBerry device, please contact Marion Resnick at 212-435-3251.

Wireless Device Approval Form PA 3943

For information about combined BlackBerry data and cell phone devices, see section 10.6 below.

10.6 BlackBerry Guidelines

10.6.1 Introduction

BlackBerry devices (data only or combined data (e-mail) & voice) are available from most wireless carriers in the Port District. Combined BlackBerry devices are designed to replace stand-alone cellular telephones and stand-alone BlackBerry data devices and they operate on the same wireless network as a stand-alone cellular telephone from the same carrier.

10.6.2 Recommendation for Essential Staff and First Responders

Technology Services does not recommend use of the BlackBerry device combining e-mail and voice capabilities for essential staff or first responders as the device becomes a single point of failure for both modes of communications. The hybrid device relies on a single network for service connection, and in an emergency, this network could be overcrowded or otherwise unavailable, resulting in the loss of both voice and e-mail service.

10.6.3 Support

Support for BlackBerry devices is provided by Technology Services through the Customer Support Desk at 212-435-7469. The E-Mail Group provides additional support as needed.

10.6.4 Breakage And Loss

Be aware that the screen used on a BlackBerry device is very fragile. Dropping a device from the height of a desktop can result in breakage. It is also sensitive to water damage. Once this happens, the device is likely to be unusable. Broken, lost or stolen devices should be reported to the Customer Support Desk at 212-435-7469, who will notify the appropriate staff for further action.

As with all PA equipment, BlackBerry devices should be used for business purposes only.

10.6.5 Data Security Considerations

Data residing on a BlackBerry device can be easily browsed by anyone having possession of the device. Users should activate the password security available on the device, and carefully consider what type of information they store on their devices. Extreme caution should be taken when using company confidential data on the devices.

10.6.6 Data Backup

Though it doesn't happen often, it is possible to lose, damage or corrupt the data that resides on the BlackBerry device. There are data backup features on the PC utilizing the BlackBerry Desktop Manager software. We recommend setting the advanced automatic backup to 7 days with the backup of all device application data. In the event of a lost or broken device, this backup may be used to recover lost data.

Appendices

Appendix 2 -- Business Resumption Plan Document Format

I. PURPOSE

Goals and objectives of plan

Benefits obtained if plan properly implemented

II. SCOPE OF PLAN

Planning assumptions

Facilities and resources included in plan

III. NOMENCLATURE

Recovery terms

Definitions and acronyms

IV. DISASTER SEVERITY DEFINITION

Define level of potential disaster based on impact to critical functions. Explain what degree of operational disruption would constitute each level of disaster:

catastrophic

serious

major

limited

V. OPERATIONS RECOVERY PROCEDURES

(Procedures for recovering services)

12. Indicate time frames in which essential operational/business functions must be resumed.

13. Specify sequence of operations recovery events and individuals responsible for activity. Note any specific activities required for particular levels of disaster severity. For example:

Notifications

Preliminary evaluation

Activate operations recovery personnel

Coordinate with emergency personnel

Evaluate recovery options and issue directive which details:

Assigned tasks

Project schedule/time frame

Coordination required

Identify relocation activities, if required

External/internal status updates

14. Identify items required for backup of critical functions. For example:

alternate work site

hardware/software

Personal computers

Necessary software packages

Documentation

Peripherals (printers, modems, etc.)

Databases

Emergency equipment

Communications

Transportation

Supplies

Security

Operations and procedures manuals

VI. OFFICE/FACILITY BUSINESS SITE RESTORATION PROCEDURES

(Procedures for restoring physical facilities)

identify restoration responsibilities

assess damage

develop restoration plan/time frames

VII. BRP UPDATE PROCEDURES

responsibility for updating and communicating BRP changes

frequency of review/update

Appendix 3 -- Communication Rooms/Closets Standards

SPACE

All data communication rooms must be designed with required and estimated space to meet immediate requirements, as well as, future growth..

ENVIRONMENTAL

The following conditions must be met:

a) Doorways/Entrances must be designed to support at least the minimum space requirements of 90"Hx72" Wx60" D.

b) The room's cooling capabilities must be sufficient to support the heat dissipation requirements for the equipment. This requirement will be measured in minimum and maximum BTUs powered by AC-powered systems. Equipment specs will be supplied by TSD upon request.

c) Backup UPS systems are necessary to avoid equipment damage in case of site power failure.

d) Telco demarcs must be located in a central location with sufficient space to house Telco termination equipment.

e) The room should be designed with the appropriate fire safety regulations such as a FM200.

f) Cables trays must also be installed in the communications room ceiling where appropriate, to support the routing of data communications and Telco cables.

g) Basic 19" W/72" H cabinets or racks must be installed to house communications equipment such as: routers, switches, hubs, DSUs/CSUs and monitors.

h) To create more wall space the use of wall mount racks can be installed. Appropriate sized plywood must be installed prior to mounting racks.

i) Category 5e cable must be terminated in wall/rack mounted patch panel.

j) Fiber patch panel must be installed in fiber IDF panel with SC female interface.

k) The fiber must be neatly tie wrapped and enclosed in flexible inner-duct.

l) Telephone access must be installed in the appropriate location to provide for basic trouble-shooting and vendor support.

m) All communications equipment and cabinets must have ample room for easy access and proper ventilation.

Appendix 4 -- Cabling

a) Teflon-coated cables should be installed per fire code regulations.

b) Overhead cable trays and drop post must be installed for cable routing.

c) Cabling scheme must be used to label and identify all cables. All cables must be neatly tie-wrapped.

Appendix 5 -- Port Authority Unified Wiring Plan

Original: 01/90
8th Revision: 03/02

To satisfy existing and future voice and data communications requirements, while minimizing the need for wiring changes and additions, the Port Authority has adopted the following lateral wiring specifications for all workstations being constructed. This plan is applicable to all PA locations, except when specifically noted.

LATERAL CABLE:

Voice and data telecommunications requirements for each workstation will be provided by a combination of three individual cables, installed between the workstation and the serving telephone closet / intermediate distribution frame (IDF), in a "home run" configuration. All cabling installed will be of plenum type, fire retardant (FEP) rated.

Cable specifications:

(3) Cables capable of supporting Category 5e capabilities as outlined in the TIA/EIA-568-B.2 standard. Specifically:

Gauge: 24 AWG

Pair Size: 4

Insulation: Plenum, fire code rating (FEP)

Cable allocations will be as following:

Cable #1: Voice**

Cable #2: Data

Cable #3: Data

- *100.0MHz is the speed the PA wants to deliver to the desktop.
- **Cable #1 is to be split in the workstation to support 2 telephones.

Technical specs for the Cat 5e cable is as follows.

TECHNICAL DATA--ELECTRICAL				
	Horizontal		Patch	
Frequency MHz	Attenuation dB/100 m max.	Next dB min.	Attenuation dB/100 m max.	Next dB min.
1	2	62.3	2.4	62.3
4	4.1	53.2	4.9	53.2

10	6.5	47.3	7.8	47.3
16	8.2	44.2	9.8	44.2
20	9.3	42.7	11.1	42.7
31.25	11.7	39.8	14.1	39.8
62.5	17	34.3	20.4	34.3
100	22	32.3	26.4	32.3

TECHNICAL DATA--PHYSICAL			
	CMR	CMP	CM (Patch)*
Conductor diameter-in. (mm)	.020 (0.52)	020 (0.52)	024 (0.61)
Cable diameter-in. (mm)	.195 (5.0)	165 (4.2)	215 (5.5)
Nominal cable weight-lb./kft. (kg/km)	21 (31)	21 (31)	23 (34.2)
Max. installation tension-lb. (N)	25 (110)	25 (110)	25 (110)
Min. bend radius-in. (mm)	1.0 (25.4)	1.0 (25.4)	1.0 (25.4)
* Patch cables utilize stranded tinned copper conductors			

PARAMETRIC MEASUREMENTS		
	Horizontal	Patch
Mutual Capacitance	4.6 nF/100 m nom.	5.6 nF/100 m nom.
DC resistance	9.38 Ohms/100 m Max.	9.09 Ohms/100 m max.
Skew	45 ns/100 m max.	45 ns/100 m max.
Velocity of	72% nom. Non Plenum	72% nom.
Propagation	72% nom. Plenum	
Input Impedance	100 + 15% 0.7772-100 MHz	100 + 15% 0.772-100MHz
	ISO/IEC 11801	

COLOR CODE			TEMPERATURE RATING	
Pair 1	White/Blue	Blue	Installation	0 degrees C to +50 degrees C
Pair 2	White/Orange	Orange	Operation	-10 degrees C to +60 degrees C
Pair 3	White/Green	Green		
Pair 4	White/Brown	Brown		

Appendix 6 -- Telephone Closet / IDF Termination Blocks

Lateral Data cabling serving each workstation will be terminated on a CAT5e patch panel (RJ45 face, 110 punch rear) in the telephone closet. For phone service, termination is to be on 110 blocks in telephone closet, allowing access to the telephone riser. For data, a patch cord is installed between patch panel and IT device. The patch panel can be mounted on the wall with a wall mount kit or in a rack if one is needed and should be appropriately numbered with the workstation number. The patch panel must be capable of supporting Category 5e the TIA/EIA-568-B.2 standard. The patch panel shall have a swing away faceplate or rack mountable.

NOTE: The Category 5e patch panel should be equivalent to the AMP SL series 110Connect Category 5e patch panel. The number of ports may vary.

Each workstation will be assigned a unique station identification number.

Appendix 7 -- Workstation Jacks

Workstations will be equipped with various components of the AMP Communications Outlet system (AMP equivalent can be used with TSD approval). Each workstation will be installed with (1) double-gang jack housing box and matching face plate, capable of securely mounting three Category 5e cables and four modular data connectors, maintaining the integrity of category 5e capabilities as outlined in the TIA/EIA-568-B.2 standard. All workstation jacks will be wired in accordance with the TIA/EIA-568-B.2 standard. All modular jacks are to be appropriately labeled.

Appendix 8 -- Standard Switches Inside the Department

Any switches in the following Cisco series are acceptable (Vendors will consult with the Technology Services Department (TSD) to determine the appropriate switch configuration at the time of proposal submission):

Cisco 3000 series – low capacity

Cisco 4000 series – medium capacity

Cisco 6000 series – high capacity

Cisco 4507 series – high capacity – New

Appendix 9 -- Desktop and Lateral Cable Identification Management

WORKSTATION AND LATERAL CABLE IDENTIFICATION/MANAGEMENT (Facility)

All lateral cabling installed to workstations at the Port Authority Facilities must be designated in accordance with the Port Authority's workstation and lateral cable identification code: This code consists of two elements, as follows:

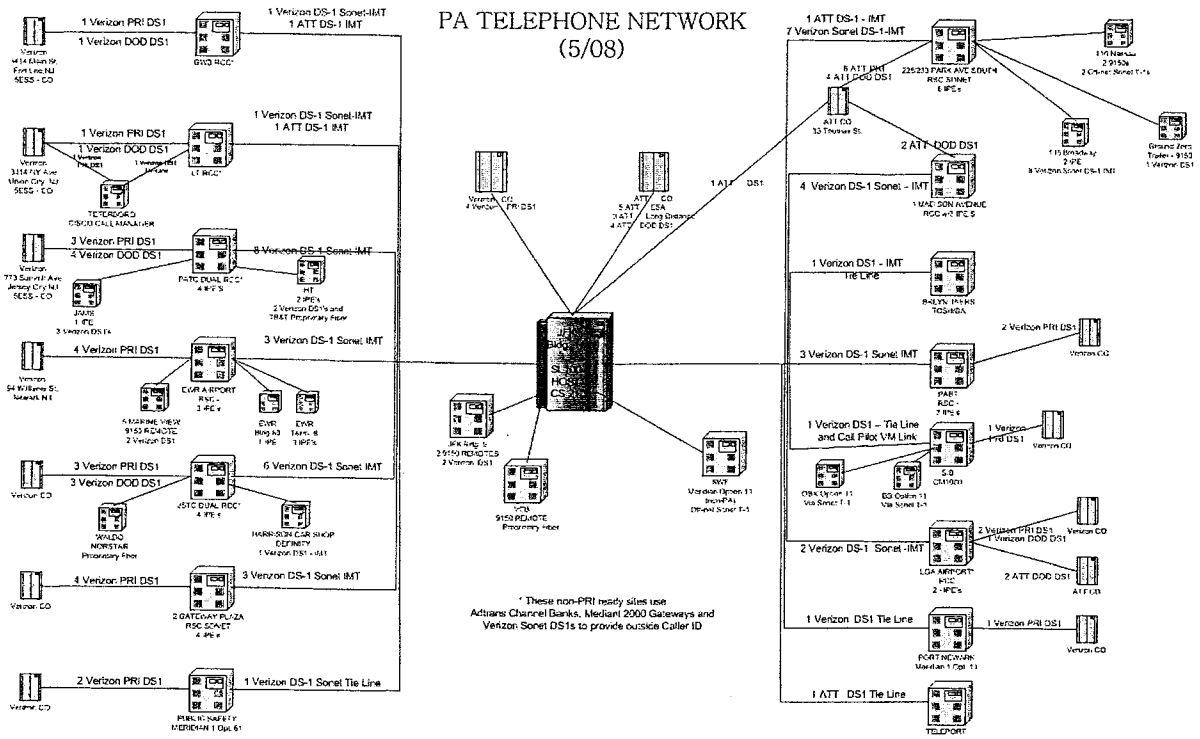
1 - Room number or department name (acronyms are acceptable).

2 - Workstations (3 numeric digits)

The cable identification code for Workstation 10 in room 3801 at LGA CTB is 3801-010.

The cable identification code for Workstation 15 in PA Automotive shop is Auto-015

Appendix 10 – PA TELEPHONE NETWORK 5/08



Appendix 11 -- Fiber Optic Specifications for Network Services - PAWANET

General Scope of Work

1. Conduct a walk thru based on the specific Scope of Work for the job in question.
2. Note that all diagrams and or sketches that may be provided are approximates and not to scale.
3. All fiber optic cable is to be installed in rigid conduit or, where applicable, in plenum rated flexible inner duct.
4. Contractor shall furnish and install fiber optic cable as designated in the specific Scope of Work.
5. Fiber optic cable type will be loose tube, gel filled, with aramid yarn water block:
   a. Multimode Fiber – **50/125*** micron diameter. Manufacturer of cable TBD
6. Fiber optic cable attenuation from the factory, before installation, shall not exceed:
   a. For multimode – 3.5 db per km @ 850nm / 1.0 db per km @ 1300nm
7. All fiber optic cable is to be labeled on each end and at any junction or patch panel with, 28 gauge, 2" wide embossed with ¼" high letters. The labels are to be fastened to the fiber optic cable using sealed wrap around labels or pliable Velcro ties.
8. Fiber optic cable shall be installed in accordance with the manufacturer's specifications. Any portion of the cable damaged during installation will be repaired or replace by the contractor without any additional cost to the Port Authority of New York New Jersey.

Fiber Optic Terminations

1. Fiber optic terminations will use **SC**** connectors unless otherwise specified in the Scope of Work.
2. Fiber optic terminations shall not yield more than 1db per mated (at the bulkhead) connector.

Fiber Optic Testing

1. Fiber optic testing shall be performed by the contractor and certified fiber optic technicians.

Fiber optic technicians will be prepared to complete test procedures with the following equipment:

- Source and power meter testing to provide optical loss measurements.

- Reference test cables and mating adapters that match the cables to be tested.
- Cleaning materials – lint free cleaning wipes and pure alcohol.
- OTDR test set with the proper launch cables and adapter types.

2. Fiber optic technicians will perform OTDR test on all terminated fibers unless otherwise noted in the Scope of Work.
3. Fiber optic test results shall be recorded, and reports provided to the PA in hardcopy and via a readable txt file (PDF or RTF is acceptable).

*50/125 micron fiber has been chosen over 62.5/125 micron fiber by Network Services:

1. Greater speeds achieved. 62.5/125 fiber will deliver 1 gigabit per second (Gbps). 50/125 fiber will deliver up 10 Gbps. This allows for equipment upgradeability.
2. Greater distances. 62.5/125 fiber will go up to 275 meters from source. 50/125 will achieve up to 550 meters from source. We can cover greater distances in an installation without having to go to the more expensive single mode fiber installation.

SC connectors have been chosen over **ST connectors by Network Services due to the fact that we utilize Cisco equipment, which come furnished with **SC** connectors on their fiber interface blades. It is more cost effective to use the standard **SC-SC** patch cable with Cisco equipment than to add the additional cost of having hybrid **SC-ST** cables made. **SC** connectors are also easier to work with and use less space in an installation.

Appendix 12 -- Public Telephone Ordering Guidelines

Technology Services (TSD) staff responsible for the management of the permit for public telephone service are available to answer any questions and provide direction for any matter relating to public telephones. The names and contact numbers are listed below

General Guidelines

All public telephone requests – that is both coin and non coin in any Port Authority space or any area of the tenant space – both "public" and "club" locations should be coordinated through Marion Resnick 212-435-3251 for sites in both New York and New Jersey.

Process

When the Facility, Property Manager, tenant or their representative (e.g. designer, architect, general contractor) has a public telephone requirement, they contact Marion Resnick of Technology Services. She will review the request and coordinate with GTL-the public telephone permittee and the facility or the tenant.

Facility:	TSD
Contact:	Marion Resnick
Telephone #:	212-435-3251
Fax #:	212-435-3363

Facility:	GTL
Contact:	Lou Pasquarella
Telephone #:	732-566-7554
Fax #:	732-566-7449

Facility:	GTL Operations
Contact:	Ben Wurzel
Telephone #:	718-289-9775
Fax #:	718-289-9733

Facility:	GTL Operations
Contact:	Henry Penna
Telephone #:	718-289-9734
Fax #:	718-289-9733

Appendix 13 -- PAWANET Services Connection Policy

PAWANET SERVICES & REQUIREMENTS

POLICY:

All communications for access to the Port Authority's Agency wide resources will be conducted over the centrally managed and administered Port Authority Wide Area Network (PAWANET). This includes but is not limited to; access to SAP, People Soft, Outlook, Internet and file and print servers. In addition, any and all facility based or departmental systems that require email, Internet access, remote access or interdepartmental communications MUST use the Agency's Network, PAWANET.

BACKGROUND

The Port Authority has made and continues to make significant investments in a centralized communications network, PAWANET, which is designed around current Technology Industry best practices and employs well documented Standards and Guidelines to ensure continued good service and interoperability through future growth and changes. PAWANET is designed to accommodate all of the Agency's current and future services in a highly secure and cost effective fashion.

PAWANET offers high performance network architecture that Departmental Business Systems owners can use to provide access to applications within the Agency's network and also to outside users/business partners and organizations. Utilizing PAWANET provides the following services and benefits:

- Business Benefits of PAWANET
    - High network availability
    - Data availability
    - Network and application design and review
    - Business continuity planning and services
    - Remote Access methods for outside personnel
    - Messaging services
    - Hosting services for web enabled applications
    - Monitoring, logging and auditing services
    - Systems administration services
    - Software support services

- Professional staff organized for appropriate separation of duties
- Server and client maintenance services
- Flexibility for growth, enhanced applications and organizational change
- Capacity planning services (network, applications)
- 7x24 Help Desk
- Local Desktop Support

- Security Benefits of PAWANET
  - Centrally managed security architecture
  - Cyber security technology
    - Firewalls
    - Intrusion detection
    - Virus protection
    - Local and Wide Area Network security
    - Software patching and vulnerability detection
    - Spyware detection
    - Spam protection
    - Encryption technologies
  - Strong user authentication and identity management services
    - Single Sign-On
    - Role-Based authentication
    - Password Synchronization
    - User directory integration
  - Secure physical infrastructure
  - Monitoring, logging and auditing services

This architecture has been deployed because most application business owners cannot provide the equivalent level of security and services on an individual application basis.

SYSTEMS WHICH BENEFIT FROM A SINGLE NETWORK

All Business owners can utilize the services discussed above but Business Applications with the following characteristics derive significant benefits from a single network. Systems which:

- Are located in multiple facilities
- Can be configured for high-availability/redundancy
- Have End Users who are currently or expected in the future to be located in any of the PA facilities (examples would include users with viewing and reporting capabilities)
- Require Consolidated/Agency wide reporting
- Require significant physical security/backups of data
- Are likely to increase in size, number of users and have a number of facilities over time
- Require secure interfaces with outside organizations via dedicated lines or Internet connectivity
- Will be connecting to multiple outside parties via dedicated communication links or Internet connectivity (ex. Transcom, EZ-Pass)
- Are likely to have large increases in transmission requirements over time
- Require monitoring/alerting for system maintenance and operating personnel
- Are likely to benefit from automated software distribution and updating (ex. client machines which require software upgrades and are not web based)
- Are capable of running on a shared/consolidated server environment (application, database, web server)
- Require significant remote management from non-local vendors

COMPLIANCE PROCESS

Before connecting devices to PAWANET, Business Systems owners and end users must ensure that such devices are in compliance with the PA Standards and Guidelines found on eNet.

PAWANET "Rules of Connections"

1. Users must submit a Service Request Form to the Technology Services Department (TSD for connecting standard / authorized end-point devices such as desktops, notebooks, workstations, and printers.

2. Users must submit a Design Request Form to TSD for servers or devices designed to provide file & print, applications (including Web, Video), software or other types of access services.

3. Users may not extend or modify a secured network in any way by installing devices such as repeaters, bridges, switches, routers, gateways, wireless access points, or permanent hubs.

4. Users must use network services provided by TSD and not attempt to provision network services such as IP (Internet Protocol) address assignment (i.e. DHCP (Dynamic Host Communications Protocol) servers), DNS (Domain Naming System), or other IT (Information Technology) infrastructure and management services.

5. Any piece of equipment that is found in violation of this policy may be subject to immediate disconnection from the network and the owner/operator may be held liable for an infraction of the Computing Resource Policy.

Appendix 14 -- PAWANET Services Summary

Service Name

High availability network services

High bandwidth capacity for current and future applications

Route Diversification with multiple high-speed data communications between facilities

Real time Network monitoring and alerting - 7x24 - from network devices to end-point devices

Capacity planning

Network equipment purchasing and maintenance to agreed upon SLA (4 hour)

Network utilization reporting

High Availability Internet Services through multiple service provided on an "on-demand" basis

Dual Network Operations Centers in New York and New Jersey

Redundant electricity (Redundant N+1 design of uninterruptible power supplies)

Redundant stand-by generator power supplies, in the event of a power failure from commercial power

Data availability

High availability and capacity Data with cross facility data replication

File and print services to provide secure centralized storage of client machine data

Secure physical infrastructure

State of the Industry Data Center which provides 24x7 facility security, staffing, environmental controls

Fire Detection and Prevention Systems

Fire Suppression Systems

Video Surveillance (Indoor and Outdoor)

Environmental monitoring (humidity, temperature, smoke, fire)

Network equipment in locked cabinets with tamper switches

Application servers in locked cabinets with tamper switches

Proximity card access control

Network and application design and review

Pre-Requirements Design Assistance

Requirements and Selection Assistance

Pre-Implementation Review Services

Post-Implementation Review Services

Business continuity planning and services

Backup/Restore Services and Storage Area Networks for high capacity data storage ensuring enterprise-wide data and application availability at lower cost

Offsite Disaster Recovery services are available utilizing our existing relationship with an outsourced leader in disaster recovery

Battery Backup (UPS)

Centrally managed security services and architectures

Multi Layered Security Architecture - Security not compromised by single vulnerability

DMZ environment separating internet facing services from back office servers

Firewall and access control with separation of duties

Intrusion Detection (Network Based)

Intrusion Detection (Host based)

Virus Protection (Server and Client) with expedited and automated protection

Virus Protection (E-Mail) through Outsourced E-mail services and 3rd Party Virus Filtering Services

Spam Protection (E-Mail) through Outsourced E-mail services and 3rd Party Spam Filtering Services

Centralized auditing and logging of server/OS activity

Industry recognized operating system and application lock downs

OS Vulnerability testing

Intra-agency Encryption (VPN) services

Vulnerability scanning of network, servers and clients

Automated Patch management for Servers

Automated Patch management for client machines

Layered security methodology and technology which protects Agency assets and which relies on no single security control to defend against emerging threats

Secure encrypted transmissions to outside organizations

Network Time Stamp Services From National Atomic Time-Clocks

Coordinated and Timely responses to alerts, intrusion incidents

Directory Names Services (DNS) - Within PA Network

Network Security - Network Address Translation for masking the internal IP address from the Internet

Network Security - Access lists configured on all edge routers

Network Security - Project specific VLANs can be implemented

Strong user authentication and identity management services

Identity Management - Automated and expedited User Provisioning/Revocation of User Rights

Single sign-on Services

Directory services, integration and synchronization between Active Directory and Novell and a unified identity management repository

Password synchronization

Identity and Role Based Access Control

Multi-form factor authentication solutions (tokens, smart card, biometric) for high security, auditing and reporting

Remote access methods for outside personnel

Unified secure encrypted web portal access via I-Chain architecture

Remote access and secure support and tools via Citrix/VPN or other thin client methods

Messaging services

E-mail services and alert routing via corporate e-mail system and SNMP servers

Blackberry and other paging services available

Hosting Services for Web Enabled Applications

Intranet (E-Net) enabled applications

Extranet (I-Chain) enabled applications

Internet hosted environment through Outside Vendor

Domain name registration and management for the Internet

Monitoring, logging and auditing Services

Server monitoring with alert message creation

E-mail forwarding services to end users, systems administrators and outside parties

Centralized auditing control, logging and reporting services

Asset management and reporting

Systems Administration Services

Outsourced services which ensure SA availability at all times

Servers and desktops configured and maintained following industry best practices and following PA Standards and Guidelines and other recognized best practices methodologies

Servers configured with self diagnostic and automated reporting tools

All servers are properly secured and managed

Software Support Services

Hardware and Software Inventory services

Automated software upgrade and maintenance

Automated patch management services for operating system and application patches

In-depth and broad knowledge in major software products

Database Support and Security Services

Professional staff organized for appropriate separation of duties

Trained professionals who are expert in each area of network services

7x24 Help Desk support with agreed to Service Levels

Operational responsibility for networks separate from computer operations

Server and client maintenance services

Consolidated database servers

Consolidated web servers

Consolidated application servers

Flexibility for growth, enhanced applications and organizational change

Network Design Services - to optimize application performance and minimize Total Cost of Ownership to Business System Owner

Existing PAWANET presence at all facilities allows new systems to be attached at a lower incremental cost.

Total Number of Services Available = 91

General Index

Administrator, 18, 19, 23, 27, 28, 29, 31, 33, 34, 36, 46, 50, 53, 55
AT&T, 9, 11, 56, 59, 70
ATM Cisco View, 13
ATMs, 9, 11, 12, 13, 78
Browsers, 41
Business Resumption Plan, 26, 29, 79
  Document Format, 79
Cabling, 14, 25, 29, 82
Change Management, 26, 27
Cisco, 9, 12, 13, 21, 64, 85
Cisco Strataview Plus, 13
Cisco Works, 13
Closed Circuit TV, 9, 11, 61
ColdFusion, 42
Communication Room, 29, 81
Computer Aided Design, 25
Computing Resources Policy, 37, 51
Comsoft Telephone Reports, 58
Databases, 25, 42, 55, 80
Dreamweaver, 42
Drive Mappings, 16, 47
Electrical Requirements
  Telecommunications, 30
Email, 37, 38, 39, 40
  Public Folders, 38, 39, 40
  Remote Access, 18, 20, 21, 40, 53
eNet, 8, 21, 27, 32, 36, 38, 41, 42, 43, 70, 73
  Development, 41
  Software, 41
Enterprise Software, 48
Escalation Procedures, 50
File Transfer Program, 53
Hardware Configuration
  Workstations, 47
Home Telephone Lines, 58
HP Open View Network Management, 13
IDF Termination Blocks, 29, 85
Information System Security Officer, 33
Internet Explorer, 41, 47
Intranet, 8, 9, 38, 41
Intruder Detection, 15, 19, 36
Inventory
  Workstations, 46
IP Addresses, 12, 15, 48, 55
iPlanet, 42
IPX Protocol, 15
IPX/SPX, 12
Jacks, 29, 85
Java, 42
LAN Devices, 14, 17
Laptops, 14, 35, 64
Local Service, 11, 56
Logins, 16, 18, 19
  Concurrent, 19
MAPI, 39
Modem Lines, 58
Modems, 20, 58
Naming Conventions, 22, 25, 46
Net8, 55
Netware, 15
Network Interface Card, 17, 27
Networks, 9, 10, 11, 12, 13, 14, 15, 17, 18, 20, 21, 22, 25, 27, 29, 30, 31, 41, 46, 47, 52, 56, 57, 65, 78
  Access, 18
  Connecting LAN Devices, 17
  Enterprise Network, 12, 14, 15, 17, 29
  Intruder Detection, 19

Logins, 19
Monitoring Software, 12
Naming Conventions, 22
Operating Systems, 17, 52
Security, 15
Nodes, 9, 78
Nortel SL100, 56, 57, 58, 86
Operating Systems, 15, 17, 25, 46, 52, 55, 71
Oracle, 42, 55
OS/390, 55
Paging, 68
Paging Devices, 68
Partition, 15
Passwords, 19, 20, 38, 58
PDAs, 35, 63, 65, 71, 72, 73
PeopleSoft, 9, 11, 48
Workstation Client (PeopleTools), 48
PeopleTools, 48
Port Authority Wide Area Network (PAWANET), 9, 10, 11, 12, 14, 17, 20, 23, 30, 41
ATM Node Assignments, 9, 11, 12, 13, 78
Diagram, 10, 56
Functions, 11
Network Monitoring Software, 12
Protocols, 12, 15
Supported Protocols, 12
Switches and Routers, 12, 14, 25, 29, 85
Printers, 14, 21, 25, 27
Private Branch Exchanges, 56
Protocols, 12, 15
Public Folder, 38, 39, 40
Public Folders, 38, 39, 40
Remote Access, 47
Routers, 12, 14, 25
SANs, 11, 14, 15, 16, 17, 21, 28
SAP, 9, 11, 48, 70
Scanners, 14, 27
Security, 15, 17, 18, 20, 33, 48, 49, 53, 55, 61, 64, 72, 76, 80
Applications, 55
Physical Security, 17, 48, 55, 61
Servers, 14, 15, 16, 17, 21, 22, 25, 28, 30, 39, 40, 42, 52, 53, 55
Application, 14
Logical Security, 17, 53
Names, 15, 22
Physical Security, 17, 55
Racks, 14
Standard Hardware, 21
Web, 42
SNA/SDLC, 12
Software
Workstations, 47
SQL Servers, 55
Sun Solaris, 15, 53, 55
Support Desk, 29, 32, 33, 34, 35, 36, 48, 49, 50, 58, 71, 72
Escalation, 50
Switches, 12, 14, 29, 85
System Backup and Recovery, 25, 27, 79
Logs, 28
Scheduling, 28
System Management, 15, 18, 19, 23, 25, 27, 28, 29, 31, 33, 34, 35, 36, 46, 48, 50, 52, 55
TCP/IP, 12, 55
Telecommunications
Electrical Requirements, 30

Standards, 29
Telecommunications Room, 29
Telephone Closets, 29, 85
Telephone Company Interface, 31
Telephone Help Desk, 58
Telephone Network, 56, 58, 59
Cabling, 14, 25, 29, 82
Diagram, 56
Time Restrictions, 19
Toll Free (800) Service, 59
Unified Wiring Plan, 82
Uninterrupted Power Supply, 15, 30, 81
Unix, 53
Logical Security, 53
User Accounts, 18, 25, 46
Creation, 18
Security, 18
Verizon, 11, 56, 57, 58, 70
Videoconferencing, 11
Virus, 34, 36
Protection, 15, 25, 35
Scanning, 32
Virus Response Team, 26, 32, 33, 34, 35, 36
Voice Mail, 58
VShield, 47
Wide Area Network, 9, 11, 12, 15, 20, 46, 62, 64
Windows 2000, 15, 47, 52
Windows NT, 15, 18, 38, 47, 52, 53
Windows Server, 52, 53
Wiring Closets, 14
Workstation
User Accounts, 25, 46
Workstations, 14, 16, 25, 29, 35, 46, 47, 48, 50, 85
Computing Resources Policy, 37, 51
Drive Mapping, 16, 47
Enterprise Software, 48
Enterprise Software (Peoplesoft Client), 48
Hardware Configuration, 47
Inventory, 46
Jacks, 29, 85
Naming Conventions, 46
Remote Access, 47
Security, 17, 48, 55, 61
Standard Software, 47
User Accounts, 46

and Software Standards and Software Standards and Software Standards Standards and Software Standards Etiquette Hardware Configurations Telephone Service Request Line

ATTACHMENT K – TECHNOLOGY SERVICES DEPARTMENT SYSTEM ADMINISTRATION GUIDE

THE PORT AUTHORITY OF NY & NJ

GUIDE

to

System Administration

Version 5.1
Revised March 29, 2011

1.0 Overview 5
1.1 Purpose of this Document and Intended Audience 5
1.2 Definition of Key Terms Used in this Document 5
1.2.1 System Management and Administration Functions 5
1.2.2 Other Terms Used in this Guide 6
2.0 Network Connections 8
2.1 Roles and Responsibilities 8
2.2 Network Connections Services 8
2.3 IP Addressing Network Support 9
3.0 Network Operating System Installation 10
3.1 Pre-Installation Procedure 10
3.1.1 Contact the Network Architecture group 10
3.1.2 Contact the LAN Planning & Design group 10
3.1.3 Verify Hardware Installation 10
3.1.4 Verify Installation Account Privileges 10
3.1.5 Confirm Design Document Compliance 11
3.1.6 Assemble Installation Utilities 11
3.1.7 Boot the Server Using the IBM ServerGuide 11
3.2 Installing Novell NetWare 12
3.2.1 Installation Guidelines 12
3.2.2 Port Authority Conventions 12
3.2.3 Creating SAN Volumes 13
3.2.4 Post installation Tasks 13
3.2.5 Drive Mapping Conventions for Novell 13
3.3 Installing Microsoft Windows Server 14
3.3.1 Installation Guidelines 14
3.3.2 Port Authority Conventions 15
3.3.3 Creating SAN Volumes 15
3.3.4 Post Installation Tasks 16
4.0 Server Monitoring and Alerts 17
5.0 Novell Directory Printing Service (NDPS) Installation for NDS 18
5.1 Installation and Configuration for HP NDPS Printers 18
5.2 Installation and Configuration for Toshiba Network Printers 18
5.3 iPrint Installation and Configuration 18
6.0 Security 19
6.1 Security Administration 19
6.2 Physical Access 19
6.2.1 Physical Access Control for Areas Containing Sensitive Information 19
6.2.2 Multi-User Computer or Communications Systems In Locked Rooms 19
6.2.3 List of Authorized Personnel 19
6.2.4 Controlling/Monitoring Access to the Restricted Area 20
6.2.5 Reporting Lost or Stolen Identification Badges and System Access 20
6.2.6 Propped-Open Doors to Restricted Areas 20
6.2.7 Physical Security for Sensitive Information 20
6.2.8 Property Pass for Removal of Hardware, Software or Data Files 20
6.2.9 Physical Access Control Codes on Worker Termination 21
6.2.10 Maintenance of List of Authorized Business System Managers 21
6.3 System and Application Access 21
6.3.1 Maintaining Authorized User Accounts 21
6.3.2 Limiting Access to the LAN 22

6.3.3 Microsoft Windows Logical Security 22
6.3.4 Unix Logical Security 24
6.4 Remote Access 25
6.5 Security Software: Kane Security Analyst 25
6.5.1 Set up and installation of Kane Security Analyst On Novell Server 25
6.5.2 Set up and Installation of Kane Security Analyst For an NT Server 28
6.6 Virus Protection 31
6.6.1 Technology Services Department Responsibilities Concerning Viruses 32
6.6.2 Server Virus Protection 33
6.6.3 Desktop Virus Protection 33
6.6.4 Virus Protection For Stand Alone and Laptop PCs and Personal Digital Assistants (PDAs) 33
6.6.5 Media: Diskettes (Floppy & Zip) and CD-ROMs, Portable Hard Disk Drives, Backup Tapes 34
6.6.6 Virus Symptoms 34
6.6.7 Incident Response 35
6.7 Software Inventory and Licensing 35
6.7.1 Software Procurement Liaison 35
6.7.2 Software Installations 36
6.7.3 License Control 36
7.0 E-mail 37
7.1 Systems Administrator Responsibilities 37
7.2 E-mail Viruses 37
7.3 Outlook Responsibilities Performed by the Support Desk 37
7.3.1 Procedure for Account Creation/Deletion/Modification: 38
7.3.2 Procedure for Resetting Passwords 38
8.0 Day to Day Operations 39
8.1 Backup & Recovery 39
8.1.1 Overview 39
8.1.2 Installation of Server Backup Components ..... **Error! Bookmark not defined.**
8.1.3 Backup Scheduling 39
8.2 Testing the Restore Procedure 39
8.3 Patches and updates 40
8.4 Application Software 40
8.4.1 Recommended Procedure for Testing and Implementing Patches 40
8.5 Adding and Deleting User Accounts 41
8.5.1 Creating New Novell User Accounts 41
8.5.2 Explanation of Technology Services Department Standard User Account Parameters 44
8.5.3 Deviations from Technology Services Department Standard User Account Parameters 45
8.5.4 Inactive User Accounts 45
8.6 Login Script 46
8.7 Guest Account 46
8.8 Administrator Accounts 46
8.9 Granting User Access to Windows Network Resources 47
8.10 Application Software Support Activities 48
8.11 Change Reporting 48
8.12 System Monitoring 49
8.13 Server/eDirectory Maintenance Procedures 49
8.13.1 Server Outage Notifications 49

8.13.2 Server Reboot Procedures 49
8.13.3 NetWare NDS Health Checks ..... **Error! Bookmark not defined.**
8.13.4 NDS/e-Directory Partition and Replica Changes ..... **Error! Bookmark not defined.**
8.13.5 Firmware upgrades on IBM Cluster Servers ... **Error! Bookmark not defined.**
8.13.6 Decommissioning of File Servers ..... **Error! Bookmark not defined.**
8.13.7 Creating a new eDirectory Container ..... **Error! Bookmark not defined.**
8.14 Suspected Account Break-Ins (Intruder Alerts) ..... **Error! Bookmark not defined.**
8.15 Systems Administrator Resources 49
9.0 Desktop and Enterprise Application Support 51
9.1 Desktop Inventory 51
9.2 Desktop Operating System Standard 51
9.3 Desktop Configuration 51
9.3.1 Desktop Naming Conventions 51
9.3.2 Desktop User Accounts 51
9.3.3 Remote Desktop Management 52
9.3.4 Drive Mappings 52
9.4 Standard Department PC Desktop Software 52
9.5 Enterprise Software 52
9.5.1 PeopleSoft 53
9.5.2 SAP 53
9.5.3 Microsoft Outlook and Exchange 53
9.5.4 eNet 53
9.5.5 Other Business Applications 53
9.6 Workstation Security 53
9.6.1 Physical Security 54
9.6.2 Logical Security 54
9.7 Port Authority Help Desk/Unisys Support 54
9.8 Network Problem Notification 54

1.0 Overview

1.1 Purpose of this Document and Intended Audience

The purpose of this guide is to document the policies and procedures governing the administration of the Port Authority's network resources. While this document is intended primarily for System Administrators, it provides information useful to any Port Authority employee, PTA (Professional, Technical, or Advisory), consultant, contractor, and/or outside vendor responsible for performing the following functions:

Business System Management
Security Management
Application Management
Application Administration
System Management
System Administration

For a definition of each of the above functions, see Section 1.2.1

This document includes only those policies and procedures that are unique to the Port Authority, and cannot be found in vendor manuals. It will not tell you everything you need to know about how to set up a Local Area Network, design, implement and configure a network application, or deploy a system. However, when agency-wide policy requires System Administrators to select settings or parameters that differ from the vendors' default settings, those settings and parameters are included in this document.

1.2 Definition of Key Terms Used in this Document

1.2.1 System Management and Administration Functions

The Port Authority's Technology Services Department (TSD) recommends that networks be managed and administered using the following organization. The positions/functions listed are needed for effective technology management and reporting. Depending on the size of the network, one person may perform multiple roles in this structure.

Function	*Definition*
Business System Manager	The Business System Manager is the individual with overall responsibility for managing the system, including applications and their data and the resources needed to support that system. Responsibilities include making decisions or recommendations to departmental management concerning functionality, funding, resource management, access control, and security. The Business System Manager is considered the de

	facto "system owner of record".
Security Manager	The security manager is responsible for establishing and approving levels of access for users, development of security procedures to safeguard the integrity of data and applications, review of security logs, informing users of their obligations to safeguard information and regularly reviewing the appropriateness of user access levels.
Application Manager	In a large system, the application manager manages the functionality of the application and oversees the work of the Application Administrator. A person closely associated with the end users of the application most often performs this function.
Application Administrator	Performs the day-to-day administration of the application's configuration and security profile, and is responsible for the distribution of application upgrades, patches, service packs and bug fixes.
Technical System Manager	The person responsible for managing the technical infrastructure for the application system, including the distribution of upgrades and bug fixes for hardware and software. The System Administrator may report to this manager or may report directly to the Business System Manager.
System Administrator:	Performs the day-to-day administration of the technical infrastructure, supporting file, print and application services available to users.

1.2.2 Other Terms Used in this Guide

Term	***Definition***
System	A file and print service capability or departmental application or corporate/enterprise application with a component located in areas under the responsibility of the Business System Manager.
Departmental LANs	Departmental networks, commonly called LAN's consist of the following components on the Port Authority side of carrier lines of demarcation: cabling, PC desktops, print servers, printers, scanners, and copiers. They differ from traditional LANs in that they are part of a larger agency-wide distributed computing network called the Enterprise network or PAWANET.

PAWANET	Acronym for Port Authority Wide Area Network. Includes routers, switches, wiring closets, racks.
Enterprise Network	The Port Authority's modern, agency-wide distributed computing network. The same as PAWANET.

For a description of the enterprise network architecture and for agency-wide standards for software and hardware, please see the *Standards and Guidelines for Port Authority Technology.* That document is intended to assist departmental managers and system designers to ensure that their systems will be compatible with, and can, therefore, be connected to the enterprise network.

2.0 Network Connections

2.1 Roles and Responsibilities

There are 5 groups within the Technology Service Department, Office of Technology Infrastructure, who are jointly responsible for network connectivity. Listed below are the key responsibilities of each:

Network Services Support

Test a new device or one with suspected network connection problems to ensure it is operating properly.

Maintain routers and switches.

Verify that the network connection in the cubicle or office is active and working properly.

Network Connections (Site Prep Staff)

Install cross-connect and station drops.

Test cabling using the proper tools.

Resolve network port problems.

Verify that the network port in the cubicle or office is active as well and is working properly.

Business System Managers (End Users)

Submit TSD Service Request for installation of new network station drops. Online form available on Enet.

TSD - WAN Design/Implementation – Cisco Support

Install routers and switches.

TSD-Network Operations – Cisco Support

Resolve network hardware and software problems.

2.2 Network Connections Services

Computer Network Solutions (CNS) continuously monitors PAWANET to ensure that

connections between all Port Authority sites are operating normally 24 hours a day, seven days a week. CNS also ensures proper configuration of switches and routers.

The System Administrator is responsible for verifying that the server or the desktop is not the cause of a user being unable to connect to the network. If there is a problem and it is not related to the server or desktop, the System Administrator, or End User should call the PA Help Desk, 212-435-7469, who will log the call and contact the appropriate groups.

When the End User determines that a new connection to PAWANET is needed, a TSD Service Request must be submitted to the Network Services Division requesting that a new connection be assigned. This process also applies when a department is relocating to another site. The Network Services Division will work in tandem with Network Connections (Site Prep) to:

Determine the devices that need to be moved.

Set up the necessary connections at the new location.

2.3 IP Addressing Network Support

All Port Authority Information Technology devices connected to PAWANET must have an Internet Protocol (IP) address. PC workstations will be dynamically assigned IP addresses through Dynamic Host Configuration Protocol (DHCP). Static IP addresses are required for servers, printers, and network attached fax machines, copiers, scanners, and all other network attached equipment. System Administrators are responsible for obtaining static IP addresses from the Network Architecture Division of the Technology Services Department. They maintain a list of all current static IP addresses on the network, including the Org Unit responsible for that device.

3.0 Network Operating System Installation

3.1 Pre-Installation Procedure

System Administrators must perform the following steps prior to installing either Novell NetWare or Microsoft Windows operating systems.

3.1.1 Contact the Network Architecture group

Contact the TSD Network Architecture Group to obtain the following settings:

IP Address
Subnet Mask
Default Gateway
DNS Server Address
WINS Server Address for Windows Servers
Latest Server Design Document (Example. JFK Cluster Design Document)
(see Appendix A for appropriate PA contacts)

3.1.2 Contact the LAN Planning & Design group

Contact the LAN Planning & Design group for determining the proper server name.

3.1.3 Verify Hardware Installation

Verify the hardware is installed properly as per the Server Design Document. Contact the LAN Planning and Design (LP&D) group to obtain the Server Name.

Exceptions to this standard are the subnets covered by the Network Operations Centers in the TeleCenter and PA Technical Center, where servers may be assigned an IP address outside the standard range.

3.1.4 Verify Installation Account Privileges

Contact the Systems Administration Team to obtain:

Account/password with Supervisor right at the [Root] of the eDirectory tree

Account/password with Supervisor right to the container where the server will be installed

Account/password with Read right to the Security container object for the eDirectory tree

3.1.5 Confirm Design Document Compliance

Confirm that the server being built has been received with all the components that were originally specified and ordered and that all items are assembled in accordance with design specification documents provided by the LAN Planning & Design Group.

3.1.6 Assemble Installation Utilities

Confirm that all the following are available for use during installation:

IBM Server Guide Setup and Installation CD

Novell NetWare or Microsoft Windows Server CD

Service Pack CD, if required.

License files or diskettes and activation keys, if required

Firmware and device drivers not available on the ServerGuide CD.

3.1.7 Boot the Server Using the IBM ServerGuide

Insert the IBM ServerGuide CD in the CD-ROM drive and boot the server for the first time. The setup and installation program detects your server model and installed adapters. The wizard interface guides you through setup and configuration.

Select *Express Configuration* for installation type. This will make the installation easier by running the required programs for the server, based upon the hardware that is detected before installing the *Operating System* itself.

- The Set Date and Time task is provided so that you do not have to use the Config/Setup utility to access these settings.
- Clear Hard Disks clears all partitions from the partition table and resets arrays to the factory default settings.
- Perform System Updates checks the server BIOS and microcode (firmware) levels for supported options and then checks the CD for a newer level. CD content can be newer than the hardware. ServerGuide can perform a flash update of the BIOS and microcode.
- The ServeRAID Manager program starts, leading you through the entire configuration process. The local SYS partition will be configured as RAID 5 (striping with parity) for NetWare servers, and the C: drive as RAID 1 (mirroring) for Windows servers.
- The Performance Optimizer program easily tunes your server for your

environment.

- Before the setup program completes, ServerGuide creates a System Partition on the default drive.

- If you chose the Custom Configuration path, you can select to copy the configuration settings and firmware levels to a Setup Replication Diskette. If you chose the Express Configuration path, you can select this task after the Configuration Summary Screen.

  ServerGuide displays a hardware configuration summary, so that you will know when you have completed all the required tasks. Verify that the server recognizes all RAM that was installed. Then, you are ready to install your NOS.

  Notes: Plug and Play adapters are configured automatically. Non-plug and play adapters or non-IBM adapters might require switch settings, additional device drivers, and installation after the NOS is installed. See the documentation that comes with the adapter.

- Diagnostics for your server are either in read-only memory (ROM) or on a separate diagnostics CD that comes with your server.

For a list of compatible adapters, go to the IBM ServerProven Web site.

- The ServerProven Web site lists adapters that are supported by your server hardware. Not all adapter device drivers are included with ServerGuide.

3.2 Installing Novell NetWare

3.2.1 Installation Guidelines

The agency is moving to Microsoft and no new Novell Clusters are being built at this time.

3.2.2 Port Authority Conventions

Use the following Port Authority conventions when configuring a Novell NetWare 6.5 Operating System installation:

Prepare a DOS partition of at least 2 GB on the clustered file servers.

At the *Specify the Server Name* screen, enter the server name obtained from the LP&D group and adhering to the Server Naming Conventions.

When prompted to assign an internal IPX number to the server, do not enter a value as the IPX protocol is no longer used on the Port Authority network.

Load TCPIP with IP address provided by the Network Architecture group.

Modify the SYS volume size. In the highlighted box type the volume size. A minimum of 10 GB is recommended. NetWare SYS volumes should not contain applications, databases or log files that may grow and jeopardize the amount of free space and the integrity of the server.

Leave the remaining free space unallocated for volume future space and adjustments.

Verify that the STARTUP.NCF and AUTOEXEC.NCF files are accurate.

3.2.3 Creating SAN Volumes

Install the APPS and DATA volumes on the Storage Area Network (SAN) using a RAID 5 configuration in accordance with Port Authority standards:

Volume names must adhere to Port Authority Naming Conventions (SYS, APPS, DATA).

3.2.4 Post installation Tasks

Following installation of the Network Operating System, install all required Novell NetWare Service Packs, antivirus software, server monitoring agents and backup software as indicated in the following document:

PA Server and Software Standards

See Section 8.1, Backup and Recovery, for installation guidelines.

All newly-built Novell servers will be QA'd using Port Authority Standard Process:

3.2.5 Drive Mapping Conventions for Novell

The following drive letters are reserved for Novell installations.

P Public Applications
Q Installation and Upgrade Utilities
S Department shared directories
U Users home directory
Z Novell system files

Public (Shared) Application software installed on a LAN file server shall reside off the root in a volume named "APPS".

Example: map P:=<*file server name*>\APPS:

Each software application installed on the LAN file server shall have its own sub-folder.

Example: P:\SAP

System software installed on a LAN file server shall reside on a volume named SYS:
Example: map S16:=<*file server name*>\SYS:PUBLIC

Data stored on a LAN file server shall reside on a volume named DATA and should be mapped to the "S:\" drive pointer.

Example: map root S:=<*file server name*>\DATA:SHARE.

Installation files used in the installation of desktop software should reside on a volume named APPS.

Example: map root q:=<*file server name*>\apps:

3.3 Installing Microsoft Windows Server

3.3.1 Installation Guidelines

Configure the Boot (C:) Partition:

> Always Select NTFS file format for security and performance reasons.
>
> To determine partition size, use a minimum of 4GB, but 8GB is recommended. This is very important because you cannot extend the size of the C drive once it has been created and this is where the Windows swapfile will reside. Use the remaining space on the local drive

For Windows servers, use the settings specified in the Windows Server QA document (see section 3.3.4).

Make the following registry change to allow more than one server to provide antivirus definition updates (DNS Round-Robin):

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters\
MaxCacheEntryTtlLimit = 1

3.3.2 Port Authority Conventions

1. Do NOT install IPX/SPX protocol on Windows servers. If the server supports an application that requires it, notify the LAN Planning and Design group.

2. ~~Do NOT install the Novell Client on a Windows server. Files can be copied to the~~ server from a Novell server via a workstation with the Novell Client installed.

3. Do NOT make an NT 4 or earlier server a domain controller, and do NOT install Active Directory domain controllers without expressed permission from the LAN Planning and Design group contacts listed in Appendix A for details)

4. Do NOT install the WINS or DNS services without expressed permission from the LAN Planning and Design (LP&D) group (see Appendix A for appropriate PA contacts).

5. The PA standard requires that you use Novell for File and Print Services. Installing user home directories and printers on Windows servers is to be avoided unless the server supports an application that requires it.

6. Do NOT install the NetBEUI protocol on Windows servers/workstations.

7. Do NOT assign user passwords that are the same as the username.

8. Do NOT start any Windows services using the Comanche (administrator) account. A separate account should be set up for this purpose.

9. Disable the Guest account.

Determine the Server's Role. By default, Microsoft application servers are designated as Member servers within the Active Directory organizational structure. If this server is being built as a Domain Controller (Primary or Backup), the LAN Planning and Design group in the Technology Services Department needs to approve the configuration.

Configure Windows Network Connections and IP settings.

Configure SNMP settings for IBM Director Server monitoring and Unisys remote ~~monitoring (see Section 4.0 of this document.)~~

If prior approval has been obtained, join the appropriate Active Directory resource organizational unit. Unless the server has already been created, you will have to login to the domain with an account that has the ability to add machines.

Enter a Maintenance note stating the date and person who installed this server

3.3.3 Creating SAN Volumes

If required, the Oracle database(s) will be installed by the Oracle DBA with 2 logical drives on the Storage Area network, one for the Oracle data files (RAID-5) and a second one for the Oracle online redo logs and control files (RAID-1). The sizes of these drives are to be determined by the Oracle DBA.

3.3.4 Post Installation Tasks

Install the latest approved Microsoft Windows Service Packs, antivirus software, and backup software as indicated in the following document:

PA Server and Software Standards

See Section 8.1 of this document, Backup and Recovery, for installation guidelines.

Create an Emergency Repair Disk by running the Windows Backup utility. Keep this disk in a secure location and updated when required (Service Pack applied or a configuration change occurs).

Run a security report and submit to the PA security officer prior to placing server into production.

All Windows servers will undergo a Quality Assurance process before being placed into production.

4.0 Server Monitoring and Alerts

Server monitoring, remote management and alert functions have been transferred to IBM Director.

Guidelines for agent installation on Windows 2003 servers are being developed and will be posted here when complete.

5.0 Novell Directory Printing Service (NDPS) Installation for NDS

The Port Authority standard Print Server is the HP Jet Direct External and Internal cards, and the Toshiba eStudio series copier with network printing capabilities. All printers are currently configured using the NWadmin utility, as there is no plan to include an NDPS snap-in for ConsoleOne. The PA's current standard is to use Novell iPrint.

5.1 Installation and Configuration for HP NDPS Printers

Before configuring the printer, make sure the following tasks have been performed:

1. **Internal print servers:** The print server is installed in the printer and the printer is directly connected to PAWANET.

   External print servers: The print server has external power and is connected to the printer's parallel port and to PAWANET

2. The printer is turned on, is online, and a JetDirect configuration page has been successfully printed. If not, see the vendor's installation guide for your print server or your printer's *Getting Started Guide* for instructions.

3. Obtain an IP address in the static IP range reserved for Network servers and printers (.201- .234) from the Network Architecture group.

5.2 Installation and Configuration for Toshiba Network Printers

Guidelines for Toshiba printer object creation are being developed and will be posted here when complete.

5.3 iPrint Installation and Configuration

We are moving to Microsoft File and Print Services and iPrint will be phasing out.

6.0 Security

6.1 Security Administration

The System Administrator and Business Systems Manager are responsible for creating and maintaining a secure system environment in keeping with the guidelines outlined in this section.

6.2 Physical Access

6.2.1 Physical Access Control for Areas Containing Sensitive Information

Access to every office, computer room and work area containing sensitive information must be physically restricted. Management responsible for the staff working in these areas must determine the appropriate access control method (receptionists, metal key locks, magnetic card door locks, locking cables, anchor pads, etc.)

6.2.2 Multi-User Computer or Communications Systems In Locked Rooms

All multi-user computer and communications equipment must be located in locked rooms to prevent tampering and unauthorized usage.

6.2.3 List of Authorized Personnel

If equipment associated with departmental applications is outside one of the Technology Services Department's Network Operations Centers or Communications Closets, the Business System Manager is also responsible for controlling authorized access to the Restricted Area where the equipment is located. The Business System Manager must maintain a list of persons authorized to enter these areas. If more than one system is located in a physical environment, there should be only one Authorized Physical Access List maintained by the Business System Manager responsible for that Restricted Area.

The Business System Manager must approve requests for additions or removals from the list. If persons enter and leave the Restricted Area using an automatic entry system, the System Manager is responsible for reconciling entry system files with the list on a regularly scheduled basis.

6.2.4 Controlling/Monitoring Access to the Restricted Area

Only those persons on the Authorized Physical Access List will be permitted access to the Restricted Area, unless escorted by a person with escort privileges. The escort must accompany the visitor for the entire duration of their stay in the Restricted Area.

All persons entering the Restricted Area must sign the Physical Access Log upon entry and exit unless the person is permitted access through an automated card access system. All escorted persons must also present acceptable picture identification in the form of valid driver's license, passport, or company ID.

The Business System Manager will review the log on a regular basis, reporting any irregularities to Departmental Management. In the event that a person granted physical access is no longer authorized for that access, the Business System Manager is responsible for removing him/her from the Authorized Physical Access List. Examples of such events are employee, PTAs (Professional Technical & Advisory personnel) or contractor staff, departure because of termination or transfer to other responsibilities.

6.2.5 Reporting Lost or Stolen Identification Badges and System Access

Identification badges and physical access cards that have been lost or stolen – or are suspected of being lost or stolen – must be reported to Departmental Management immediately. Likewise, all computer or communication system access tokens (smart cards with dynamic passwords, telephone credit cards, etc.) that have been lost or stolen – or are suspected of being lost or stolen – must be reported to the Business System Manager.

6.2.6 Propped-Open Doors to Restricted Areas

Whenever access doors to a Restricted Area are propped open, perhaps for moving equipment, furniture or supplies, the entrance must be continuously monitored by an employee or escort.

6.2.7 Physical Security for Sensitive Information

All information storage media (such as hard disk drives, floppy disks, magnetic tapes, and CD-ROMs) containing sensitive information must be physically secured when not in use.

6.2.8 Property Pass for Removal of Hardware, Software or Data Files

Computer systems, portable computers, modems, software installation media, backup media, data files and related information systems equipment must not leave company premises unless accompanied by an approved property removal pass (PA 3072).

6.2.9 Physical Access Control Codes on Worker Termination

In the event that a worker terminates his or her relationship with the company, all physical security access codes for the Restricted Area known by the worker must be deactivated or changed. For example, the serial number recording on a magnetic strip attached to an identification badge must be changed before the badge is reissued to another worker.

6.2.10 Maintenance of List of Authorized Business System Managers

A list of managers who are designated "Business System Managers" to grant access to Restricted Area(s) must be kept up-to-date. The Department Director or their designee who delegated authority to these Systems Managers must also periodically review this list.

6.3 System and Application Access

Depending on the application, security may be administered at the application, database, module, screen, data field, and/or transaction level. Prior to implementation, the Business System Manager should review the capabilities of the application and assure implementation of the appropriate security levels. When in production, the Application Administrator is responsible for maintaining the selected security profiles. This may require a second level of passwords beyond the Novell e-Directory login and/or other external verification of the user's authorization.

6.3.1 Maintaining Authorized User Accounts

The System Administrator is responsible for creating and maintaining accounts for all users authorized to access PAWANET and its connected systems. All Port Authority users accessing PAWANET must have a Novell e-Directory account for File & Print Services.

Business System Managers should re-evaluate the access privileges granted to all users of their applications, or systems, every six months.

Application Administrators work in conjunction with the System Administrator to identify Individual user accounts that need access to their applications, and define the level of access required. Each distinct level of access requires a unique Global Group be created on the Domain Controller by the System Administrator, and populated with the User accounts specified by the Application Administrator. Application Administrators are responsible for maintaining a local group, or groups, to organize and manage application access. Local Groups are populated by adding the Global Groups created by the System Administrator as members of the Local Group. This method distinguishes between user account management and application access, dividing the responsibilities between the

System Administrator, at the Domain, or Enterprise level, and the Application Administrator at the departmental or application level.

Application Managers should re-evaluate the privileges granted to all users of the application at six-month intervals, or at whatever period is appropriate for the level of security and sensitivity of information stored on that system. The Application Manager should provide the Business System Manager with a report of this information regularly for review. The report must indicate the applications that each user is authorized to use. It is important to keep these lists up-to-date as new employees and consultants are added and as others resign or are transferred and are no longer authorized.

6.3.2 Limiting Access to the LAN

The System Administrator will limit access to the LAN by doing the following:

Create logon IDs for only those persons authorized by the Business System Managers.

Reconcile the list of users with the list of persons authorized by the Business System Managers periodically.

Follow the Port Authority standards for password assignment, expiration and change.

Establish controls over supervisor, or other privileged account, passwords, or other special passwords, so that their use is documented and approved by the Business System Manager.

Research sign-on violations to determine if a pattern is evident and report findings to the Business System Manager as necessary.

6.3.3 Microsoft Windows Logical Security

The System Administrator is responsible for logically securing Microsoft Windows servers from unauthorized access. To aid in the creation of a secure computing environment, the following steps should be taken at a minimum:

1) User accounts are not to be created locally on Windows servers if at all possible. Local security groups containing global user groups are the methods of rights management in Active Directory.

2) Disable Remote Access Server. The only authorized remote access is described in Section 6.4 Remote Access.

3) Limit access to Network Monitor. Access to Network Monitor enables the capturing of packets and potentially compromising passwords and security.

4) Secure tape backups. Backup tapes should be stored offsite in fireproof cabinets. Unrestricted access to encrypted backup tapes can compromise data and system

security.

5) Physically secure Emergency Repair Disks. Emergency Repair Disks are critical in restoring a damaged Microsoft Windows server, but contain a copy of the password database. Physically securing the disks minimizes the potential of unauthorized access to the password database.

6) Use NT File System (NTFS) for the boot partition. Microsoft Windows manages security only on NTFS file system partitions and not on FAT partitions. Use of NTFS partitions adds another layer of security for the system.

7) Separate the boot partition from user data. This helps ensure that user files are not affected by service packs or upgrades and prevents user access to critical system files.

8) Enable weak password filtering. The Notification Packages value in the registry should be modified to require that all passwords are at least 6 characters in length, contain characters from at least three of four groupings (lower case, upper case, numbers and non-alphanumeric characters) and that passwords do not contain the user name or any part of the user's full name.

9) Enforce the requirement that passwords be changed upon initial logon and no less often than every 90 days thereafter.

10) Control access to the command scheduler. Users should not have permission to schedule services or jobs, or to list previously scheduled jobs.

11) Enable Administrator account lockout and rename the Administrator account. The Administrator account should be configured to lockout after repeated failed access attempts over the network. The account should still be accessible from the system console. In addition, the Administrator account should be renamed so it is not as easily accessible to unauthorized individuals.

12) Establish separate accounts for System Administrators. Administrators should only use privileged accounts when necessary for system administration. *All other times they should use individual user accounts*, which limits the possibility that unauthorized individuals can access administrator accounts.

13) Default Guest Account should be renamed and disabled. In addition, a strong account password should be in place and all rights should be removed from the account.

14) Null session should be disabled if not required by the system.

15) Secure and manage event logs. NTFS permissions should be set on the event log files to allow only Administrators and System access. In addition, auditing should be enabled on event log files to detect when they have been copied or viewed.

16) Encrypt the Security Account Manager (SAM) password database with 128-bit encryption. This minimizes the possibility that passwords can be cracked and used by unauthorized individuals.

17) Disable Internet Information Server. Web based applications should be used only on approved platforms and with proper security enabled. Standard NT application servers should not function as both application and web servers.

18) Disable remote registry access. The appropriate registry entry should be modified to disable access to the server's registry over the network. This minimizes unauthorized access to the server.

19) NT Kane Security Report must be produced at least quarterly and forwarded to the Business System Manager for review.

20) Monitor for security patches and updates.

21) Security and System Administrators should attend security training.

6.3.4 Unix Logical Security

The System Administrator is responsible for logically securing the Unix server against unauthorized access. The following steps should be taken at a minimum:

1) Modify startup scripts to disable unnecessary services. Ensure that only the root account can edit startup files.

2) Enable additional logging. The /etc/syslog.conf file should be modified to add logging to capture unsuccessful login attempts, successful and failed su attempts and reboots via the auth.info entry.

3) Disable sendmail, if not required by the application.

4) Monitor for security patch updates.

5) Verify valid account login shells for users. Expiration dates should also be set for all temporary accounts.

6) Verify valid home directories for all users.

7) Restrict access to crontab file to the administrator account and ensure that crontab and inittab jobs do not access files that are writeable by anyone other than root.

8) Disable remote access to the Unix system as root.

9) Disable anonymous FTP.

10) Never use "xhost+" on an x-server.

11) System log files, which contain information about system activity, should be reviewed and archived on a daily basis.

12) Usage of sensitive commands should be recorded in a system log and reviewed daily for unusual activity. These reports should be forwarded to the Business System Manager for review.

13) A Security Report, such as ESM for Unix, should be produced at least quarterly and forwarded to the Business System Manager for review.

14) Security and System Administrators should attend security training.

6.4 Remote Access

The Port Authority has a secure Remote Access system. This system is the authorized way for users to remotely access LANs and applications on the Port Authority's Enterprise network. Direct dial-in communications through any other means is not permitted unless approved by the Port Authority's Cyber Security Officer. If a vendor requests direct dial-in communications with the application system's server(s) and other devices, the application system should not reside on the Port Authority Enterprise network.

The Systems Administrator works with the Technology Services Department Remote Access group in providing remote access services for end users. The Systems Administrator is responsible for providing the appropriate Novell login script and by making necessary changes to Novell day/time restriction to 24x7 access. Access to Microsoft Windows application servers by third party vendors, are handled on a case-by-case basis.

End users who need remote access must submit a *PA3624A* Form, Request for Access to Information Systems. To submit a request for Remote Access, please visit Enet.

6.5 Security Software: Kane Security Analyst

The System Administrator is responsible for running the Kane Security Analyst quarterly and submitting copies to the Audit Department and Business System Managers for all Novell and NT domain controllers, application and member servers.

6.5.1 Set up and installation of Kane Security Analyst On Novell Server

Select the settings listed below when installing the Kane Security Analyst on a Novell Server. Be aware that settings for Novell must not conflict with the Kane Security Analyst. The settings for Novell should be set according to PA standards or the report produced may result in a lower security rating

Security Best Practice Area and Tests	Setting
Account Restrictions	
Limit Number of Concurrent Logins	Yes
Account Not Disabled by Administrator	Yes
Account Not Locked by Intruder Detection	Yes
Number of Maximum Connections	1 Connection
Dormant User ID Period	90 Days
User Station Restrictions in Use	No
User Time Restrictions in Use	Yes
User Account Expiration Dates in Use	No
Note: Accounts used by consultants or job shoppers must have an expiration date.	
Login Script Exists for All Users	No
User Template Object Exists For All Containers	No
Password Restriction	
Days between Forced Password Changes	90 days
Periodic Forced Password Changes	Yes
Users Have Ability to Change Passwords	Yes
Grace Logins Limited	Yes
Grace Logins Maximum	3 Logins Allowed
User Passwords Required	Yes
Password Minimum Length	6 Characters
Require Unique Passwords When Changed	Yes
Access Control	
Users with Administrative Privileges	List

Access Control Lists	
Not Security Equivalent To Another Object	Yes
Excessive Object Rights	Yes
Excessive Property Rights	Yes
System Monitoring	
Intruder Detection	Activated
Failed Logins Prior to Lockout	3 Failures
Minimum Bad Login Retention Period	1 Days 0 Hrs. 0 Mins.
Minimum Login Account Lockout Time Period	7 Days 0 Hrs. 0 Mins.
Parse Error Log for Login Violations	Yes
Auditing is Enabled on Volumes and Containers	No
Accounting System Feature Installed	No
Data Integrity	
System Fault Tolerance Activated (SFT)	Yes
Minimum SFT Level Installed	Level 2
Transaction Tracking Feature Activated	Yes
Read After Write Verify	Yes
Auto Repair of Volume Turned On	Yes
Percentage of Space In Use By Deleted Files	10 %
Data Confidentiality	
NCP Packet Signing	Activated
NCP Packet Signature Level	Level 1
Remote Console Password Not Scripted In Clear Text	Yes
Secure Console is Enabled	No
Allow Change To Client Rights	Enabled
Allow Unencrypted Passwords Is Turned Off	Yes

Immediate Purge of Deleted Files	Yes
Minimum Time Before Deleting Files	2 Days 0 Hours 0 Mins
Kane Security Analyst Context:	OU=SID.O=panynj

6.5.2 Set up and Installation of Kane Security Analyst For an NT Server

Select the settings listed below when installing the Kane Security Analyst on an NT workstation for analyzing an NT server.

Security Best Practice Area and Tests	**Checked/Unchecked**
Account Restrictions	
Account Disabled by Administrator	Yes
Account Locked by Intruder Detection	Yes
Dormant Inactive User ID Period	90 Days
User Station Restrictions in Use	Yes
User Time Restrictions in Use	Yes
User Account Expiration Dates in Use	No
Force Logoff of Remote Users When Logon Hours Expire	Yes
Password Strength	
Days between Forced Password Changes	90 days
Periodic Forced Password Changes	Yes
Users Have Ability to Change Passwords	Yes
User Password Required	Yes
Password Minimum Length	6 Characters
Minimum Password Age In Days	1 Day
Remember Previous Passwords	Yes
Number Of Passwords Remembered	Last 5 Passwords
Hide The Last User To Logon	Yes

Perform Password Cracking	Yes
Access Control	
Flag Administrator Equivalence	Yes
Only Administrators May Map Drives & Printers	Yes
Allocate Floppy Drives At Logon	Yes
Allocate CD-ROM Drives At Logon	Yes
Flag Remote Access Servers	Yes
Flag Users With Excessive User Rights	Yes

Define Excessive User Rights as indicated below:

- Act as Part of the Operating System
- Backup Files and Directories
- Change the System Time
- Force Shutdown from Remote System
- Generate Security Audits
- Increase Scheduling Priority
- Log On as a Batch Job
- Log On as a Service
- Log On Locally
- Manage Auditing and Security Logs
- Restore Files and Directories
- Shut Down the System
- Take Ownership of Files or Other Objects

System Monitoring

Account Policy

Account Lockout	On
Failed Logins Prior To Lockout	3 Failures
Minimum Bad Login Retention Period	1 Day
Minimum Logon Account Lockout Time Period	7 Days
Parse Error Log For Login Violations	Yes
Audit Policy	
Logon And Logoff	Failure

File and Object Access	Failure
Use Of User Rights	Failure
User And Group Management	Success & Failure
Security Policy Changes	Success & Failure
Restart & Shutdown	Success & Failure
Process Tracking	Blank

Event

Application Log Size	4096 KB
Application Log Retention	4096 KB
System Log Size	4096 KB
System Log Retention	Overwrite When Needed

Note: Application Log Size, System Log Size and Security Log Size should be set to allow 14 days of data to be maintained online. Afterwards, log data should be removed and stored on another media and maintained according to records retention or legal requirements.

Security Log Size	10,240 KB
Security Log Retention	Overwrite As Needed
Scan for Login Violations	Yes
Halt System When Security Log Is Full	No

Data Integrity

Uninterruptible Power Supply

Installed	No*

(* *Note:* If using a UPS other than a large Liebert answer Yes)

Service Started	Yes
Run A Command File Upon Power Failure	No

(* *Note:* If using a UPS other than a large Liebert answer Yes)

Delay Between Power Failure And First Message	5 Seconds
Delay Between Subsequent Messages	120 Seconds

Machine Shutdown Requires A Logon On	Server & Workstation
OS2 Subsystem Not Installed	Yes*
Posix Subsystem Not Installed	Yes*

* *Note:* Although the Posix and OS2 settings should be Yes, in most cases certain maintenance providers in an enclosed system may want you to have OS2 or Posix subsystems installed.

Flag FTP Services	Yes
Flag DHCP Client Service	Yes
Flag SQL Server Service	Yes
Flag Internet Information Server Service	Yes
Do not allow machines to be shutdown from the console without a logon on workstations	Yes
Anti-Virus Software Status Inoculan	No
Data Confidentiality	
System Root Resides On An NTFS Partition	Yes
Passwords Not Scripted In Start Up Files	
Display Legal Notice Prior To Logon Display on Servers	Yes
Check That Auto Logon Is Disabled	Yes

6.6 Virus Protection

System Administrators are responsible for downloading and installing current standard virus protection application and signature files. This involves the following steps:

Provide floppy diskette boot protection.

Protect by using a screen saver password with a recommended 15-minute time-out period.

System and application passwords should conform to the Technology Services Department standards.

Configurations must conform to security parameters identified by Kane Security Analyst software.

Perform deleted file purges immediately or no later than 6 days after file deletion.

Scan servers and desktops for viruses on a daily basis.

Scan for viruses all PC desktops upon the first daily network log-in.

Scan for viruses all incoming data from users, server peripherals diskette, CD-ROM, tape drives, other servers, and the Internet.

In addition, to help in recovery from a virus infection, the following steps should be taken:

Advise users to save all mission critical files to the server each day, because the server is backed up each night, and is fully protected against viruses. Most desktops are not protected in the same way.

Perform daily incremental backups and full backups weekly.

Store all backups off-site at a secure location.

Test recovery procedures annually.

6.6.1 Technology Services Department Responsibilities Concerning Viruses

In order to prevent or detect and remove computer viruses, the Technology Services Department will:

Plan and assist in the implementation of virus prevention and eradication procedures and methodologies.

Provide high-level technical support for quick containment of virus incidents to minimize disruption of business operations.

Purchase software license(s) for agency-wide use.

As more advanced enterprise software distribution tools are implemented, the Technology Services Department will assist with the automatic deployment of new or updated virus definition files or new virus scanning software to department servers and desktops.

Notify all departmental System Administrators of new or updated virus detection and eradication files and new virus scanning software.

Notify all departmental System Administrators first by e-mail and, if appropriate, by telephone or beeper of any publicized warning of imminent, significant virus attacks or virus hoaxes and any posted warnings. Provide System Administrators with as much warning time as possible and provide advice and recommend appropriate procedures.

Provide for the central reporting of all computer virus incidents through the Technology Services Department Help Desk.

Maintain a computer virus incident database to record all computer virus incidents reported to the Technology Services Department.

Below are descriptions of the virus awareness program initiatives used to inform departmental and facility staff.

The *What's New* page on the Enet informs users of new *Virus Alerts*

Messaging under Outlook is used for virus alerts/notifications. Virus infections of e-mail file attachments are cleaned and reported to the sender and recipient of the e-mail and to the Exchange Administrator.

Training of key staff, such as departmental System Administrators.

Participate on a joint Technology Services Department/Audit computer virus awareness program to educate departmental and facility staff.

6.6.2 Server Virus Protection

The Virus Signature (DAT) files should be updated as required, but no less frequently than weekly. There is an automated procedure that is part of the NetShield software, which allows the server to retrieve the latest DAT files from a distribution server. To see the current standard version of Anti Virus software, click below.

PA Server and Software Standards

In addition, the System Administrator and Business Systems Manager should review server logs daily to identify virus incidents.

6.6.3 Desktop Virus Protection

There are two ways to check the desktops both using virus scanning software. One is a full scan of the desktop that runs daily automatically after successful login to the Novell server. The standard server virus software scan generates virus logs that need to be checked manually. If a virus is found, the user should notify the Technology Services Department Help Desk immediately. Additional virus scanning software runs continuously on the desktop checking for viruses and displays a graphic alerting the user if a virus is found.

6.6.4 Virus Protection For Stand Alone and Laptop PCs and Personal Digital Assistants (PDAs)

Users of stand-alone PCs, laptops and PDAs are responsible for the virus protection of

these devices. When these devices are connected to the network, it is crucial that users follow the Port Authority's policy of allowing virus-scanning software to complete its scan before transferring any data into the network. Users of such devices should see their department System Administrator for assistance in acquiring and installing virus protection software on the device.

All users must have VShield installed on their desktops with virus scanning enabled for Internet downloads. Be aware that VShield may conflict with other software. The possibility of locking up the users' desktop exists. To see the standard version of VShield, refer to Section 6.5 (Standard Department Workstation Software) of the Technology Services Standards & Guidelines:

Standards and Guidelines for Port Authority Technology

6.6.5 Media: Diskettes (Floppy & Zip) and CD-ROMs, Portable Hard Disk Drives, Backup Tapes

System Administrators should be aware that they might need to scan any files restored from a backup tape containing data from desktops and stand-alone PCs or from any device not protected by VShield or by continuous virus protection.

6.6.6 Virus Symptoms

There are certain oddities that are known to occur in PC desktops infected with particular viruses. Some symptoms only occur once the virus is in place and the virus is triggered to perform its particular function. Others occur while the virus is still spreading. Examples of virus symptoms that users should watch for include:

File date and time stamps changing for no apparent reason

Programs taking longer than usual to load or execute

Programs or files disappearing

Programs attempting to write to write-protected media for no apparent reason

Unexplained decreases in the amount of available PC desktop memory or hard disk storage, or increases in hard disk sectors marked as "bad"

Executable files changing size for no apparent reason

PC desktops unexpectedly "rebooting" when certain previously-correct programs are run, or after a relatively constant amount of time from start-up

Unfamiliar graphics or unusual messages appearing on display screens

Unexpected changes to disk volume labels

An unusual load on local networks or other communication links.

It is important to remember, however, that future viruses may exhibit none of these symptoms. Users should be alert to any abnormalities and should report them to the Help Desk immediately. The Help Desk will notify the appropriate System Administrator who must respond within 15 minutes.

6.6.7 Incident Response

Once a computer virus is detected, the System Administrator, on the advice of the Computer Virus Response Team, should do the following even if the virus has already been removed:

An infected PC desktop should be powered off and re-booted with a virus-free floppy diskette containing a virus scan program. Booting from this virus scan diskette ensures that any "Master Boot Record (MBR)" or "memory resident" viruses have been removed. These types of viruses can infect files even after a login scan has completed on an infected machine.

In an infected network server, another scan of the network disk drives should be scheduled after active sessions have been terminated and logins disabled to ensure that all viruses have been removed. All subsequent logins should then be performed with virus scanning. Removing the viruses from infected files stored on the network disk drives should render the network server safe.

Print and review PC desktop or network server log files for use in determining the source of the infection.

If the source of infected files is determined to be a PC desktop, that desktop should be considered infected and scanned as described above.

Any infected files on floppy diskettes should be scanned and cleaned, or the floppy diskette should be destroyed. The desktop should be scanned again by rebooting with a virus free floppy diskette containing a virus scan program.

6.7 Software Inventory and Licensing

Customer departments are responsible for the accurate inventorying of all software used on all servers and desktops within their department. In addition, departments are responsible for ensuring that all software is properly licensed and that appropriate documentation is maintained as proof of license ownership.

6.7.1 Software Procurement Liaison

Departments should identify a single point of contact for internal department staff and Procurement for notification of software orders. The software liaison facilitates the processing of software orders and ensures that appropriate documentation is maintained including license cards and purchasing/invoice materials. In addition, the software liaison

ensures that the System Administrator is notified of software acquisitions and that software is only installed by authorized staff.

6.7.2 Software Installations

Software should only be installed by the System Administrator or his/her designee. Following installation of software, the System Administrator should remove the original software media and return it to the appropriate software liaison for storage and inventory. Individual users should not retain original software media, license certificates or original invoices or proof of purchase.

6.7.3 License Control

Departments are responsible for maintaining a current inventory of all licensed software including proof of license. At least once per year, System Administrators, working with the Business System Manager, should verify the accuracy of the software inventory by matching inventory lists with physical software media and purchasing records. Obsolete software should be destroyed by erasing media and records retained of the date of destruction. Questions regarding the nature of documentation required as proof of license should be directed to the department's Technology Services Department IT Coordinator.

7.0 E-mail

7.1 Systems Administrator Responsibilities

The Systems Administrator is responsible for the desktop deployment of the Port Authority's electronic mail client software, currently Microsoft Outlook 2007, and upgrading and troubleshooting of the client-side mail software as requested. The Systems Administrator should try to identify, resolve, or, if necessary, redirect desktop problems. If the Systems Administrator cannot resolve user desktop problems, he/she can contact the Help Desk/Unisys Support Desk. If the problem still cannot be corrected, he/she can contact the Technology Services Department's Messaging Group for further assistance.

7.2 E-mail Viruses

Trend Micro's InterScan Messaging Security Suite (IMSS) provides anti-virus protection for incoming and outgoing e-mail. Trend Micro's ScanMail for MS Exchange product scans incoming e-mail on the MS Exchange servers (currently at USi) for viruses, and cleans e-mails, and deletes virus-infected e-mail file attachments stored on the MS Exchange servers. The Trend Micro products, however, are not designed to clean virus-infected files on the user's computer. In addition to anti-virus functionality, IMSS and ScanMail also block e-mail file attachments with the extensions pre-defined by Port Authority's messaging policy.

In case a virus is found in an e-mail message, the Trend Micro product promptly deletes the virus and notifies the Exchange Administrator of a virus instance via e-mail message. The message indicates the name of the detected virus, the action taken, and the sender and recipient's information. If a user creates or receives an e-mail containing a virus on their desktop email client (Outlook), the desktop anti-virus software (McAfee) will detect the virus and take corrective action to clean or quarantine the virus and issue an alert to the Virus Response Team.

7.3 Outlook Responsibilities Performed by the Support Desk

Tasks performed by the Support Desk for E-mail services include the following:

- Creation of new e-mail mailboxes and associated Active Directory accounts
- Deletion/modifications of the existing e-mail mailboxes and accounts
- Resetting of Active Directory account passwords used for access to mailboxes

The Technology Services Department requires audit and security controls over the account management process and utilizes the "Request for Access to Information Systems" form PA3624A for this purpose.

7.3.1 Procedure for Account Creation/Deletion/Modification:

A request for the creation, deletion or modification of an Exchange mailbox or the associated Active Directory account requires the completion of form 3624A.

A form must be filled out for each new or changed mailbox and must be signed by an authorized departmental representative and approved by the Authority's Customer Support Manager.

The completed form is faxed to the Support Desk, Technology Services Department, Fax Number (585) 742-6584 for processing.

7.3.2 Procedure for Resetting Passwords

The Outlook (Active Directory) user ID and password is synchronized with the Novell ID and password. Therefore, customers requiring a password reset must follow the Novell account password reset procedure.

8.0 Day to Day Operations

8.1 Backup & Recovery

8.1.1 Overview

The backup schedule for Port Authority servers reflects the intent to protect data, files and electronic records stored on these servers in the event of data loss or corruption. In addition, the backup process provides for disaster recovery for servers as designated by contract.

The Port Authority approved standard software product used to perform scheduled server backups is FDR Upstream Reservoir.

> FDR Upstream Reservoir is used to create backups, on the Reservoir Servers, that will be stored remotely and managed centrally.

For the current standard version of FDR Upstream Reservoir, click below.

PA Server and Software Standards

8.1.2 Backup Scheduling

The System Administrator is responsible for ensuring that Port Authority servers are backed up and that the backup contains all data, application and system files. This must be done as follows:

> A full backup of each server to be performed weekly, bi-weekly or monthly, dependent on time constraints and the amount and type of data to be backed up. A full backup is a backup of all files on the server.
>
> Daily incremental backups of each server must be performed. The type of daily backup performed depends on time constraints and the amount and type of data to be backed up. Incremental backups are backups of all files changed since the last backup.

8.2 Testing the Restore Procedure

The System Administrator is responsible for verifying that system backups can be used to successfully restore the backed up data. It is recommended that the test restore be performed on a single non-critical directory only, not the entire server. When incremental or differential backups are routinely used, the test restore procedure should incorporate the following:

Immediately prior to performing the test restore procedure, do a special full backup on the directory being tested.

Testing a full restore should only be performed on a non-production server.

Testing should be performed at least annually.

Test results should be documented.

8.3 Patches and updates

The System Administrator is responsible for ensuring that the current Port Authority approved software and patches are installed on all desktops and servers. Security patches should be implemented as soon as possible when they eliminate or control a security exposure. To see the current approved Port Authority software, refer to Section 6.5 (Standard Department Workstation Software) of the Technology Services Standards & Guidelines:

Standards and Guidelines for Port Authority Technology

PA Server and Software Standards

An untested patch should never be applied to a production system, except when an alert is issued to correct a security exposure or to fix a condition that results in extensive loss of service. In this case, the Technology Services Department should be consulted to evaluate the risk to the Port Authority and to consider implementing the correction immediately.

8.4 Application Software

The System Administrator is responsible for ensuring that the appropriate vendor maintains the currency of custom/application software.

8.4.1 Recommended Procedure for Testing and Implementing Patches

Install patches on a stand-alone system, or in the Technology Services Department Lab, for testing and evaluation before installing in a production environment.

Use the basic functions of that software to verify that the patch does not negatively impact normal operations.

Install the patch on a non-critical production system and test again as above.

Install the patch on production systems.

NOTE: For operating system patches that will be installed on systems running nonstandard, custom, or mission critical applications, the System Administrator should check with the application vendor to verify that the patch is compatible with their software.

8.5 Adding and Deleting User Accounts

The Systems Administrator is responsible for creating new accounts and deleting inactive accounts. Appropriate documentation should be maintained by the System Administrator to verify proper authorization.

8.5.1 Creating New Novell User Accounts

User accounts are created and managed using the Novell ConsoleOne utility. Soon we will begin using Active Roles Server for user account creation.

8.5.1.1 Enter the following information about the user in ConsoleOne's Identification page:

Full Name
Last Name
First Name
Employee ID
Telephone Number and Location.

8.5.1.2 Create the Novell Login ID using the following naming convention:

Note: The Novell Login ID is the same as the user account name. All Novell Login ID's must be unique. To avoid creating duplicate Login ID's, check with *The Outlook Response Team* to verify that the proposed Novell Login ID is available for use before you create it.

Use the first initial of the first name and the full last name.

Example:	***Real User's Name***	**Novell Login ID**
	Tony Robinson	trobinson

If two users have the same name, insert the middle initial.

Example:	**Real User's Name**	**Novell Login ID**
	Tony T. Robinson	Ttrobinson

If a second user has the same name and the same middle initial, include the second letter of the user's first name:

Example:	Real User's Name	Novell Login ID
	Tony T. Robinson	torobinson

If a third user has the same name and the same middle initial, include the second and third letter of the user's first name.

Example:	Real User's Name	Novell Login ID
	Tony T. Robinson	tonrobinson

For hyphenated names, use the first initial of the first name, followed by the first initial of the first part of the hyphenated name, and then the last part of the hyphened name.

Example:	Real User's Name	Novell Login ID
	Alice Gonzales-Robinson	agrobinson

8.5.1.3 Create a Novell Template object in each container that has active (or soon to have active) users using the following parameters:

Login Restrictions

Limit Number of Concurrent Logins	Yes
Account Not Disabled by Administrator	Yes
Account Not Locked by Intruder Protection	Yes
Number of Maximum Connections	1 Connection
Inactive User ID Period	90 Days
User Station Restrictions in Use	No
User Time Restrictions in Use	Yes
User Account Expiration Dates in Use	No
Login Script Exists for All Users	No

Password Restrictions

Days between Forced Password Changes	90 Days
Periodic Forced Password Changes	Yes
Users Have Ability to Change Passwords	Yes

Grace Logins Limited	Yes
Grace Logins Maximum	3 Logins Allowed
User Passwords Required	Yes
Password Minimum Length	6 Characters
Require Unique Passwords When Changed	Yes
Password Exists for Each User Login	Yes

Security

Intruder Detection	Activated
Failed Logins Prior to Lockout	3 Failures
Minimum Login Account Lockout Time Period	1 Day 0 Hrs. 0 Mins.
Minimum Bad Login Retention Period	7 Days 0 Hrs. 0 Mins.
Parse Error Log for Login Violations	Yes
Auditing is enabled on Volumes and Containers	No
Accounting System Feature Installed	No

Group Membership

Everyone (used to assign permissions to department SHARE folders)

"U" and "S" Drive Rights

- User should have all rights to their "U" drive except for "A" access control and "S" supervisory, so users will not be able to grant rights to their home directory.
- Files should be shared only by using the Share, ("S") drive.
- Access to a user's home directory, by anyone other than the owning user is prohibited.

Share Drive/Folder Structure

- The Share folder will include three subfolders, one called "Projects", one called "ORG", and one called "Everyone".
- All departmental projects will be kept in the "Projects" folder. Projects folders will be created and have user rights assigned by a group having the same name as the project. Only staff requiring access to project files should be granted rights to a specific project folder.

- Under the Projects folder will be two folders, one called "Active" and one called "Completed". Active projects reside in the "Active" folder.
- When staff identify a project as "Completed", the project folder will be moved to the "Completed" folder and all rights, except for Read and FileScan, will be removed from the folder. This will ensure that the final project documents remain unchanged, while still allowing staff to review the old documents and use them as templates for new documents if desired. The "Completed" folder will be set to archive its data.
- Under the "ORG" folder will be subfolders with names corresponding to the various divisions within the department. By default, only staff within a division will have access to a division's folder. These folders are intended to hold data for a specific division that would not normally be shared departmentally. Staff from other divisions would not have access to these folders unless the division manager of the owning division gives their approval.
- The Systems Administrator, at the direction of the Director, may from time to time remove any data deemed to be non-business related.
- A folder called "Everyone" will be created in the Share folder. All staff in the department will have full access to this folder to store and retrieve files that are not related to a project or a division's day-to-day operations.
- Additional shared folders, with access restricted to only specific users, if required, will be created in the Share folder. Access will be restricted through the use of Novell Inherited Rights Filters and access will be granted through the use of groups. These groups will be named using the same name as the folder name.
- In general, rights to any folder will be granted through the use of a group having the same name as the folder. The group would have trustee rights to the folder, and users would be added to or removed from the group as needed.
- All rights would be granted or revoked through the use of form PA-3624A. Designated staff in each department are required to approve these requests.

8.5.2 Explanation of Technology Services Department Standard User Account Parameters

8.5.2.1 Concurrent Logins

It is Port Authority policy to limit Login sessions to one (1) connection per user to avoid unauthorized access to the system.

8.5.2.2 Intruder Detection

It is Port Authority policy to activate the system-monitoring feature using the following parameters in order to curb unauthorized users from guessing a user's password.

Set the system to lock out the account after 3 incorrect login attempts.

Set the lock out period to 7 days after which time the login will be re-enabled.

8.5.2.3 Passwords

All user accounts must have a password according to the following rules.

The password must be at least six (6) characters.

Passwords should be a combination of letters, numbers and special characters.

The password should not be easily guessed.

Passwords should not be written down.

The password should be set to expire after 90 days.

Passwords for sensitive and high privileged accounts should have 8 or more characters and should be changed at least every 60 days.

Grace logins should be activated and limited to three.

Users should be notified several days in advance of password expiration.

Users should be forced to change their password on initial login and once it expires.

Unique passwords should be required. Users should be prevented from reusing a previous password for a minimum of one year.

Passwords should be encrypted in storage.

Passwords used in system startup files and login scripts must be encrypted.

Servers should be protected by using a screen saver password. The recommended time-out period is 15 minutes.

For certain users, where security is an issue, protect with a short boot –up password during power on.

8.5.3 Deviations from Technology Services Department Standard User Account Parameters

The department Business System Manager must approve any deviations from the above Technology Services Department standard user account parameters. The approval of any deviations should be documented and maintained on file.

8.5.4 Inactive User Accounts

Dormant accounts must be removed because unauthorized use of these accounts would go unnoticed. Inactive accounts as noted in the Audit Report should be disabled after six (6) months and removed from the system after one (1) year.

8.5.4.1 Deleting Inactive User Accounts

The form PA3624A, *Request for Access to Information Systems* is used to request deletion of a Novell or an e-mail account:

Accounts are also deleted based on information contained in the *Terminations and Transfers Report*, distributed weekly by TSD.

8.6 Login Script

A Novell Login Script is a list of commands that are executed after a user successfully logs into the network. There are three types of login scripts: the container, user and default login scripts. For security reasons, and ease of administration, only the container login script is used.

The Container Login Script is used to set environment variables, drive mappings, automate software distribution, and initiate other programs. These programs typically include hardware inventory, checking the local PC for viruses, and e-Mail profile manipulation. All container Login Scripts should end with an EXIT command to prevent unauthorized User login scripts from executing. Caution should be exercised when using the EXIT command, however, since placing this ahead of necessary mappings could render the system unusable.

Drive mapping should be performed in the container login script as described in Drive Mapping Conventions. Comments should be noted at the top of each Novell login script, including the date of the change, a description of the change and the Sys Admin name.

8.7 Guest Account

The Guest account is automatically created when Microsoft Windows is installed. Leaving this account active on servers has proven to be a security risk. For this reason the account should be disabled on all servers and renamed to "Cherokee".

8.8 Administrator Accounts

The default Administrator (Novell & Microsoft Windows) accounts should not be used for daily administration activities. The Microsoft Windows Administrator account should be renamed to "Comanche". The password should be stored in a secure location. These accounts should be used only for special situations that require rights to the entire tree or server. When the Administrator account is used, its password should be changed and returned to its secure location.

For audit trail purposes, System Administrators should have and use their own unique accounts. The preferred naming convention for these accounts is a leading "a" (for

admin) followed by the standard first initial and last name of the user. These accounts should have all the privileges an administrator would need to perform the required tasks for the containers being administered.

Novell refers to these accounts as Supervisor-Equivalent accounts. Supervisor-Equivalent accounts should be created for System Administrators only.

8.9 Granting User Access to Windows Network Resources

The process for granting access to a user for a specific resource is as follows:

1. The local Application Administrator requests that the account domain (PANYNJ) System Administrator in the Technology Services Department create a Global Group for particular access to that resource. The form PA3624A, *Request for Access to Information Systems* is used to request access to Windows network resources:

   The account domain System Administrator will adhere to the following naming convention to create the group for that application.

   > Example: Access to the application named Rbase.
   > Group Names: *Rbase Users (read-only access), Rbase Admins (read-write access).*

   Note: NT Global Groups are limited to 20 characters and they cannot be renamed.

2. The Local Application Server Administrator requests that domain user accounts be added from the Master Account Domain PANYNJ into the appropriate Global Group.

3. The Local Application Administrator creates a Local Group at the application Server where the resource resides.

   > Example: New Local Group "Rbase Users" is created on TELEAS04, which is a member of the PARES Resource Domain (which trusts the PANYNJ account domain).

4. Local NTFS permissions are assigned to the Local Group created by the Application Administrator.

   > Example: The Read permission is granted to TELEAS04\Rbase Users for the directory D:\Rbase.

5. Local System Administrator adds correct Global Group into the Local Group on the server.

   > Example: Local System Administrator adds the Global Group PANYNJ\Rbase Users into the Local Group TELEAS04\Rbase Users.

6. Ongoing administration is handled locally, by the local application server administrator and enterprise-wide by the Technology Services Department domain administrator.

> Example: Every time a new user requires access to Rbase, the Application Administrator requests that the domain System Administrator place the newly named application user's user object in the Global Group PANYNJ\Rbase Users.

If new permissions are required for access, the local System Administrator has the ability to change them.

8.10 Application Software Support Activities

The System Administrator, assisted by a desktop support specialist, will support all Port Authority standard software. He/she will work with applications support and the associated vendor when necessary.

8.11 Change Reporting

System Administrators are responsible for participating in the weekly Change Management meetings

System Administrators are responsible for reporting to the Technology Services Department Standards all changes pertaining to:

Departmental hardware:

- Servers
- All network connected devices, such as:
  - Printers
  - Print servers
  - Scanners
  - Network Interface Cards

Software:

- Network Operating Systems, Desktop Operating Systems, standard applications, including:
  - Upgrades
  - Service packs
  - Patches
- Non-standard operating systems
- Non-standard applications

8.12 System Monitoring

The System Administrator is responsible for monitoring servers and clusters to ensure that:

Volume storage space being utilized does not exceed 80%

Percentage of processor utilization does not reach 100% for an extended period of time, defined as 20 minutes or longer.

On Unix machines, ensure that system and application processes are still active and check /var/adm/messages for hardware or software error messages and application logfiles for application error message

In addition, the System Administrators are responsible for installing Port Authority standard server monitoring software. This software will automatically detect potential hardware failures and send a notification to the responsible System Administrator, allowing him/her to address problems before they cause system downtime.

8.13 Server/eDirectory Maintenance Procedures

8.13.1 Server Outage Notifications

The following email distribution list has been created for notification of any unplanned server outages:

DL - TSD - Network_Server Outage

This list of users must be notified of any service interruption as soon as possible after the incident.

8.13.2 Server Reboot Procedures

Server reboots will be performed according to the standard Port Authority procedures:

8.14 Systems Administrator Resources

Links to web sites that provide useful information to System Administrators:

Compaq/HP Tech Support HP Tech Support Website

Dell Tech Support	http://support.dell.com/
IBM Tech Support:	http://www.ibm.com/support/us/ http://www.pc.ibm.com/us/eserver/xseries/library/configtools http://www.redbooks.ibm.com/
Network Associates:	http://www.nai.com/
Novell Tech Support	http://support.novell.com/
Microsoft Tech Support	http://support.microsoft.com/
ARCserve Support:	http://supportconnect.ca.com/

9.0 Desktop and Enterprise Application Support

Technology Services Department's Support Desk is the primary source of troubleshooting and support for desktops. This includes assisting users in installing, configuring and maintaining hardware and software applications. Where required, additional support is available from the Technology Services Department Senior LAN Engineers (SLE), System Administrators and the Port Authority contractor for hardware maintenance.

9.1 Desktop Inventory

All computer related hardware, including printers must be maintained in the Port Authority's (PA) PC inventory. Tivoli is the standard inventory database for all managed PC assets within the PA. It contains employees, departments and location information, and works in conjunction with a client-based auto discovery tool called Peregrine Desktop Inventory (PDI).

PDI performs periodic scans on all PCs on the Port Authority Wide Area Network (PAWANET) using the Asset Tag as a unique identifier, and reports hardware characteristics, software installations and configuration information. When the scan files are loaded into the Tivoli database and a match is found, the records are automatically updated with current information. This data is used to generate our monthly inventory reports.

9.2 Desktop Operating System Standard

The Port Authority's standard operating system for desktops is Microsoft's Windows. In limited circumstances, where business objectives warrant, alternative operating systems may be deployed with the approval of the department director and concurrence of the Chief Technology Officer.

9.3 Desktop Configuration

9.3.1 Desktop Naming Conventions

All departmental PC desktops, laptops and CAD workstations should conform to the following naming convention, regardless of the operating system being used. The Computer Name must be identical to the computer manufacturer's serial number.

9.3.2 Desktop User Accounts

Windows desktop users should have Microsoft Active Directory domain user accounts

that correspond to their Novell NetWare identifications. All Microsoft Windows workstations should include at least one local login account with local administrative privileges. Only the TSD support personnel should use the local administrative account for workstation maintenance.

9.3.3 Remote Desktop Management

The Port Authority also distributes software applications and upgrades via Novell's ZENworks. Each workstation must have Novell's Desktop Management module installed as part of the NetWare Client. This will enable remote software and application distribution software updates, hardware inventory and workstation troubleshooting. The current version and configuration settings for ZENworks are accessible from the link below in Section 6.5 (Standard Department Workstation Software) of the Technology Services Standards & Guidelines:

Standards and Guidelines for Port Authority Technology

9.3.4 Drive Mappings

Workstation drive mappings and drive pointers to shared network storage are accomplished exclusively through the Novell NetWare login script. Local drive mappings on the desktop are not supported.

9.4 Standard Department PC Desktop Software

The following software is the standard Port Authority software for departmental workstations. New computer installations should conform to the existing standard. Previous installations may use the alternate standard until they are replaced or upgraded.

Because technology is rapidly changing, Section 6.5 (Standard Department Workstation Software) of the Technology Services Standards & Guidelines should be consulted to obtain the most recent versions of standard software.

Standards and Guidelines for Port Authority Technology

Department directors should establish appropriate internal approval processes to authorize the purchasing and use of nonstandard software. Nonstandard software should only be used where there is a compelling business justification and done in consultation with the department's Technology Services Department customer technology manager.

9.5 Enterprise Software

The sections below describe the standard Enterprise software.

9.5.1 PeopleSoft

Users requiring access to the Port Authority's Human Resources – Payroll System (PeopleSoft) must have the Internet Explorer web browser installed on their desktop. No other client software is required.

9.5.2 SAP

Users requiring access to the Port Authority's financial and procurement system (SAP) must have the current client installed on their desktop. System administrators are responsible for installing appropriate components on the user's desktop as well as maintaining current application files on the network server for use.

9.5.3 Microsoft Outlook and Exchange

The standard Port Authority client to access e-mail is Microsoft Outlook. Technology Services Department Support Desk and Senior LAN Engineers are responsible for installing Outlook and configuring the client through the use of a pre-configured profile.

9.5.4 eNet

The Technology Services Department Support Desk and Senior LAN Engineers are responsible for installing and configuring the Internet browser to access the Port Authority's employee Intranet.

9.5.5 Other Business Applications

Other Enterprise applications are deployed on occasion to user desktops. This includes systems like the Business Expenses system and others. Technology Services Department Support Desk and Senior LAN Engineers are responsible for deploying the desktop clients and network server software according to standards and directions provided by the Technology Services Department.

9.6 Workstation Security

Workstation users and their managers are responsible for the security of computer equipment and safeguarding critical corporate data and access to Port Authority's network resources. This includes both the physical securing of equipment as well as the logical safeguarding of equipment and data.

9.6.1 Physical Security

The method of control should be based on the value of the equipment, the sensitivity of the data, its portability and the degree of exposure to theft. All workstations and laptops should be physically secured with a cable and lock. In addition, it is recommended that PC desktops be assigned a coded theft recovery ID.

9.6.2 Logical Security

Port Authority departments are responsible for providing for the security of computer resources and devices:

For certain users, where security is an issue, workstations should be protected with a boot-up password during power on.

Screen saver passwords should be implemented with a maximum of a fifteen (15) minute time-out.

All critical data should be backed up nightly onto either exterior media or a network drive.

9.7 Port Authority Help Desk/Pomeroy Support

Please refer to the Port Authority Help Desk and Pomeroy Support sections (currently Sections 6.8 and 6.9) of the TSD Standards and Guidelines for responsibilities, hours of staffing and escalation procedures:

Standards and Guidelines for Port Authority Technology

9.8 Network Problem Notification

CNS (Computer Network Solutions) monitors the Port Authority's Wide Area Network (PAWANET) under the supervision of the Office of Technology Infrastructure – Network Operations. CNS notifies the appropriate PA staff, via email and telephone, of any outage of key communication links in PAWANET.