



The Port Authority of New York & New Jersey

Information Security Handbook

October 15, 2008, corrected as of November 14, 2013

The Port Authority of New York and New Jersey
Information Security Handbook

Copyright © 2008, 2013 The Port Authority of New York and New Jersey
No copyright is claimed in the text of U.S. regulations or statutes quoted within.

TABLE OF CONTENTS

	<u>Page</u>
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	11
3.5 NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENTS (NDAs)	11

3.6 UNAUTHORIZED DISCLOSURE OF INFORMATION	12
3.7 SECURITY CLEARANCE AND ACCESS PROHIBITIONS	12
3.8 BACKGROUND SCREENING	12
3.9 AUTHORIZED PERSONNEL CLEARANCE LIST	13
3.10 DEVELOPMENT OF CONFIDENTIAL INFORMATION PRACTICES AND PROCEDURES (CIPP).....	13
3.11 PROCUREMENT STRATEGIES	14
 CHAPTER 4	
MARKING, HANDLING, STORAGE, TRANSMITTAL AND DESTRUCTION REQUIREMENTS.....	17
4.1 MARKING OF PROTECTED INFORMATION.....	17
4.2 HANDLING PROTECTED INFORMATION.....	19
4.3 TRANSMITTAL OF PROTECTED INFORMATION	19
4.4 STORAGE OF PROTECTED INFORMATION	22
4.5 DOCUMENT ACCOUNTABILITY LOG.....	22
4.6 REPRODUCTION	23
4.7 DESTRUCTION OF PROTECTED INFORMATION	23
4.8 INFORMATION TECHNOLOGY SYSTEMS HANDLING OF ELECTRONIC INFORMATION /DATA	24
4.9 TRANSMISSION/EXCHANGE OF ELECTRONIC INFORMATION	24
4.10 ELECTRONIC STORAGE	25
4.11 USER ACCESS DEACTIVATION	26

CHAPTER 5

AUDITING AND MONITORING 27

5.1 PURPOSE..... 27

5.2 AUDITS AND INVESTIGATIONS..... 27

5.3 SELF-ASSESSMENT..... 28

CHAPTER 6

POLICY VIOLATIONS AND CONSEQUENCES 29

6.1 RESPONSIBILITIES 29

**6.2 VIOLATIONS, INFRACTIONS, OR BREACH OF
 INFORMATION SECURITY PROTOCOLS 29**

**6.3 VIOLATION REPORTING, INVESTIGATION AND FACT
 FINDING 29**

6.4 DISCIPLINARY ACTION..... 29

CHAPTER 7

**INFORMATION SECURITY EDUCATION AND AWARENESS
TRAINING 31**

7.1 PURPOSE..... 31

7.2 OVERVIEW..... 31

7.3 TRAINING PROGRAM ELEMENTS 31

APPENDICES OF HANDBOOK

A - PROTECTED INFORMATION

B – NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENTS

B-1: Non-Disclosure and Confidentiality Agreements with reference to Handbook

B-2: Non-Disclosure and Confidentiality Agreements without reference to Handbook

B-3: PA/PATH Employee Non-Disclosure and Confidentiality Agreement

C – BACKGROUND SCREENING CRITERIA

D – THE SECURE WORKER ACCESS CONSORTIUM (SWAC)

E – COVERSHEET FOR CONFIDENTIAL PRIVILEGED INFORMATION

F – TRANSMITTAL RECEIPT

G –GUIDELINES FOR THE STORAGE OF PROTECTED INFORMATION

H- GUIDELINES FOR THE DISPOSAL AND DESTRUCTION OF PROTECTED 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 Protected 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 of Information Code (Code), inasmuch as it further defines certain information that may be exempt from release under the Code. The guidelines contained in this Handbook are not intended to, in any way, be in derogation of the FOI Code adopted by the Board in March 2012. The Code continues to provide open, timely and uninhibited access to the Port Authority's (and its subsidiary corporations') public records and reflects the New York Freedom of Information Law ("FOIL") and New Jersey's Open Public Records Act ("OPRA"). . This Handbook prescribes requirements and other safeguards that are needed in order to prevent unauthorized disclosure of Protected 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.

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, Protected 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:

Chief 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 Director of Technology Services Department 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.

Corporate Information Security Officer (CISO) – the CISO reports directly to 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 Code; 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.

Director of Technology Services Department– is the head of the Technology Services Department (TSD). The Director of TSD, or the Director'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 Director of Technology Services Department 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. The OIG's Security Inspection Division is responsible for conducting investigations, inspections, reviews, and audits pertaining to all Port Authority security programs in all departments. It should be noted that cases involving investigations are exempt from CISO approval.

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 Director of Technology Services Department. 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) **“Information”** means, collectively, all 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.

(b) **“Protected Information”** means and includes collectively, Confidential Information, Confidential Privileged Information, Sensitive Security Information (SSI), Critical Infrastructure Information (CII) or Health Insurance Portability and Accountability Act (HIPAA) 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 Protected 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 Protected.

(c) **“Confidential Privileged Information”** means and includes collectively Information that reveals security risks, threats, vulnerabilities, documentation that identifies specific physical security vulnerabilities or revealing specific security vulnerabilities details related to emergency response protocols, egress plans, flow paths, egress capacities, (diagrams, codes, standards) etc., which is not publicly available.” and 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.

(d) **“Confidential Information”** means and includes collectively, 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. It also 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 Code. It also includes sensitive financial, commercial and other business information received from third parties under Non-Disclosure and Confidential Agreements.

(e) **“Health Insurance Portability and Accountability Act (HIPAA)”** Employees, associates or other contract personnel who have access to Protected Health Information (PHI) must refer to, and comply with, the Privacy Policies and Procedures to Protect Personal Health Information. Privacy regulations issued under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA” or “Privacy Laws”) place restrictions on the Group Health Plans of the Port Authority and PATH (the “Plans”) ability to use and disclose Protected Health Information (“PHI”).

(f) **“Attorney Work Product”** Attorney work product and other privileged information should be protected and treated in accordance with the established rules of the legal profession and may carry the label “Privileged & Confidential” or “Attorney Work Product”. Certain attorney work product information may also fall within the definitions of Confidential Privileged and/or Confidential Information as established by the Handbook, and as such, should be marked and treated in accordance with the Handbook and the Law Department CIPP.

(g) **“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.

(h) **“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.

(i) **“Non-Disclosure and Confidentiality Agreement”** (NDA) refers to the Agreements attached hereto as Appendix “B” (which include Appendices B-1 through B-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.

(j) **“Non-Disclosure Instructions”** (NDI) refers to the instructions attached hereto as Appendix “C.” 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.

2.2 General Process for Categorization

As defined hereinabove, the term Protected Information includes all Port Authority Information protected pursuant to this Handbook or as governed by statutory regulations. Any sensitive Information not specifically deemed Confidential Privileged Information should be categorized as Confidential Information. In addition, certain other types of Protected Information, such as HIPAA, 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 Protected Information, unless otherwise specified. Where a different or additional requirement applies to a specific sub-category of Protected Information, it will be noted.

Each DISO, in consultation with the CISO, shall create a list of examples of Confidential 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, SIM, supervisors, managers or the CISO, as may be appropriate, should take the action needed to process the Protected 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 Protected Information. If management, employees, consultants, third-party contractors, or other agency personnel determine that Information under review contains Protected Information, the Protected 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 DISO or SIM, where applicable, and the unit supervisor of the group/entity proposing the categorization.
2. Obtain DISO concurrence and approval.
3. Obtain CISO approval (except in the case of the PA OIG).
4. If approved, mark and label the information, and, if appropriate, apply a cover sheet (See Appendix F).

If Information has been nominated for Confidential or Confidential Privileged 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 or Confidential Privileged Information for the same project or task.

2.3 Training and Information Review

Port Authority managers, including, but not limited to, the DISO, SPM and the SIM will complete training. This enables them to conduct a continuing review of Protected Information under their control in order to identify and categorize it as Confidential or Confidential Privileged Information. Employees, consultants, third-party contractors or other agency personnel must participate in and complete the Policy training, which enables them to continue the process of review, identification, and categorization of Protected Information.

Each Department Director will determine which staff members in the respective department require Policy training and will do so on an ongoing basis. When access to Protected 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, Protected Information may no longer be considered Confidential or Confidential Privileged, 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 Protected 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 Protected Information must adhere to the requirements set forth in this Handbook.¹ Protected 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 Protected Information and/or other contractual, civil, administrative or criminal action.

All employees, consultants, third-party contractors, individuals and/or entities given access privileges to Protected Information are responsible for overseeing the safeguarding and protection of Protected Information in their possession or under their control as per this Handbook's requirements. Questions concerning the safeguarding, protection, release, and/or access to Protected 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 certain Protected Information to be considered for approval, all individuals including PA staff, must meet and complete the following criteria, unless otherwise required under federal or state regulations:

- 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 OIG and/or the CSO where and when circumstances so require.
- Obtain sponsorship for a request to be given access to Protected 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. (OIG is exempt from this)
- Forward the request through the individual's supervisory chain to the CISO, "(except in the case of the PA OIG) , via the appropriate DISO, SPM, or SIM, requesting that a specific background check be undertaken, where appropriate and/or required.
- Background check required to access CP information and/or accessing a PA Facility that requires background screening."
- Complete the Port Authority Information Security Education and Awareness Training.

¹ The CSO and/or the OIG 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.

- Execute a Port Authority NDA (See Appendix B), or an Acknowledgement of an existing executed NDA, and, if the individual is Port Authority represented staff, have been provided with the NDI. Consultants or third party need's to designate a Security Information Manager (SIM)
- 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, or Port Authority Authorized Personnel Clearance List for access to Confidential and/or Confidential Privileged Information. 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 Protected Information, since access is conditioned on need to know criteria. The OIG may access, without approval of the CISO, DISO, SPM or SIM, all Protected 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 Protected 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) Protected Information

Access to Protected Information shall be on a need to know basis only, as determined by the DISO. In certain limited instance's access, privileges may be conditioned on the satisfactory completion of a background investigation(s). The background investigation, if warranted, 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 certain Protected Information, such as Confidential Privileged, and/or Confidential Information, requires that the parties execute a NDA or an Acknowledgment of an existing NDA if the CISO or OIG determines that a NDA and/or Acknowledgment is required.

(i) 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 execute a NDA or an Acknowledgment of an existing NDA if the CISO or OIG determines that a NDA and/or Acknowledgment is required.

(ii) Confidential Privileged Information

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 Confidential Privileged 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 is subject to the satisfactory completion of a background investigation for non-Port Authority individuals and to continuing periodic checks. A list of disqualifying crimes for the different levels of background screening is attached as Appendix "D." A more stringent background investigation may be required of the individual for access to certain Confidential Privileged Information if determined by the DISO. 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 DISO. 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 the case of certain represented employees/individuals, and in some cases NDIs may be utilized in lieu of NDAs upon the approval of the CISO.

3.4 Access Disqualification

Any employee, consultant, third-party contractor, or other individual and/or entity, who has been granted access to Protected 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 Protected Information, or disclosed, disseminated, or released Protected Information to an unauthorized individual or entity. Further, access to Protected Information can be denied when improper or incomplete verification checks of employees, entities, or individuals are discovered. In addition, if an individual's SWAC has expired, or access level has changed that individual may no longer have access to Protected Information.

Where it is determined that an individual has misused, mishandled or otherwise improperly disclosed, released or disseminated Protected 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, OIG, 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 and/or Confidential Privileged Information, except in the case of certain Port Authority employees and third parties where a NDI may be utilized in instructing and advising the Port Authority employee and/or third party of the obligations and the requirements for handling Confidential Information. 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. The DISO is responsible for determining whether a NDA/NDI is required as a condition to being granted access privileges to certain Protected Information, other than Confidential Privileged Information. If an individual refuses to execute an individual Acknowledgment, PA Employee NDA or to receive the NDI, if it is deemed required by the DISO, CISO or OIG, access to the certain Protected Information must 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 PA DISO and Third Party SIM. Original executed NDAs shall be forwarded to the CISO, by the DISO, for filing in the official Port Authority records repository, with a copy to Law Department DISO.

3.6 Unauthorized Disclosure of Information

If employees, consultants, third-party contractors, or other individuals and/or entities with authorized access to Protected Information become aware that Protected Information has been released to unauthorized persons, lost, stolen or compromised, they are required to immediately notify the DISO, 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 of SSI or CII.

3.7 Security Clearance and Access Prohibitions

Access to Protected Information is not a right, privilege, or benefit of contracting with or employment by the Port Authority, rather it is based on pre-established guidance. Protected 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 DISO, CISO or OIG. The following security clearance and access guidelines and/or prohibitions are in effect to protect Protected Information:

- Protected 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 or OIG. No other disclosure or use of Protected Information is authorized.
- Individual access to Protected Information will be rescinded when an employee, consultant, third-party contractor, individual or entity, who had been granted access to Protected 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 Protected 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 Protected Information should be prohibited. Each individual in a group must have security clearance to access Protected Information.
 - Persons who rarely, if ever, require access to Protected 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

In order to determine if any individual poses a potential security threat to the Port Authority or its Facilities, the Port Authority requires background screening to verify the personal identity of, and determine the criminal history of, all contactors and consultants working in secure areas at Port Authority facilities or handling security related Protected Information. As such, employees of third party contractors/consultants requiring access to certain Protected Information relating to security on a specific project must obtain clearance through a background check prior to being provided access to information unless otherwise waived in writing by the CISO or OIG. This

includes all individuals working on the project, including administrative and back-up staff that have access to and/or are handling Confidential or Confidential Privileged Information.

All background checks for third parties required under the Policy should normally be conducted through the "Secure Worker Access Consortium" (SWAC), 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 three years, at the end of which the member must renew the 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 or OIG.

The DISO/SIM 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 "E."

In some cases TSA's Transportation Workers Identifications Credentials (TWIC) or Security Identification Display Area (SIDA) background screening and credential may be used in lieu of the SWAC process with approval by the DISO.

3.9 Authorized Personnel Clearance List

The DISO 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 SIM to ensure that the list is current and that each individual's access to Protected Information is still required. 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 Protected Information.

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 Protected 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 Protected 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 Protected 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 Protected Information is discovered thereafter by Procurement, or any reviewing department, the originator's department manager or designee should be contacted immediately to retrieve the Protected 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 Protected 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, general contractors, 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 consultant, prime vendor, general contractor or commercial enterprise 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. Consultants, Prime Vendors, General Contractors, or Commercial Enterprises should contact the Port Authority to request authority prior to releasing RFP Protected 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 certain Protected Information to undergo background pre-screening. The pre-screening may parallel the screening requirement used by the Port Authority to grant access to Protected 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 Protected Information procurements or projects to designate a SIM to ensure information security and Protected Information requirements are followed. A second employee may be designated as an alternate SIM. All SIM's will be required to get SWAC'd.

(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 Protected Information to ensure that the storage and protection of Protected 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 Protected Information consistent with the handling procedures set forth in Chapter 4 of this Handbook.

(vii) Website Restrictions. Prohibit posting, modifying, copying, reproducing, republishing, uploading, downloading, transmitting, or distributing Protected Information on unauthorized 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 Protected 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/Subconsultants. Require the prime vendor, general contractor, or consultant to mandate that each of its subcontractors/sub consultants maintain the same levels of security required of the prime vendor, general contractor, or consultant under any Port Authority awarded contract.

(x) Publication Exchanges. Prohibit the publication, exchange or dissemination of Protected Information developed from the project or contained in reports, except between authorized vendors, subcontractors and subconsultants, 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 Director of Technology Services Department 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 Protected 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 Protected 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 Certain Protected Information

(a) Confidential Privileged and Confidential Information

All documents, drawings, and all other Information that contain Confidential Privileged, 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 or equally visible typeface.

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 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 visible typeface 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 Protected 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 Protected 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:

CP – LAW – 13 – 1 – 1

CP – 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. If deemed necessary by the DISO or CISO, certain Confidential Information or other Protected Information may be given a control number.

4.2 Handling Protected Information

Handling refers to the physical possession of, and includes working on or with, Protected 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. Protected 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. Protected 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 Protected Information, and certain requirements that apply only to Confidential Privileged and Confidential 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 Protected Information

Transmission refers to the sharing among individuals and/or entities, and/or the transfer or movement of Protected Information from one location to another using either physical or electronic means. The following chart sets forth the methods by which Protected Information should be transmitted. In all instances, Protected 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 DISO or SIM, 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 “F” 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 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 Protected 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 Livelink ² or a similar approved secure repository	X	
Electronic Mail: restricted from using e-mail accounts to transmit. NOTE: Confidential Information may be transmitted using encryption with express permission by the DISO/SIM, in writing	X	
Hand Carried or delivered in the personal custody of Authorized Individual: (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	X (b and c only)
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		

² Livelink is a secure collaborative repository for the documents of a project.

exterior of a 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 non-land line 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 mobile or internet devices.	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 secure binding to prevent individual sheets from being removed from a set.

4.4 Storage of Protected Information

Steps should be taken to prevent unauthorized access to Protected Information. Certain Protected 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. Protected Information should be gathered and stored in a minimum number of office locations. Confidential Privileged Information must never be left unattended outside its storage location for long durations. A storage space or security container/receptacle may not be left open and unattended at any time. At no time should Confidential Privileged or Confidential Information be stored, except for short periods during work, 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, leaves the project 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 combinations of locks utilized to secure certain Protected Information must be safeguarded at the same level of protection as paper documents. The "Guidelines for the Storage of Confidential Privileged, Confidential and Law Enforcement Confidential Information" attached as Appendix "H" 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 written authorization of the SIM or DISO.

Downloading of any Confidential Privileged Information and Confidential Information carries with it the responsibility to protect 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, transmittal and disposal of this Confidential Privileged and Confidential Information.

4.5 Document Accountability Log

All entities, Port Authority Departments and third-parties having Protected 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 with respect to Confidential Privileged and Confidential Information 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 Document Destruction Certification, 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

Protected 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 Protected 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 Protected 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 Protected Information

All Protected 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. 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 Document Destruction Certificate must be provided to the DISO or SIM for any document being destroyed, including original or copies thereof. 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 Protected Information is no longer needed, but the Port Authority Records Program requires retention of the original, the original Protected document shall be retained by the Departmental Records Coordinator 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 "I" provides further detailed information and instruction.

Since deleted electronic files can be recoverable by utilizing software tools, certain Protected 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 Protected Information be permanently removed from a computer. This request shall be made by providing relevant information on a TSD Service Request (TSR), found on eNet on the TSDpage.

4.8 Information Technology Systems – Handling of Electronic Information/Data

All transmission, storage and destruction of all electronic information and data must be in compliance with the Technology Services Department's (TSD) "Cyber Security Guidelines for the Port Authority of New York and New Jersey"

Information Technology (IT) Systems that are used to electronically capture, create, store, process or distribute Protected Information must be appropriately managed to protect against unauthorized disclosure of the contents. The main objectives of these electronic handling guidelines are to:

- Provide access exclusively to the authorized individuals.
- Compartmentalize Protected Information as required by a Department's CIPP.
- Complete removal of Protected Information from the system when it is no longer needed.

This section is intended to describe the processes used to control secure electronic data, and is to be implemented for the control, processing, handling, storage, and destruction of all "Protected" electronic data as generated, received, or distributed by Authority staff, consultants, contractors or third parties.

4.9 Transmission/Exchange of Electronic Information

The Authority uses Livelink (moving toward PACS) as its project and program website solution to collaborate with team members (i.e., authorized individuals) both inside and outside the Agency's firewall. Additionally, the Authority also uses secure internet websites with secure transmission to collaborate with team members outside the Agency. The use of a web-based collaboration tool has numerous benefits that result s in time and cost savings, accountability, security, and disaster recovery. For example, within the Authority, the Downtown Restoration Program (DRP), the Security Capital Program, Office of Emergency Management, and the Goethals Bridge Program, utilize Livelink website collaboration.

Access to these password-protected websites is controlled by permissions that apply to each individual user account. In this manner, users are allowed to access folders and files only when approved by the SIM, Project Manager or Program Manager directly responsible for the information.

With these measures in place, the Authority has deemed that all electronic exchange of Protected Information must be accomplished using a secure project website solution with centrally managed access control on a per individual basis and with encrypted transfer.

Although the entire Port Authority Website is secure, in order to provide better organization and auditing of files that contain Confidential Privileged or Confidential Information, special secure folders must be created and maintained specifically to house this information. Information that has been designated as Confidential Privileged Information may only reside in these secure folders in order to further compartmentalize it from other types of information.

Additional secure Protected Information folders will allow other files such as reports, presentations, etc., to be stored.

In addition to the Livelink website, certain electronic Protected Information may also be shared via secure Local Area Networks (LAN). Protected Information should be removed from the LAN as soon as the recipient has acknowledged receipt of the information. As with the website, these LANs are password protected, and access to them is only for those individuals who have signed the NDA and are provided with permission by the SIM or DISO, if required.

E-mailing of Confidential Privileged Information is not permitted, E-mailing of any other Protected Information must be encrypted as per TSD standards.

4.10 Electronic Storage

Technology advances allow increasingly larger amounts of information to be stored on increasingly smaller devices. This creates a greater risk of information security breaches due to the size and portability of these devices, which can be lost or misplaced more easily when taken outside of the office. If a situation arises whereby electronic files must be exchanged by electronic media such as flash drives, CD or DVD, all provisions within this manual for handling physical documents must be satisfied.

Possession of Protected Information in any format (hardcopy, electronic, photo, video, etc.) carries with it the responsibility to protect that information in accordance with the requirements of the Handbook. Authorized individuals in possession of electronic files containing Protected Information assume full responsibility for the proper handling, storage, transmittal, and destruction of this type of information in the same or comparable manner as hard copy requirements.

Users who possess electronic files containing Protected Information shall adhere to the following guidelines to maintain the proper protection of this material:

Desktops/Laptops/CAD Machine Users

Individuals granted access to The Port Authority Network or information systems shall secure computers from unauthorized access.

- When leaving a computer unattended, users shall apply the “Lock Workstation” feature (ctrl/alt/delete, enter).
- Unattended computers shall be secured from viewing by password protected screen savers.
- Computers shall activate the automatic screensaver feature after a period of non-use. The period of non-use is fifteen (15) minutes, or a shorter time period if required by a DISO.
- Desktop computer users shall only store Confidential Privileged and Confidential Information on a secure password protected network drive (directory on The Port Authority Network) and not the computer’s local hard drive.
- Laptop computer users shall store Confidential Information locally, when necessary, with encryption software. Users shall contact their respective DISO to request or confirm that Port Authority standard encryption technology is installed on their assigned laptop computer.
- Computer users shall not disable or alter security safeguards, such as virus detection or encryption software, installed on Port Authority computers.

Portable Media

- Confidential Privileged Information shall be encrypted on portable devices, including handheld devices, if they are carried outside secure worksites.
- All Protected Information stored on portable devices shall be password protected at the document level.
- Mobile laptop computers, computer media and any other forms of removable storage (e.g., diskettes, CD ROMs, flash drives) shall be stored in a secure location or locked cabinet when not in use.

4.11 User Access Deactivations

In addition to accessing the IT Systems, Port Authority, through the appropriate Systems Administrator, may deactivate a User's IT privileges, whether or not the user is suspected of any violation of this Policy, when necessary to preserve the integrity of facilities, user services, or data.

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, Audit, and/or OIG 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 "J", 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 Protected 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, Protected Information material sign out and sign in records, where appropriate, 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 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 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 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 CISO, OIG, their DISO, and third party SIM, who shall in turn report the same to their supervisor/manager. 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 Protected 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, Protected Information could be subject to compromise or loss. For example, an individual may unintentionally discard Protected Information, mislabel Protected Information, sent through the internal mail routing system, or drop or inadvertently leave Protected Information in a public place. Intentional disclosure of Protected 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 DISO, CISO, OIG and to their supervisor or manager. 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 possible respective disciplinary actions that may be taken against any individual and/or entity, having authorized access to Protected Information, who violates their responsibilities in handling such information:

- a) Non-deliberate violations involving negligence and/or carelessness, such as leaving Protected 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 Privileged and 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 Protected Information, regardless of position or grade level, have an appropriate understanding of the need to adhere to security procedures in order to secure Protected 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 accessing Protected 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 and SIM, should be provided to all employees, consultants, third-party contractors, and other agency personnel requiring access to Protected Information. These individuals, regardless of rank or position in a particular organization, must complete initial indoctrination and 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) refresher training, recommended every three years. 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 refresher training, if warranted.

(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 Protected Information under the Policy, how to identify Protected 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 Protected 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 Protected 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 Protected Information. Individuals completing this level of training should be introduced to the DISO or SIM, understand the organizational elements of the Policy, know how to process Protected 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) Refresher Training

Within a three (3) year time period during the anniversary month of the individual's start date on a project, or initial access to Protected 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 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 Protected 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 Protected 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
PROTECTED INFORMATION

Confidential Privileged Information

- Information that reveals security risks, threats, vulnerabilities, built –in or potential to Port Authority facilities and/or assets
- Documentation that identifies specific physical or system security vulnerabilities, when referring to specific security or terrorist threats and/or the specific capabilities in-place to counter a threat
- Documentation revealing specific security vulnerabilities at a new or existing PANYNJ facility, if specific weaknesses are reflected or maximum tolerances are provided
- Information revealing details of defeating a security system(s) or revealing the system in its entirety
- Drawings or documents that reveal specific security design criteria or ratings with regard to security performance
- Information identifying the basis for implementing an operational or technical security solution
- Details related to emergency response protocols, egress plans, flow paths, egress capacities, security systems, etc., not publicly available (diagrams, codes, standards)

Information includes, but is not limited to:

1. Security Risk and Threat Assessments (SRA);
2. Design Basis Threat Analysis (DBT);
3. Facility Security Programs/Plans (to the extent such Programs/Plans are not designated as SSI or CII);
4. Continuity of Operations Plans;
5. Security White Papers;
6. Blast Protection Design Requirements; Blast Analysis; Vector Analysis (Security Barriers, Bollards, etc.);
7. Structural plans, details and specifications if site specific information involves details regarding the capability or vulnerability of security system(s) or additional protection to a critical structure(s);
8. Drawings and/or documents with specific forced entry ratings;
9. Security System(s) designs when high technology data, which was developed by or for the Port Authority, is site specific or concerns core area system;
10. Critical element of security or life safety system; such as master controls, overrides, backup power sources when such elements would not be readily observable by the public;
11. Security system(s) command and control operating instructions and supporting countermeasures when referring to a specific site or project location;
12. Design data revealing engineering, construction of a Communication or Data Center electrical system, network connections, or facility support system with signal cable (e.g., intercom, telephone);

Confidential Information

- Specific security system/hardware model number installed at specific locations
- Details concerning overall security system(s) or individual sub systems(s), including design engineering, construction, fabrication and rollout schedule when data is site specific or concerns core area systems
- Structural plans and details if site-specific information involves details of security system(s) of protection
- Design data revealing engineering, construction, or fabrication details of primary and emergency electrical power systems supporting security, communications or life safety systems
- Documents identifying protective measures around Operations & Control Centers
- Documents identifying the location of Police and Emergency Communication Lines
- Security budget information
- Security Capital Plan
- Security personnel information

Information includes, but is not limited to:

1. Methods utilized to mitigate vulnerabilities and threats, such as identity, location, design, construction, schedule, and fabrication of security systems;
2. Details concerning overall security system(s) or individual subsystem(s), including design, engineering, construction, fabrication and rollout schedule when data is site specific or concerns core area systems;
3. Concept of Operations (CONOPS) documents;
4. Structural plans and details if site-specific information involves details of security system(s) or protection;
5. Documents identifying protective measures around Operation Control and Data Centers;
6. Documents identifying the location of Police, Emergency Communication and Network Lines;
7. Security White Papers
8. Secure Identification Display Area (SIDA) Badge Application (Aviation)
9. Selected Environmental Documents – Condition Surveys containing information on contaminated sites;
10. Emergency Operations Plan (to be shared with other Agencies);
11. Guidance for Managing Multi-Agency Response to WMD/CBREN Incidents;
12. Security system logs and reports, system operators and users including all related personal and company data;
13. System information used to construct and protect security systems;
14. Information/documents compiled for law enforcement or official investigatory purposes;
15. Sensitive financial, commercial and other business information received from third parties under Non-Disclosure and Confidentiality Agreements:
16. Security Project Management budget Information;
17. Security Project Management Capital Plan;
18. Property Lease Agreements (Negotiations);
19. Legal Settlement agreements (when specified in the final settlement agreement);
20. Financial Analysis relating to ongoing litigation;
21. 5-year Capital Security Plan.
22. Law Enforcement investigatory material based upon the sensitive or confidential nature of the information

Health Insurance Portability and Accountability Act (HIPAA)

Employees, associates or other contract personnel who have access to Protected Health Information (PHI) must also refer to, and comply with, the Privacy Policies and Procedures to Protect Personal Health Information. Privacy regulations issued under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA” or “Privacy Laws”) place restrictions on the Group Health Plans of the Port Authority and PATH (the “Plans”) ability to use and disclose Protected Health Information (“PHI”).

To protect the privacy and confidentiality of PHI and to comply with HIPAA, all members of Employee Benefits, including the Customer Service Representatives, and any others who have access to PHI, must comply with the policies and procedures set forth in this manual (the “Policies and Procedures”). The purpose of this manual is to establish how the Privacy Laws are to be implemented by the Plans and Employee Benefits in particular. This document maintained by the Employee Benefits Division of HRD, addresses Privacy Law Concerns related to the Health Insurance Portability and Accountability Act (HIPAA).

HIPAA defines **Protected Health Information (PHI)** as all individually identifiable health information that is transmitted or maintained by the benefit plans in any medium – electronic, oral or written. The Port Authority receives this information in its employer capacity and, therefore, it is not considered to be PHI:

- An individual’s name, address, birth date, marital status, dependent information and Social Security number;
- An individual’s choice of health plan;

Attorney Work Product

Attorney work product and other privileged information should be protected and treated in accordance with the established rules of the profession and may carry the marking “Privileged & Confidential”. Certain work product information may also fall within the definitions of Confidential Privileged and/or Confidential Information as established by the Handbook, and as such, should be marked and treated in accordance with the Handbook and the Law Department CIPP.

Federal Designations:

Security Sensitive 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.

1. Facility Security Programs/Plans (Aviation and Port Facilities fall under SSI);
2. Exclusive Area Agreements (Aviation and Ports – An agreement between PA and tenant that has a security program, which permits the tenant to assume responsibility for security within the affected area(s). SSI);
3. TAS Security Directives (SSI);
4. SEA LINK Database and corresponding applications (Ports - SSI/Privacy Act Information).
5. Security Directives issued by the TSA

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.

PROTECTED INFORMATION (CONFIDENTIAL INFORMATION)	
Handbook Marking <ul style="list-style-type: none">• Confidential Privileged• Confidential• CII & SSI	Outside Handbook Marking Protocols <ul style="list-style-type: none">• HIPAA• Litigation/Law• Law Enforcement Investigatory Material• Active Negotiations• RFP Proposals under evaluation

APPENDIX B

Non-Disclosure and Confidentiality Agreements

B-1
Non-Disclosure and Confidentiality Agreement
with reference to Handbook

**NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT
BETWEEN**

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 _____, _____, 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 _____ (“**Recipient**”).

WHEREAS, the Port Authority desires, subject to the terms and conditions set forth below, to disclose to Recipient Protected Information (as defined below) in connection with _____
(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 protected, 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 protected, 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:

(a) **“Authorized Disclosure”** means the disclosure of Protected Information strictly in accordance with the Confidentiality Control Procedures applicable thereto: (i) as to all Protected Information, only to a Related Party that has a need to know such Protected 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 or Exhibit B, as applicable; 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.

(b) **“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.

(c) **“Protected Information”** means and includes collectively, Confidential Information, Confidential Privileged Information, Sensitive Security Information (SSI), Critical Infrastructure Information (CII) or Health Insurance Portability and Accountability Act (HIPPA) 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 Protected 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 Recipient, the Port Authority or others, or when the Port Authority receives such information from others and agrees to treat such information as Protected. The following Information shall not constitute Protected Information for the purpose of this Agreement:

- (i) 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 Protected Information.
- (ii) 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.
- (iii) Information that is known to or was in the possession of the Recipient or a Related Party on a non-confidential basis prior to the disclosure of such Information by the Port Authority.

(d) **“Confidential Information”** means and includes collectively, 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. It also 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 Code.

(e) **“Confidential Privileged Information”** means and includes collectively, (i) Information that reveals security risks, threats, vulnerabilities, documentation that identifies specific physical security vulnerabilities or revealing specific security vulnerabilities details related to emergency response protocols, egress plans, flow paths, egress capacities, (diagrams, codes, standards) etc., which is not publicly available.” and 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, and (ii) certain Critical Infrastructure Information.

(f) **“Confidentiality Control Procedures”** means procedures, safeguards and requirements for the identification, processing, protection, handling, care, tracking and storage of

Protected Information that are required under applicable federal or state law, the Port Authority Handbook, or by the terms of this Agreement.

(g) "**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.

(h) "**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).

(i) "**Health Insurance Portability and Accountability Act**" (HIPAA) Information Employees, associates or other contract personnel who have access to Protected Health Information (PHI) must refer to, and comply with, the Privacy Policies and Procedures to Protect Personal Health Information. Privacy regulations issued under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA" or "Privacy Laws") place restrictions on the Group Health Plans of the Port Authority and PATH (the "Plans") ability to use and disclose Protected Health Information ("PHI").

(j) "**Port Authority Handbook**" means The Port Authority of New York and New Jersey. Information Security Handbook, as may be amended by the Port Authority, from time to time.

(k) "**Project Purposes**" means the use of Protected 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.

(l) "**Related Party**" and "**Related Parties**" means the directors, employees, officers, partners or members of the Recipient, as applicable, and the Recipient's outside consultants, attorneys, advisors, accountants, architects, engineers or subcontractors or sub-consultants (and their respective directors, employees, officers, partners or members) to whom any Protected Information is disclosed or made available.

2. **Use of Protected Information.** All Protected Information shall be used by the Recipient in accordance with the following requirements:

(a) All Protected 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 or Exhibit B, as applicable, and

applicable legal requirements. Protected Information may be disclosed, only if and to the extent that such disclosure is an Authorized Disclosure.

(b) 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 Protected 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.

(c) 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 Protected 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 Protected Information. Recipient and each Related Party shall undertake reasonable steps consistent with such Confidentiality Control Procedures to assure that disclosure of Protected Information is compartmentalized, such that all Protected 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.

(d) The Port Authority reserves the right to audit Recipient's Confidentiality Control Procedures, and those of each Related Party, as applicable, to ensure that it is in compliance with the terms of this Agreement.

(e) 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 Protected 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 Protected Information if the Recipient or any of the Related Parties do not agree in writing to apply such controls.

(f) Nothing in this Agreement shall require the Port Authority to tender or provide access to or possession of any Protected Information to the Recipient or its Related Parties, whether or not the requirements of this Agreement are otherwise satisfied. However, if such Protected Information is provided and accepted, the Recipient and its Related Parties shall abide by the terms, conditions and requirements of this Agreement.

(g) 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 Protected 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 Protected Information has been made available to the Recipient or such Related Parties, or the content or import of such Protected 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.

(h) As to all Protected 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 Protected Information is received by the Recipient or any Related Party, Recipient shall notify the Port Authority thereof, to the extent permitted by law, 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 Protected Information as is legally required to be disclosed. If at any time Protected 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 Protected Information.** Upon the earlier occurrence of either the Port Authority's written request or completion of Recipient's need for any or all Protected Information, such Protected Information, all writings and material describing, analyzing or containing any part of such Protected Information, including any and all portions of Protected 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 Protected Information that may be stored in electronic or similar form, such Protected Information shall be deleted and completely removed so that such Protected Information is 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 Protected 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 Protected 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 copies of Protected Information (in any format), 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 Protected 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 Protected Information is no longer considered protected, 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 Protected 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 9.

Original to the Port Authority: The Port Authority of New York and New Jersey

with a copy to: The Port Authority of New York and New Jersey
225 Park Avenue South - 14th Floor
New York, NY 10003
Attn: General Counsel's Office c/o Caroline Ioannou, Law
DISO

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.

RECIPIENT:

Signature: _____

Print Name: _____

Title: _____

Date: _____

EXHIBIT A

ACKNOWLEDGMENT BY RELATED PARTY INDIVIDUAL

I, _____ (“**Related Party**”), am employed as a(n) _____ by _____. 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 _____, both my employer and I may be provided with access to, and/or copies of, sensitive security materials, protected or confidential information. If it is required for me to review or receive Protected 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 Protected 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.

Signature: _____

Print Name: _____

Date: _____

EXHIBIT B

ACKNOWLEDGMENT BY RELATED PARTY ENTITY

The undersigned, _____, is the _____ of _____, a _____ (**“Related Party”**), located at _____, 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 _____ in connection with _____ 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.

Signature: _____

Print Name: _____

Date: _____

B-2
Non-Disclosure and Confidentiality Agreement
without reference to Handbook

**NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT
BETWEEN**

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 _____, _____, 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 _____ ("Recipient").

WHEREAS, the Port Authority desires, subject to the terms and conditions set forth below, to disclose to Recipient Protected Information (as defined below) in connection with _____ (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 protected, 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

Port Authority Non-Handbook NDA 103113

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 protected, 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:

(a) **“Authorized Disclosure”** means the disclosure of Protected Information strictly in accordance with the Confidentiality Control Procedures applicable thereto: (i) as to all Protected Information, only to a Related Party that has a need to know such Protected 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 or Exhibit B, as applicable; 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.

(b) **“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.

(c) **“Protected Information”** means and includes collectively, Confidential Information, Confidential Privileged Information, Sensitive Security Information (SSI), Critical Infrastructure Information (CII) or Health Insurance Portability and Accountability Act (HIPPA) 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 Protected 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 Recipient, the Port Authority or others, or when the Port Authority receives such information from others and agrees to treat such information as Protected. The following Information shall not constitute Protected Information for the purpose of this Agreement:

- (i) 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 Protected Information.
- (ii) 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.
- (iii) Information that is known to or was in the possession of the Recipient or a Related Party on a non-confidential basis prior to the disclosure of such Information by the Port Authority.

(d) **“Confidential Information”** means and includes collectively, 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. It also 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 Code.

(e) **“Confidential Privileged Information”** means and includes collectively, (i) Information that reveals security risks, threats, vulnerabilities, documentation that identifies specific physical security vulnerabilities or revealing specific security vulnerabilities details related to emergency response protocols, egress plans, flow paths, egress capacities, (diagrams, codes, standards) etc., which is not publicly available.” and 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, and (ii) certain Critical Infrastructure Information.

(f) **“Confidentiality Control Procedures”** means procedures, safeguards and requirements for the identification, processing, protection, handling, care, tracking and storage of Protected Information that are required under applicable federal or state law or by the terms of this Agreement.

(g) **"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.

(h) **"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).

(i) **"Health Insurance Portability and Accountability Act"** (HIPAA) Information Employees, associates or other contract personnel who have access to Protected Health Information (PHI) must refer to, and comply with, the Privacy Policies and Procedures to Protect Personal Health Information. Privacy regulations issued under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA" or "Privacy Laws") place restrictions on the Group Health Plans of the Port Authority and PATH (the "Plans") ability to use and disclose Protected Health Information ("PHI").

(j) **"Project Purposes"** means the use of Protected 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.

(k) **"Related Party"** and **"Related Parties"** means the directors, employees, officers, partners or members of the Recipient, as applicable, and the Recipient's outside consultants, attorneys, advisors, accountants, architects, engineers or subcontractors or sub-consultants (and their respective directors, employees, officers, partners or members) to whom any Protected Information is disclosed or made available.

2. **Use of Protected Information.** All Protected Information shall be used by the Recipient in accordance with the following requirements:

(a) All Protected 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. Protected Information may be disclosed, only if and to the extent that such disclosure is an Authorized Disclosure.

(b) 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 Protected 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.

(c) 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 Protected 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 Protected Information. Recipient and each Related Party shall undertake reasonable steps consistent with such Confidentiality Control Procedures to assure that disclosure of Protected Information is compartmentalized, such that all Protected 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.

(d) The Port Authority reserves the right to audit Recipient's Confidentiality Control Procedures, and those of each Related Party, as applicable, to ensure that it is in compliance with the terms of this Agreement.

(e) 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 Protected 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 Protected Information if the Recipient or any of the Related Parties do not agree in writing to apply such controls.

(f) Nothing in this Agreement shall require the Port Authority to tender or provide access to or possession of any Protected Information to the Recipient or its Related Parties, whether or not the requirements of this Agreement are otherwise satisfied. However, if such Protected Information is provided and accepted, the Recipient and its Related Parties shall abide by the terms, conditions and requirements of this Agreement.

(g) 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 Protected 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 Protected Information has been made available to the Recipient or such Related Parties, or the content or import of such Protected 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.

(h) As to all Protected 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 Protected Information is received by the Recipient or any Related Party, Recipient shall notify the Port Authority thereof, to the extent permitted by law, 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 Protected Information as is legally required to be disclosed. If at any time Protected 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 Protected Information.** Upon the earlier occurrence of either the Port Authority's written request or completion of Recipient's need for any or all Protected Information, such Protected Information, all writings and material describing, analyzing or containing any part of such Protected Information, including any and all portions of Protected 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 Protected Information that may be stored in electronic or similar form, such Protected Information shall be deleted and completely removed so that such Protected Information is 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 Protected 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 Protected 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 copies of Protected Information (in any format), 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 Protected 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 Protected Information is no longer considered protected, 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 Protected 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 9.

Original to the Port Authority:

The Port Authority of New York and New Jersey

with a copy to:

The Port Authority of New York and New Jersey
225 Park Avenue South - 14th Floor
New York, NY 10003

If to the Recipient:

Attn: General Counsel's Office c/o Caroline Ioannou, Law DISO

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.

RECIPIENT:

Signature: _____

Print Name: _____

Title: _____

Date: _____

EXHIBIT A

ACKNOWLEDGMENT BY RELATED PARTY INDIVIDUAL

I, _____ (“Related Party”), am employed as a(n) _____ by _____. 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 _____, both my employer and I may be provided with access to, and/or copies of, sensitive security materials, protected or confidential information. If it is required for me to review or receive Protected 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 Protected 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.

Signature: _____

Print Name: _____

Date: _____

EXHIBIT B

ACKNOWLEDGMENT BY RELATED PARTY ENTITY

The undersigned, _____, is the _____ of _____, a _____ ("Related Party"), located at _____, 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 _____ in connection with _____ 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.

Signature: _____

Print Name: _____

Date: _____

B-3
**PA/PATH Non-Disclosure and
Confidentiality Agreement**

**PA EMPLOYEE NON-DISCLOSURE
AND CONFIDENTIALITY AGREEMENT**

THIS NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT (this “**Agreement**”) is made as of this _____ day of _____, _____, by and between **THE PORT AUTHORITY OF NEW YORK AND NEW JERSEY**, 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 its related entities, including, but not limited to, Port Authority Trans-Hudson Corporation (collectively referred to as the “**Port Authority**”) and having an office and place of business at 225 Park Avenue South, New York, New York, 10003, and _____, of _____ Department, an employee of the Port Authority (“**Employee**”), having the Port Authority 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 protected, 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 protected, 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 Protected 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. “**Protected Information**” means and includes collectively, Confidential Information, Confidential Privileged Information, Critical Infrastructure Information (CII), Sensitive Security Information (SSI), or Health Insurance Portability and Accountability Act (HIPPA) 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 Protected 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 Recipient, the Port Authority or others, or when the Port Authority receives such information from others and agrees to treat such information as Protected.

Port Authority Employee NDA 103113

- b. **“Confidential Information”** means and includes collectively, 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. It also 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 Code.
- c. **“Confidential Privileged Information”** means and includes collectively, (i) Information that reveals security risks, threats, vulnerabilities, documentation that identifies specific physical security vulnerabilities or revealing specific security vulnerabilities details related to emergency response protocols, egress plans, flow paths, egress capacities, (diagrams, codes, standards) etc., which is not publicly available.” and 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, and (ii) certain Critical Infrastructure Information.
- d. **“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.
- e. **“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.
- f. **“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).
- g. **“Health Insurance Portability and Accountability Act”** (HIPAA) Information Employees, associates or other contract personnel who have access to Protected Health Information (PHI) must refer to, and comply with, the Privacy Policies and Procedures to Protect Personal Health Information. Privacy regulations issued under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA” or

“Privacy Laws”) place restrictions on the Group Health Plans of the Port Authority and PATH (the “Plans”) ability to use and disclose Protected Health Information (“PHI”).

- h. **“Port Authority Handbook”** means The Port Authority of New York and New Jersey Information Security Handbook, as may be amended by the Port Authority, from time to time.
- 2. **Compliance with the Port Authority Handbook.** All Protected 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 Protected Information in a manner consistent with this Agreement and in conformity with the Port Authority Handbook.
- 3. **Use of Protected Information.** Protected 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 Protected 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 Protected 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 Protected 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 Protected 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 Protected Information is no longer considered protected, confidential and/or privileged by the Port Authority, and that fact is communicated in writing to Employee.

EMPLOYEE:

Signature: _____

Print Name: _____

Date: _____

APPENDIX C

Background Screening Criteria



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 transportation 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 than 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. 5845(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 transportation 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. 5845(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 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) 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 (SWAC)

Secure Worker Access Consortium (SWAC 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, SWAC 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 SWAC Customer Service may be contacted at (212) 608-0855.

o Consultants / Contractors

- o 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.
- o 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.)
- o Step 2: The applicant is photographed, provides a digital signature and presents the required identification documents at an operational SWAC Processing Center.
- o Step 3: SWAC 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 (212) 608-0855.

o Individuals

- o Step 1: Individual completes the Individual Membership Application Form online. <http://www.secureworker.com>
- o Step 2: Individual immediately takes the required government issued identity documents to a SWAC Processing Center to complete the second and final step of the SWAC application process. **NOTE:** This step is required before your background screening is initiated.

- **SWAC Processing Centers** - check the SWAC 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 & Fridays, 6:30AM to
12:30PM

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

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 Recipient]

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 PROTECTED INFORMATION

I. GENERAL

This section describes the **preferred methods** for the physical protection of Protected 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. PROTECTED INFORMATION STORAGE

A. Approved Containers

The following storage containers are approved for storage of PANYNJ Protected 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 examples of types approved for storage of PANYNJ Protected Information, but not limited to these locks:

1. Any restricted keyway 7-pin tumbler lock or equivalent pick resistant lock.
2. A combination padlock such as a Sesame four-position dial padlock. See photo at right.

For Port Authority facilities, locks and locking devices available from Port Authority stock room or approved vendor will meet this requirement.

C. Combinations to Security Containers, Cabinets, and Vaults

If required, 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 Protected 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 Protected 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 Protected 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 Protected 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 Protected 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 Protected 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 PROTECTED INFORMATION.

I. GENERAL

This section describes the preferred methods for the disposal and destruction of Protected 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.

Protected Information no longer needed shall be processed for appropriate archiving or disposal. Protected Information approved for destruction shall be destroyed in accordance with this section. The method of destruction must preclude recognition or reconstruction of the Protected Information or material.

All persons in possession of Protected materials shall establish procedures for review of their Protected holdings on a recurring basis to reduce these inventories to the minimum necessary for effective and efficient operations. Multiple copies, obsolete material, and Protected 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 Protected material being retained.

Original records must be retained in accordance with the Agency's Records Management Policy and Retention Schedules.

II. DISPOSAL AND DESTRUCTION

A. Destruction Requirements

All persons in possession of Protected 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, Protected material shall be destroyed by commercial grade cross cut shredders located conveniently throughout the workplace for use by authorized individuals.
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 Protected 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 Protected file will require a bit-by-bit overwrite of the storage area used by the file. 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

Protected 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

Protected 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.

Protected waste shall be destroyed as soon as practical. This applies to all waste material containing Protected Information. Pending destruction, Protected waste shall be appropriately safeguarded. (See also Appendix G - Guidelines for the Storage of Protected Information.)

III. PROTECTED WASTE

A. Approved Receptacles

1. Receptacles utilized to accumulate Protected 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 Protected 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 Protected 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 Protected 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 Protected



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 Protected 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 Protected Information?

CLASSIFICATION

- Does the contractor have adequate procedures for evaluating Protected material being created, extracted, or summarized?
- Is contractor-developed Protected 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 Protected 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 Protected material, regardless of its physical form, marked properly?
- Is all Protected 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 Protected compilations if required?

TRANSMISSION

- Is Protected Information properly prepared for transmission outside the facility?
- Are Transmittal Receipts included with Protected Information if required?
- Is a suspense system established to track transmitted documents until the signed receipt is returned?
- Are authorized methods used to transmit Protected material outside the facility?
- Is the NDA of the receiving facility determined prior to transmission of Protected Information?

PROTECTED INFORMATION CONTROLS

- Do contractor employees understand their safeguarding responsibilities?
- Is the contractor's accountability system capable of facilitating the retrieval and disposition of Protected material as required?
- Are external receipts and dispatch records maintained as required?
- Is all Protected material received at the contractor facility and delivered directly to designated personnel?
- Do contractor employees promptly report the loss, compromise, or suspected

compromise of Protected Information to the SIM?

DISPOSITION

- Is a program established to review Protected retention on a recurring basis for the purpose of reduction?
- Is Protected material destroyed as soon as possible after it has served its purpose?
- Does the contractor employ an effective method of destruction?
- Is Protected material destroyed by the appropriate employees?
- Is Protected waste properly safeguarded until its timely destruction?

REPRODUCTION

- Does the facility's reproduction control system keep reproduction of Protected material to a minimum?
- Is the reproduction of Protected Information accomplished only by properly authorized, and knowledgeable employees?
- Is reproduction authorization obtained as required?
- Are reproductions of Protected 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 Protected Information handled in a manner consistent with the handling of Confidential documents?
- Are all AIS storage media, internal memory, and equipment, that contain Protected Information, properly sanitized prior to removal from protection?

Suggested Questions When Interviewing Employees NOT Authorized Access to Confidential Information:

- What is Protected Information?
- Have you ever seen Protected Information?
- If you found Protected Information unprotected, what would you do?

Suggested Questions When Interviewing Employees Authorized Access to Protected 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 Protected Information?
- Have you ever had access to Protected Information outside of this facility?
- Did anyone else from the facility accompany you?
- Did you take any Confidential notes or Protected Information back to the facility?
- What procedures were followed to protect this information?
- Where is this information now?
- Have you ever provided access to Protected Information to visitors?
- How did you determine their need-to-know?
- Have you ever been approached by anyone requesting Protected Information?
- Do you ever work overtime and access Protected 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 Protected Information?
- Where do you typically work when you generate Protected Information?
- What procedures do you follow to protect Protected Information while working on it?
- Do you ever use a computer to generate Protected 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 Protected material?
- Have you reproduced Protected Information? Describe the procedures.
- Have you destroyed Protected Information? What procedures were used?
- Do you have any questions regarding security?