

**THE PORT AUTHORITY OF NY & NJ**

**PROCUREMENT DEPARTMENT  
2 MONTGOMERY STREET, 3<sup>RD</sup> FL.  
JERSEY CITY, NJ 07302**

3/18/2013

ADDENDUM # 1

To prospective Proposer(s) on RFP # **32529 for IT COMPUTING RESOURCES  
MANAGEMENT SERVICES - REQUEST FOR PREQUALIFICATION**

Due back on 04/02/2013, no later than 2:00PM

*The following changes/modifications are hereby made to the solicitation documents:*

In the “Response Requirements” portion of the RFPQ (item 6, Section g: “Non-Disclosure and Confidentiality Agreements and Acknowledgements” on page 12 and Appendix 1 “Non-Disclosure and Confidentiality Agreement”, pages 25 – 32 replace attachments with the following documents attached herein.

Attached documents:

- Confidential Information, 1.1.1
- Template: Port Authority Non-Disclosure and Confidentiality Agreement (NDA)
- Non-Disclosure and Confidentiality Agreement (NDA), pages 1 – 9
- Template: Port Authority Acknowledgment by Related Party Individual (Exhibit A)
- Exhibit A, Acknowledgment By Related Party Individual
- Exhibit B, Acknowledgment By Related Party Entity
- The Port Authority of New York & New Jersey Information Security Handbook, October 15, 2008, corrected as of February 9, 2009

This communication should be initialed by you and annexed to your Response upon submission. In case any Respondent fails to conform to these instructions, its submission will nevertheless be construed as though this communication had been so physically annexed and initialed.

THE PORT AUTHORITY OF NY & NJ

KATHY LESLIE WHELAN, MANAGER  
COMMODITIES & SERVICES DIVISION

RESPONDENT FIRM NAME: \_\_\_\_\_

INITIALED: \_\_\_\_\_ DATE: \_\_\_\_\_

QUESTIONS CONCERNING THIS ADDENDUM MAY BE ADDRESSED TO JEANETTE ANDERSON AT (201) 395-3430 or at [jeanette.anderson@panynj.gov](mailto:jeanette.anderson@panynj.gov).

PS11A11

### 1.1.1 Confidential Information

Prequalified Firms in the preparation of Proposals will require access to Port Authority Confidential Information. Confidential Information is information belonging to the Port Authority that, if it were subject to unauthorized access, modification, loss or misuse could seriously damage the Authority, public safety, or homeland security. Protecting this sensitive information requires the application of uniform safeguarding measures to prevent unauthorized disclosure and to control any authorized disclosure of this information within the Authority or when released by the Authority to outside entities. Therefore, both corporate non-disclosures agreements and individual non-disclosure acknowledgments are required for all prequalified firms, their staff and subcontractors working on the RFP. These procedures and forms are identified in the Authority's "Information Security Handbook". For reference, the Information Security Handbook is attached.

To that end, the Authority maintains a secure collaborative Program Website called Livelink to store, share and distribute all Project documentation to the successful firm that is awarded the contract. For any information deemed to be Confidential & Privileged Information / Sensitive Security Information, Livelink is the only acceptable means of electronically distributing and sharing such information. Each Prequalified Firm and each participant in a joint venture will be required to designate a Security Information Manager ("SIM") responsible for identifying members of their team who will need access to Livelink and for assuring that those members have passed the requisite background checks and have completed the requisite Livelink access forms. The SIM will be responsible for maintaining their firm's Livelink user account access list. In addition, the SIM will identify an individual who will be trained by the Authority and that individual will subsequently be responsible for training the Prequalified Firm.

#### **Notes on security and personnel requirements:**

- The Information Security Handbook requires that certain criteria be met prior to being granted access to Confidential Information. Generally, an individual must be a U.S. Citizen, 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 in exceptional circumstances and contractors should refer to § 3.2 of the Information Security Handbook for details on this policy and the process for waiver.
- Prequalified Firms in the preparation of Proposals should be aware that background checks will be required of all individuals who require access to the RFP for these services, of which either sections or the total document will be deemed Confidential Information. Background checks are performed through SWAC, the secure worker access consortium ([www.secureworker.com](http://www.secureworker.com)). The Authority typically requires all individuals for whom security check is necessary receive a high clearance level.
- Be advised that the following must be supplied to the Agency prior to the release of the hard copy RFP:
  - A Project Security Information Manager must be identified with their contact information,

- Corporate NDA's (file name 2011 General NDA Template\_Handbook \_12-20-10) executed by an officer of the firm
- Individual NDA Acknowledgement Exhibit A (file name Exhibit A B 12-20-10) for the Prequalified Firms PSIM and Corporate Officer (CO) executing the corporate non-disclosure agreement,
- and proof of successful SWAC background checks (for the PSIM and CO) must all be submitted.
- At the conclusion of the RFP process the firm's SIM must collect and return all original Confidential Information supplied by the Authority. All copies must be destroyed by the firm's SIM and acknowledged to the Authority.

Template: Port Authority Non-Disclosure and Confidentiality Agreement (NDA)

Please fill in the NDA as described below. All original NDA's must be forwarded to the Port Authority contact with a copy to the Port Authority Law Department (as described on Page 8 of the NDA).

<b>Field Form Number</b>	<b>Description of Data to be Entered</b>
[1]	Insert Name of Company (All caps)
[2]	Insert Calendar Day
[3]	Insert Month
[4]	Insert Name of Company (All caps)
[5]	Insert Company's full street address (no P.O. boxes) – city, state, and zip code
[6]	Insert Scope of Work
[7]	Insert Name of Port Authority Contact
[8a]	Insert Full Street Address including Floor/Suite (if applicable)
[8b]	Insert City, State, and Zip code
[9]	Print Name
[10]	Print Title
[11]	Insert Date Signed

**NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT  
BETWEEN**

[1]

**AND**

**THE PORT AUTHORITY OF NEW YORK AND NEW JERSEY**

**THIS NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT** (this “**Agreement**”) is made as of this \_\_\_\_\_[2] day of \_\_\_\_\_[3], 2013, 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 \_\_\_\_\_[4] having an office and place of business at \_\_\_\_\_[5] (“**Recipient**”).

**WHEREAS**, the Port Authority desires, subject to the terms and conditions set forth below, to disclose to Recipient Confidential Information (as defined below) in connection with \_\_\_\_\_[6] (insert description of project/work) (collectively, the “**Project(s)**”, or “**Proposed Project(s)**”); and

**WHEREAS**, the Recipient acknowledges that the Port Authority, in furtherance of its performance of essential and critical governmental functions relating to the Project, has existing and significant interests and obligations in establishing, maintaining and protecting the security and safety of the Project site and surrounding areas and related public welfare matters; and

**WHEREAS**, in furtherance of critical governmental interests regarding public welfare, safety and security at the Project site, the Port Authority has collected information and undertaken the development of certain plans and recommendations regarding the security, safety and protection of the Project site, including the physical construction and current and future operations; and

**WHEREAS**, the Port Authority and Recipient (collectively, the “**Parties**”) acknowledge that in order for Recipient to undertake its duties and/or obligations with regard to its involvement in the Project, the Port Authority may provide Recipient or certain of its Related Parties (as defined below) certain information in the possession of the Port Authority, which may contain or include confidential, privileged, classified, commercial, proprietary or sensitive information, documents and plans, relating to the Project or its occupants or other matters, the unauthorized disclosure of which could result in significant public safety, financial and other damage to the Port Authority, the Project, its occupants, and the surrounding communities; and

**WHEREAS**, Recipient recognizes and acknowledges that providing unauthorized access to, or disclosing such information to third parties in violation of the terms of this Agreement

could compromise or undermine the existing or future guidelines, techniques and procedures implemented for the protection against terrorist acts or for law enforcement, investigation and prosecutorial purposes, and accordingly could result in significant irreparable harm and injury; and

**WHEREAS**, in order to protect and preserve the privilege attaching to and the confidentiality of the aforementioned information as well as to limit access to such information to a strict need to know basis, the Port Authority requires, as a condition of its sharing or providing access to such confidential, privileged, classified, commercial, proprietary or sensitive information, documents and plans, that the Recipient enter into this Agreement and that its Related Parties thereafter acknowledge and agree that they will be required to treat as strictly confidential and/or privileged any of such information so provided, as well as the work product and conclusions of any assessments and evaluations or any recommendations relating thereto, and to also fully comply with applicable federal rules and regulations with respect thereto; and

**WHEREAS**, as a condition to the provision of such information to Recipient and certain Related Parties, the Recipient has agreed to enter into this Agreement with respect to the handling and use of such information and to cause Related Parties to join in and be bound by the terms and conditions of this Agreement.

**NOW, THEREFORE**, in consideration of the provision by Port Authority of Information for Project Purposes (as each such term is defined below) and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged by the Recipient and each Related Party that receives such Information, the Recipient and each such Related Party agrees, as follows:

1. **Defined Terms.** In addition to the terms defined in the Recitals above, the following terms shall have the meanings set forth below:

(a) **“Authorized Disclosure”** means the disclosure of Confidential Information strictly in accordance with the Confidentiality Control Procedures applicable thereto: (i) as to all Confidential Information, only to a Related Party that has a need to know such Confidential Information strictly for Project Purposes and that has agreed in writing to be bound by the terms of this Agreement by executing a form of Acknowledgment as set forth in Exhibit A; and (ii) as to Confidential Privileged Information, only to the extent expressly approved in writing and in advance by the Port Authority, and then only the particular Confidential Privileged Information that is required to accomplish an essential element of the Project.

(b) **“Confidential Information”** means and includes collectively, Confidential Proprietary Information, Confidential Privileged Information, and Information that is labeled, marked or otherwise identified by or on behalf of the Port Authority so as to reasonably connote that such Information is confidential, privileged, sensitive or proprietary in nature. The term Confidential Information shall also include all work product that contains or is derived from any of the forgoing, whether in whole or in part, regardless of whether prepared by the Recipient, the Port Authority or others. The following Information shall not constitute Confidential Information for the purpose of this Agreement:

- (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 Confidential 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.

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

(d) **“Confidential Proprietary Information”** means and includes Information that contains financial, commercial or other proprietary, business Information concerning the Project, the Port Authority, or its facilities.

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

(f) **“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.

(g) **“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.

(h) **“Limited Access Safety and Security Information”** means and includes sensitive Information, the disclosure of which would be detrimental to the public interest and might compromise public safety and/or security as it relates to Port Authority property, facilities,

systems and operations, and which has not otherwise been submitted for classification or designation under any Federal laws or regulations.

(i) **“Port Authority Handbook”** means the Port Authority of N.Y. & N.J. Information Security Handbook, a copy of which is attached hereto as Exhibit B, as may be amended by the Port Authority, from time to time.

(j) **“Project Purposes”** means the use of Confidential Information strictly and only for purposes related to Recipient’s and its Related Parties’ participation and involvement in the Project, and only for such period of time during which Recipient and its Related Parties are involved in Project related activities.

(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, advisors, accountants, architects, engineers or subcontractors or subconsultants (and their respective directors, employees, officers, partners or members) to whom any Confidential Information is disclosed or made available.

(l) **“Sensitive Security Information”** has the definition and requirements set forth in the Transportation Security Administrative Rules & Regulations, 49 CFR 1520, (49 U.S.C. §114) and in the Office of the Secretary of Transportation Rules & Regulations, 49 CFR 15, (49 U.S.C. §40119).

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

(a) All Confidential Information shall be held in confidence and shall be processed, treated, disclosed and used by the Recipient and its Related Parties only for Project Purposes and in accordance with the Confidentiality Control Procedures established pursuant to Paragraph 2(c), below, including, without limitation, the Port Authority Handbook, receipt of which is acknowledged by Recipient and shall be acknowledged in writing by each Related Party by signing the Acknowledgment attached hereto as Exhibit A, and applicable legal requirements. Confidential Information may be disclosed, only if and to the extent that such disclosure is an Authorized Disclosure.

(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 Confidential Information may result in penalties and other enforcement or corrective action as set forth in such statutes and regulations, including, without limitation, the issuance of orders requiring retrieval of Sensitive Security Information and Critical Infrastructure Information to remedy unauthorized disclosure and to cease future unauthorized disclosure and (ii) pursuant to the aforementioned Federal Regulations, including, without limitation, 49 C.F.R. §§ 15.17 and 1520.17, any such violation thereof or mishandling of information therein defined may constitute grounds for a civil penalty and other enforcement or corrective action by the

United States Department of Transportation and the United States Department of Homeland Security, and appropriate personnel actions for Federal employees.

(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 Confidential Information to control and safeguard against any violation of the requirements of this Agreement and against any unauthorized access, disclosure, modification, loss or misuse of Confidential Information. Recipient and each Related Party shall undertake reasonable steps consistent with such Confidentiality Control Procedures to assure that disclosure of Confidential Information is compartmentalized, such that all Confidential Information shall be disclosed only to those persons and entities authorized to receive such Information as an Authorized Disclosure under this Agreement and applicable Confidentiality Control Procedures. The Confidentiality Control Procedures shall, at a minimum, adhere to, and shall not be inconsistent with, the procedures and practices established in the Port Authority Handbook.

(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 Confidential Information as a precondition for its disclosure. The Port Authority may decline any request by the Recipient or any of its Related Parties to provide such item of Confidential Information if the Recipient or any of the Related Parties do not agree in writing to apply such controls.

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

(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 Confidential Information under circumstances where the Recipient is not fully satisfied that the person or entity to whom such disclosure is about to be made shall act in accordance with the Confidentiality Control Procedures whether or not such person or entity has agreed in writing to be bound by the terms of this Agreement or any "Acknowledgement" of its terms or (ii) the fact that Confidential Information has been made available to the Recipient or such Related Parties, or the content or import of such Confidential Information. The Recipient is responsible for collecting and managing the Acknowledgments signed by Related Parties pursuant to this Agreement. Recipient shall, at the Port Authority's request, provide the Port Authority a list of all Related Parties who have signed an Acknowledgment, and copies of such Acknowledgments.

(h) As to all Confidential Information provided by or on behalf of the Port Authority, nothing in this Agreement shall constitute or be construed as a waiver of any public interest privilege or other protections established under applicable state or federal law.

3. **Disclosures and Discovery Requests.** If a subpoena, discovery request, Court Order, Freedom of Information Request, or any other request or demand authorized by law seeking disclosure of the Confidential Information is received by the Recipient or any Related Party, Recipient shall notify the Port Authority thereof with sufficient promptness so as to enable the Port Authority to investigate the circumstances, prepare any appropriate documentation and seek to quash the subpoena, to seek a protective order, or to take such other action regarding the request as it deems appropriate. In the absence of a protective order, disclosure shall be made, in consultation with the Port Authority, of only that part of the Confidential Information as is legally required to be disclosed. If at any time Confidential Information is disclosed in violation of this Agreement, the Recipient shall immediately give the Port Authority written notice of that fact and a detailed account of the circumstances regarding such disclosure to the Port Authority.

4. **Retention Limitations; Return of Confidential Information.** Upon the earlier occurrence of either the Port Authority's written request or completion of Recipient's need for any or all Confidential Information, such Confidential Information, all writings and material describing, analyzing or containing any part of such Confidential Information, including any and all portions of Confidential Information that may be stored, depicted or contained in electronic or other media and all copies of the foregoing shall be promptly delivered to the Port Authority at Recipient's expense. In addition, as to Confidential Information that may be stored in electronic or other form, such Confidential Information shall be completely removed so as to make such Confidential Information incapable of being recovered from all computer databases of the Recipient and all Related Parties. The Recipient may request in writing that the Port Authority consent to destruction of Confidential Information, writings and materials in lieu of delivery thereof to the Port Authority. The Port Authority shall not unreasonably withhold its consent to such request. If the Port Authority consents to such destruction, the Recipient and each Related Party shall deliver to the Port Authority a written certification by Recipient and such Related Party that such Confidential Information, writings and materials have been so destroyed within such period as may be imposed by the Port Authority. Notwithstanding the foregoing, to the extent required for legal or compliance purposes, the Recipient may retain a copy of Confidential Information, provided that (a) the Port Authority is notified in writing of such retention, and (b) Recipient continues to abide by the requirements of this Agreement with respect to the protection of such Confidential Information.

5. **Duration and Survival of Confidentiality Obligations.** The obligations under this Agreement shall be perpetual (unless otherwise provided in this Agreement) or until such time as the Confidential Information is no longer considered confidential and/or privileged by the Port Authority.

6. **Severability.** Each provision of this Agreement is severable and if a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

7. **Injunctive and Other Relief.** Recipient and each Related Party acknowledges that the unauthorized disclosure and handling of Confidential Information is likely to have a material adverse and detrimental impact on public safety and security and could significantly endanger the Port Authority, its facilities (including, without limitation, the Project site), its patrons and the general public and that damages at law are an inadequate remedy for any breach, or threatened breach, of this Agreement by Recipient or its Related Parties. The Port Authority shall be entitled, in addition to all other rights or remedies, to seek such restraining orders and injunctions as it may deem appropriate for any breach of this Agreement, without being required to show any actual damage or to post any bond or other security.

8. **Governing Law.** This Agreement shall be governed by and construed in accordance with the laws of the State of New York, without regard to conflict of laws principles. The Port Authority (subject to the terms of the Port Authority Legislation (as defined below)) and the Recipient specifically and irrevocably consent to the exclusive jurisdiction of any federal or state court in the County of New York and State of New York with respect to all matters concerning this Agreement and its enforcement. The Port Authority (subject to the terms of the Port Authority Legislation (as defined below)) and the Recipient agree that the execution and performance of this Agreement shall have a New York situs and, accordingly, they each consent (and solely with respect to the Port Authority, subject to the terms of the Port Authority Legislation (as defined below)) to personal jurisdiction in the State of New York for all purposes and proceedings arising from this Agreement. **“Port Authority Legislation”** shall mean the concurrent legislation of the State of New York and State of New Jersey set forth at Chapter 301 of the Laws of New York of 1950, as amended by Chapter 938 of the Laws of New York of 1974 (McKinney’s Unconsolidated Laws §§7101-7112) and Chapter 204 of the Laws of New Jersey of 1951 (N.J.S.A. 32:1-157 to 32:1-168).

9. **Notices.** Any notice, demand or other communication (each, a **“notice”**) that is given or rendered pursuant to this Agreement by either party to the other party, shall be: (i) given or rendered, in writing, (ii) addressed to the other party at its required address(es) for notices delivered to it as set forth below, and (iii) delivered by either (x) hand delivery, or (y) nationally recognized courier service (e.g., Federal Express, Express Mail). Any such notice shall be deemed given or rendered, and effective for purposes of this Agreement, as of the date actually delivered to the other party at such address(es) (whether or not the same is then received by other party due to a change of address of which no notice was given, or any rejection or refusal to accept delivery). Notices from either party (to the other) may be given by its counsel.

The required address(es) of each party for notices delivered to it is (are) as set forth below. Each party, however, may, from time to time, designate an additional or substitute required address(es) for notices delivered to it, provided that such designation must be made by notice given in accordance with this Paragraph 9.

Original to the Port Authority: \_\_\_\_\_ [7]  
The Port Authority of New York and New Jersey  
\_\_\_\_\_ [8a]  
\_\_\_\_\_ [8b]

with a copy to: The Port Authority of New York and New Jersey  
225 Park Avenue South - 14<sup>th</sup> 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: \_\_\_\_\_ [9]

Title: \_\_\_\_\_ [10]

Date: \_\_\_\_\_ [11]

Template: Port Authority Acknowledgment by Related Party Individual (Exhibit A)

Please fill in the Related Party Individual Acknowledgment as described below. All original Related Party Individual Acknowledgments must be forwarded to the Port Authority contact with a copy to the Port Authority Law Department.

<b>Field Form Number</b>	<b>Description of Data to be Entered</b>
[1]	Insert Name of Employee
[2]	Insert Title
[3]	Insert Name of Employer
[4]	Insert Name of the Company NDA you are Acknowledging (All caps)
[5a], [5b] & [5c]	Insert Month, Date, and Year of the Company NDA you are Acknowledging
[6]	Insert Name of Recipient, or the Port Authority if Related Party Individual is an employee of Recipient
[7]	Print Name
[8]	Insert Date Signed

**EXHIBIT A**

**ACKNOWLEDGMENT BY RELATED PARTY INDIVIDUAL**

I, \_\_\_\_\_ [1] (“**Related Party**”), am employed as a(n) \_\_\_\_\_ [2] by \_\_\_\_\_ [3]. I have been provided with and have read the Non Disclosure and Confidentiality Agreement between \_\_\_\_\_ [4] (the “**Recipient**”) and The Port Authority of New York and New Jersey (the “**Port Authority**”) dated \_\_\_\_\_ [5a] \_\_\_\_\_ [5b], \_\_\_\_\_ [5c] (hereinafter the “**Agreement**”), and the Port Authority Handbook attached to the Agreement. I understand that because of my employer’s relationship with \_\_\_\_\_ [6], both my employer and I may be provided with access to, and/or copies of, sensitive security materials or confidential information. If it is required for me to review or receive Confidential Information, as it is defined in the aforementioned Agreement, I acknowledge that I will be bound by each and every term and provision contained therein, and that failure to do so may include, but is not limited to, the imposition of disciplinary action and sanctions, and/or the institution of legal action seeking injunctive relief, monetary and/or criminal penalties for violation of law and/or Port Authority policies and procedures, as well as for violation of federal and/or state regulations.

To the extent that I am currently in the possession of, or have previously come into contact with, marked information as it relates to the aforementioned Agreement, I agree to conform my handling procedures for Confidential Information to the practices and procedures set forth and defined herein, or risk loss of access to said Information, removal from said Project and/or subjecting myself to the aforementioned disciplinary actions and/or civil and criminal penalties.

Signed: \_\_\_\_\_

Print Name: \_\_\_\_\_ [7]

Date: \_\_\_\_\_ [8]

**EXHIBIT B**

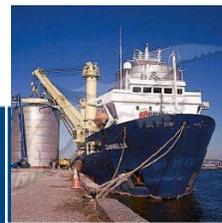
**ACKNOWLEDGMENT BY RELATED PARTY ENTITY**

The undersigned, \_\_\_\_\_ [1], is the  
\_\_\_\_\_ [2] of \_\_\_\_\_ [3], a  
\_\_\_\_\_ [4] (“**Related Party**”), located at  
\_\_\_\_\_ [5], 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 \_\_\_\_\_ [6] in connection  
with \_\_\_\_\_ [7] 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 \_\_\_\_\_ [8a] \_\_\_\_\_ [8b], \_\_\_\_\_ [8c], between  
\_\_\_\_\_ [9] (the “**Recipient**”) and the Port Authority  
(hereinafter the “**Agreement**”), and by the Port Authority Handbook described in the Agreement.  
Appropriate and responsible officers and employees of the Related Party have carefully read and  
understand the terms and conditions of the Agreement. The Related Party has notice and  
acknowledges that any breach or violation of such terms, requirements and conditions may result  
in the imposition of remedies or sanctions as set forth or otherwise described therein against such  
Related Party.

Signed: \_\_\_\_\_

Print Name: \_\_\_\_\_ [10]

Date: \_\_\_\_\_ [11]



The Port Authority of New York & New Jersey

# Information Security Handbook

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

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

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

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

## 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 .....	10
3.5 NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENTS (NDAs).....	11

3.6 UNAUTHORIZED DISCLOSURE OF INFORMATION .....	11
3.7 SECURITY CLEARANCE AND ACCESS PROHIBITIONS.....	11
3.8 BACKGROUND SCREENING .....	12
3.9 AUTHORIZED PERSONNEL CLEARANCE LIST .....	12
3.10 DEVELOPMENT OF CONFIDENTIAL INFORMATION PRACTICES AND PROCEDURES (CIPP).....	12
3.11 PROCUREMENT STRATEGIES .....	13
 <b>CHAPTER 4</b>	
<b>MARKING, HANDLING, STORAGE, TRANSMITTAL AND DESTRUCTION REQUIREMENTS .....</b>	<b>16</b>
4.1 MARKING OF CONFIDENTIAL INFORMATION .....	16
4.2 HANDLING CONFIDENTIAL INFORMATION .....	18
4.3 TRANSMITTAL OF CONFIDENTIAL INFORMATION.....	18
4.4 STORAGE OF CONFIDENTIAL INFORMATION .....	21
4.5 DOCUMENT ACCOUNTABILITY LOG.....	21
4.6 REPRODUCTION .....	22
4.7 DESTRUCTION OF CONFIDENTIAL INFORMATION .....	22
 <b>CHAPTER 5</b>	
<b>AUDITING AND MONITORING .....</b>	<b>23</b>
5.1 PURPOSE.....	23
5.2 AUDITS AND INVESTIGATIONS.....	23
5.3 SELF-ASSESSMENT .....	24
 <b>CHAPTER 6</b>	
<b>POLICY VIOLATIONS AND CONSEQUENCES .....</b>	<b>25</b>
6.1 RESPONSIBILITIES.....	25
6.2 VIOLATIONS, INFRACTIONS, OR BREACH OF INFORMATION SECURITY PROTOCOLS .....	25

6.3 VIOLATION REPORTING, INVESTIGATION AND FACT FINDING .....	25
6.4 DISCIPLINARY ACTION .....	25
<b>CHAPTER 7</b>	
<b>INFORMATION SECURITY EDUCATION AND AWARENESS TRAINING.....</b>	<b>28</b>
7.1 PURPOSE.....	28
7.2 OVERVIEW.....	28
7.3 TRAINING PROGRAM ELEMENTS .....	28

## **APPENDICES OF HANDBOOK**

### **A – NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENTS**

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

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

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

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

### **C – BACKGROUND SCREENING SPECIFICATIONS**

### **D – THE SECURE WORKER ACCESS CONSORTIUM**

### **E – COVERSHEET FOR CONFIDENTIAL PRIVILEGED INFORMATION**

### **F – TRANSMITTAL RECEIPT**

### **G –GUIDELINES FOR THE STORAGE OF CONFIDENTIAL INFORMATION**

### **H – GUIDELINES FOR THE DISPOSAL AND DESTRUCTION OF CONFIDENTIAL INFORMATION**

### **I - AUDIT PROCEDURES**

## INTRODUCTION

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

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

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

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

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

## **CHAPTER 1 - PORT AUTHORITY INFORMATION SECURITY ORGANIZATIONAL STRUCTURE**

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

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

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

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

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

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

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

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

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

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

## CHAPTER 2 - CATEGORIZATION OF INFORMATION

### 2.1 Definitions

For purposes of this Handbook the following definitions shall apply:

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

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

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

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

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

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

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

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

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

## **2.2 General Process for Categorization**

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

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

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

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

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

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

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

### **2.3 Training and Information Review**

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

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

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

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

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

#### **2.4 Removal of Category Designation**

At some point, Confidential Information may no longer be considered Confidential and should therefore have its designation removed or eliminated. This may occur as a result of any number of circumstances, including changes within the Policy, the changing nature of information security, a better understanding of particular material, and/or changes in public policy or law, among others. In order to determine whether category designations should be removed from particular materials, the CISO may establish criteria for the periodic review of all sensitive material. In any case, the category designation of any particular Confidential Information may not be removed without the approval of the CISO. A record of any removal of categorization for particular information must be kept by the DISO, with a copy provided to the CISO.

## **CHAPTER 3 – INFORMATION ACCESS**

### **3.1 Applicability**

Each employee, consultant, third-party contractor, tenant, individual and/or entity requiring, or requesting, access to Port Authority Confidential Information must adhere to the requirements set forth in this Handbook.<sup>1</sup> Confidential Information is intended for official business use only. Failure to abide by the procedures set forth in the Handbook can lead to a denial of access privileges to Confidential Information and/or other contractual, civil, administrative or criminal action.

All employees, consultants, third-party contractors, individuals and/or entities given access privileges to Confidential Information are responsible for overseeing the safeguarding and protection of Confidential Information in their possession or under their control as per this Handbook's requirements. Questions concerning the safeguarding, protection, release, and/or access to Confidential Information should immediately be brought to the attention of the CISO, DISO, SPM, or SIM, as may be appropriate, in the particular circumstance.

### **3.2 General Criteria**

In order for access to Confidential Information to be considered for approval, all individuals including PA staff, must meet and complete the following criteria:

- Be a citizen of the United States of America, or be an alien who has been lawfully admitted for permanent residency or employment (indicated by immigration status), as evidenced by Immigration and Naturalization Service documentation, or be a national of the United States as defined by the Immigration and Nationality Act. This requirement may be waived by the CISO with the concurrence of the Director of Public Safety and/or the CSO where and when circumstances so require.
- Obtain sponsorship for a request to be given access to Confidential Information through the individual's assigned chief, director, manager, or supervisor. The written request must include justification for access, level of access required, and indicate the duration for which access privileges are required.
- Forward the request through the individual's supervisory chain to the CISO, via the appropriate DISO, SPM, or SIM, requesting that a specific background check be undertaken, where appropriate and/or required.
- Complete the Port Authority Information Security Education and Awareness Training.
- Execute a Port Authority NDA (See Appendix A), or an Acknowledgement of an existing executed NDA, or, if the individual is Port Authority represented staff, have been provided with the NDI. This requirement may be waived if approved by the CISO.

---

<sup>1</sup> The CISO in consultation with the Law Department may modify and/or waive the condition of complying with the requirements of the Handbook where such compliance is impractical, such as in the case of a governmental entity having its own information security procedures and/or protocols governing the handling and protection of sensitive information. In addition, certain sensitive information is required to be submitted to other governmental entities under applicable laws, rules or regulations, or the Port Authority may elect to submit Confidential Information to a governmental entity, such as in the case of the CII process, wherein it may elect to submit Confidential Information to the Department of Homeland Security in order to secure the protection of the CII regulatory scheme.

- Be granted final approval of the security clearance level, in writing, by the CISO who verifies that all requirements have been met.

The individual's name must be entered on the appropriate department, project, or company Authorized Personnel Clearance List. See Sec. 3.9 for more information regarding this List (Note: If an individual's name does not appear on the appropriate Authorized Personnel Clearance List, access must be denied).

Individuals who meet and complete the criteria listed above are neither guaranteed, nor automatically granted, access to Confidential Information, since access is conditioned on need to know criteria. The OIG may access, without approval of the CISO, DISO, SPM or SIM, all Confidential Information when it is needed in connection with an OIG investigation, audit or inspection work, or any other Port Authority related work, subject to the handling requirements set forth in this Handbook.

### **3.3 Information Access Controls**

Access to all Confidential Information falling within any of the Port Authority Information categories shall be undertaken in a manner that complies with and maintains all applicable state, federal and common law protections. Access to particular Information must be conditioned upon a strict need to know basis with regard to the particular, discrete Information, regardless of any federal security clearance, or other Port Authority or other organizational information access authorization. An individual's need to know is not established simply by reason of the individual possessing a recognized federal security clearance, including one that allows for access to a higher level of classified information than is otherwise required for the discrete Port Authority Information to which access is sought. All requests for access to SSI by anyone who does not possess the requisite "need to know" under SSI regulations must be reported to the Transportation Security Administration ("TSA") or, if applicable, the United States Coast Guard ("USCG") and, in certain instances, the Department of Transportation ("DOT").

#### **(a) Confidential Information**

Access to Confidential Information shall be on a need to know basis only, as determined by the DISO. In certain instances access privileges may be conditioned on the satisfactory completion of a background investigation(s). The background investigation should utilize the least stringent criminal history access disqualification criteria that is appropriate for granting access to the particular information for both Port Authority and non-Port Authority employees. Where a background investigation is a condition to granting access, a DISO may determine that periodic updates of such investigations are required as a condition to maintaining continued access privileges. Access by third parties to Confidential Information may require that the parties execution a NDA or an Acknowledgment of an existing NDA if the CISO determines that a NDA and/or Acknowledgment is required.

#### **(b) 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 Information only to the extent

that it is necessary and/or is required by the individual in order to fulfill and/or carry out his/her duties, obligations and responsibilities to the Port Authority. Access to Confidential Privileged information may be subject to the satisfactory completion of periodic background investigations for both Port Authority and non-Port Authority employees. A list of disqualifying crimes for the different levels of background screening is attached as Appendix "C." A more stringent background investigation may be required of the individual for access to certain Confidential Privileged Information if determined by the CISO. All access to such Information must be granted and received in a manner that does not compromise or abrogate the particular privilege attaching to the Information.

Confidential Privileged Information may not be disclosed to any individual without appropriate prior approvals. Approval for disclosure of Confidential Privileged Information to third parties must be obtained from the CISO. A Port Authority employee or other individual may not waive any privilege attaching to Port Authority Information without the Port Authority's express permission as granted by the CISO, unless the Information to which the Port Authority asserts a privilege is personal to a particular employee or individual and the privilege is directly derived by reason of that circumstance. Access by third parties to Confidential Privileged Information will be conditioned on the parties' execution of a NDA or an Acknowledgment of an existing executed NDA, as may be appropriate and determined by the CISO. In certain circumstances, a Memorandum of Understanding or Memorandum of Agreement containing approved non-disclosure and confidentiality requirements may be utilized, in which cases approvals are required from the CISO and the General Counsel, or their respective designees. In the case of certain represented employees/individuals, NDIs may be utilized in lieu of NDAs.

### **3.4 Access Disqualification**

Any employee, consultant, third-party contractor, or other individual and/or entity, who has been granted access to Confidential Information, may be temporarily denied access while an investigation is conducted regarding any report to the CISO, OIG and the DISO that such individual misused, mishandled, or lost Confidential Information, or disclosed, disseminated, or released Confidential Information to an unauthorized individual or entity. Further, access to Confidential Information can be denied when improper or incomplete verification checks of employees, entities, or individuals are discovered. Where it is determined that an individual has misused, mishandled or otherwise improperly disclosed, released or disseminated Confidential Information without authorization, that individual may be subject to disqualification of access privileges and may also be subject to sanctions, including formal disciplinary actions where the individual is a PA employee, with possible penalties up to and including termination of employment. The foregoing action shall be documented and provided to the individual's employer, SPM, DISO, or departmental manager and the CISO, as may be appropriate. In the case of third parties, remedial action may include, but is not limited to, imposition of a monitor to oversee compliance with information security and general security requirements, or possible disqualification, and/or termination of present and/or future business relationships. Individuals and entities may also be subject to criminal or civil legal action, as may be appropriate. Additionally, see Chapter 6 regarding the possible consequences of violations of this Policy.

### **3.5 Non-Disclosure and Confidentiality Agreements (NDAs)**

Employees, consultants, third-party contractors, tenants, or other individual or entities, including governmental agencies where appropriate, will be required to sign NDAs or an Acknowledgment of an existing NDA, or be subject to an NDI, as a condition of being granted access to Confidential Privileged Information and, where appropriate, Confidential Information. Employees, consultants, third-party contractors, or other agency personnel who refuse to sign a NDA, in situations where it is required, will be denied access to Confidential Information, except in the case of certain employees and third parties where a NDI may be utilized in instructing and advising the employee and/or third party of the obligations and the requirements for handling Confidential Information. The DISO is responsible for determining whether a NDA/NDI is required as a condition to being granted access privileges to Confidential Information, other than Confidential Privileged Information. If an individual refuses to execute an individual Acknowledgment, or to receive the NDI, access to the Confidential Information is to be denied. The SIM is also responsible for keeping proper documentation for employees and individuals subject to NDIs, including the date when the individual was given the NDI and by whom. A copy of all executed agreements and acknowledgements are to be provided to the SIM. Original executed NDAs shall be forwarded to the CISO for filing in the official Port Authority records repository.

### **3.6 Unauthorized Disclosure of Information**

If employees, consultants, third-party contractors, or other individuals and/or entities with authorized access to Confidential Information become aware that Confidential Information has been released to unauthorized persons, they are required to immediately notify the CISO, the Office of Inspector General, and any other appropriate information security officer and report the discovery. In the case of SSI, the CISO must inform the TSA, DOT, or USCG and, in the case of CII, the Department of Homeland Security (“DHS”), of the breach of security. DOT, DHS, TSA and USCG rules govern the reporting of any unauthorized disclosure.

### **3.7 Security Clearance and Access Prohibitions**

Access to Confidential Information is not a right, privilege, or benefit of employment by the Port Authority, rather it is based on pre-established guidance. Confidential Information should not be divulged, released, turned over, or provided to any individual in any organization who does not meet the established criteria or conditions set forth herein, or who has not been approved for a security clearance issued by the Port Authority CISO. The following security clearance and access guidelines and/or prohibitions are in effect to protect Confidential Information:

- Confidential Information shall only be used in the performance of required job responsibilities, or in order to complete assigned tasks as determined by the SIM and DISO, with the concurrence of the CISO. No other disclosure or use of Confidential Information is authorized.
- Individual access to Confidential Information will be rescinded when an employee, consultant, third-party contractor, individual or entity, who had been granted access to Confidential Information, is no longer employed by the Port Authority, or is no longer under contract with, or no longer has a relationship with the Port Authority, or is no longer in a position that requires access to Confidential Information in order for the individual or entity to perform duties or complete tasks/projects.

- Employees may not unilaterally sponsor themselves for background verification or enter their name on an Authorized Personnel Clearance List.
- Group access of organizations to Confidential Information should be prohibited. Each individual in a group must have security clearance to access Confidential Information.
- Persons who rarely, if ever, require access to Confidential Information, (i.e., maintenance, food service, cleaning personnel, vendors and other commercial sales, or service personnel, who perform non-sensitive duties), should not be approved for a security clearance.

### **3.8 Background Screening**

All background checks for third parties required under the Policy should normally be conducted through the "Secure Worker Access Consortium" (S.W.A.C.), which is presently the only Port Authority approved service provider of a background screening checks, except as otherwise required by federal law and or regulation. The Office of Emergency Management administers this provider. S.W.A.C. is accessed by an online application (<http://www.secureworker.com>) that enables the secure collection, processing, maintenance and real-time positive identity verification (PIV) of individuals. The S.W.A.C. background check is not a replacement for any federal agency (DHS, TSA, etc.) required background screening. S.W.A.C. membership is valid for one year, at the end of which the member must renew his online application. In addition, certain employees, such as those in the Public Safety Department, will have their criminal history background checked through the electronic databases maintained by federal and/or state law enforcement agencies when required as a condition of employment, or when required by federal or state laws, rules, and/or regulations, or, in certain cases, where it is legally permitted and is deemed appropriate by the CSO.

The SIM/SPM has authority to obtain the background check information from S.W.A.C. Additional information about S.W.A.C., corporate enrollment and online applications can be found at <http://www.secureworker.com>, or it may be contacted at (877) 522-7922. The S.W.A.C. application process is described in Appendix "D."

### **3.9 Authorized Personnel Clearance List**

The CISO will maintain a master list database containing the names of all employees, consultants, third-party contractors, and other individuals and/or entities that have been granted a Port Authority security clearance and the specific category for which the security clearance was received, including, but limited to, for a particular project, or for specific Confidential Information. The DISO, SPM, and SIM are responsible for compiling, maintaining, and updating their respective list databases on an ongoing basis and forwarding the information to the CISO for compilation into a master listing. Each DISO shall periodically review its department's/business unit's list with its SPM and/or SIM to ensure that the list is current and that each individual's access to Confidential Information is still required.

### **3.10 Development of a Confidential Information Practices and Procedures (CIPP)**

Departments, offices and/or business units may adopt an individualized, discrete CIPP tailored to their respective particular business practices for handling Confidential Information. The CIPP is meant to augment the Handbook and must be consistent with it. Each CIPP must be approved by the CISO before being implemented.

### **3.11 Procurement Strategies**

#### **(a) General**

As a public agency, the Port Authority has an established procurement process based on openness, integrity, and fairness to the vendor community. The security of Confidential Information must be incorporated at the beginning of the procurement process in order to establish a security benchmark that may be applied throughout the procurement process, as well as during the term of the award/contract.

#### **(b) Lifecycle Phases and Procurements**

A project may contain Confidential Information in one or more of its lifecycle phases (pre-award, award, design, construction, close-out, or maintenance/service operation contracts, etc.).

Procurement and lifecycle information should be thoroughly reviewed by the originator before being submitted to the Procurement Department for processing. If Confidential Information is discovered thereafter by Procurement, or any reviewing department, the originator's department manager or designee should be contacted immediately to retrieve the Confidential Information and process it in accordance with the Policy and this Handbook.

#### **(c) Risk Exposure and Business Risk Strategy**

Procurement shall develop and retain, by project, a current listing of pre-screened persons or pre-qualified firms to bid on sensitive projects who agree to abide by the Policy requirements. Requirements must be included in procurement documents in order to help reduce potential disclosure of Confidential Information and to provide bidders with certain security requirements in advance. They must also be included in contract awards to ensure information protection practices, procedures, and protocols are included in each project's lifecycle phase. The typical requirements are:

**(i) Non-Disclosure and Confidentiality Agreements (NDA).** Require prospective consultants, prime vendors, or commercial enterprises to enter into a NDA with the Port Authority before obtaining a copy of a RFP. NDAs should be project and procurement specific and should be completed in a timely manner for specific types of procurements or projects. A broad or generic NDA should not normally be utilized to cover all procurements and projects under contract to a particular vendor over a long period of time, however, it may be appropriate in certain situations to utilize such a NDA, if approved by the DISO with the concurrence of the CISO. Vendors should contact the Port Authority to request authority to release the information prior to releasing RFP information to a sub-contractor. The sub-contractor may have to execute an Acknowledgement that it will comply with the terms of any NDA that the successful bidder has executed.

**(ii) Background Screening.** Require potential users seeking access to Confidential Information to undergo background pre-screening. The pre-screening may parallel the screening requirement used by the Port Authority to grant access to Confidential Information under Section 3.3. S.W.A.C.'s background screening is usually finalized within five to ten business days.

**(iii) Designation of a Security Information Manager (SIM).** Require companies involved in Confidential Information procurements or projects to designate a SIM to ensure information security and Confidential Information requirements are followed. A second employee may be designated as an alternate SIM.

**(iv) Information Security Education and Awareness Training.** Require consultants, vendors, contractors and commercial enterprises to attend training to ensure security awareness regarding Port Authority information.

**(v) Physical Security.** Outline the specific guidelines and requirements for the handling of Confidential Information to ensure that the storage and protection of Confidential Information is consistent with the requirements of Chapter 4 of this Handbook.

**(vi) Transfer or Shipping Sensitive Information.** Prohibit or place restrictions on the transfer, shipping, and mailing of Confidential Information consistent with the handling procedures set forth in Chapter 4 of this Handbook.

**(vii) Website Restrictions.** Prohibit posting, modifying, copying, reproducing, republishing, uploading, transmitting, or distributing Confidential Information on websites or web pages. This may also include restricting persons, who either have not passed a pre-screening background check, or who have not been granted access to Confidential Information, from viewing such information.

**(viii) Destruction of Documents.** Require Confidential Information to be destroyed using certain methods, measures or technology consistent with the requirements set forth in Chapter 4 of this Handbook.

**(ix) Use of Similar Agreements Between Prime Vendor and Subcontractors.** Require the prime vendor or general contractor to mandate that each of its subcontractors maintain the same levels of security required of the prime vendor or general contractor under any Port Authority awarded contract.

**(x) Publication Exchanges.** Prohibit the publication, exchange or dissemination of Confidential Information developed from the project or contained in reports, except between vendors and subcontractors, without prior approval of the Port Authority. Requests for approval should be routed to and reviewed by the CISO in conjunction with the Law Department and, where appropriate, Public Affairs.

**(xi) Information Technology.** Matters involving information technology policy, or use of particular hardware or software, should require the application of specific protocols and/or software tools to support Port Authority projects. Coordination of information technology and consultation with the CTO and the CISO may be required for the success of particular projects.

**(xii) Audit.** Include provisions to allow the Port Authority to conduct audits for compliance with Confidential Information procedures, protocols and practices, which may include, but not be limited to, verification of background check status, confirmation of completion of specified training, and/or a site visit to view material storage locations and protocols.

**(xiii) Notification of Security Requirements.** Advise all consultants, third-party contractors, and other individuals and/or entities, as may be appropriate, that Port Authority security procedure requirements may be imposed throughout the duration of the project.

**(xiv) Reproduction/Copies.** Reproductions of Confidential Information shall be consistent with the requirements of Chapter 4 of this Handbook.

## **CHAPTER 4 – MARKING, HANDLING, STORAGE, TRANSMITTAL AND DESTRUCTION REQUIREMENTS**

### **4.1 Marking of Confidential Information**

#### **(a) Confidential Privileged Information and Confidential Information**

All documents, drawings, and all other Information that contain Confidential Privileged Information or Confidential Information must be marked with the appropriate respective protective marking: “CONFIDENTIAL PRIVILEGED” (alternatively “CONFIDENTIAL AND PRIVILEGED”) or “CONFIDENTIAL” (alternatively, where appropriate, Confidential Proprietary Information). The markings must be conspicuous and in bolded Arial with a 16 point font size. All copies of Confidential Information, Confidential Privileged Information, Sensitive Security Information, and Critical Infrastructure Information documents shall also bear the required markings and warnings.

The front page (or front and back cover, if appropriate) shall be marked at the top and bottom of the page. In addition, all interior pages within the document must also be marked at the top and the bottom of the page. Sets of documents large enough to be folded or rolled must be marked or stamped so that the marking is visible on the outside of the set when it is rolled or folded. The marking must be visible from the exterior container of the material, e.g., the spine of a binder, or compact disc container or cover.

All Confidential Privileged Information and Confidential Information must bear the following warning sign on its front cover, back cover, and title sheet or first page. For compact discs, DVDs or other smaller materials, the warning sign may be printed on an adhesive label and affixed to the material. It should be in 8-point font size and state:

"WARNING": The attached is the property of The Port Authority of New York and New Jersey (PANYNJ). It contains information requiring protection against unauthorized disclosure. The information contained in the attached document cannot be released to the public or other personnel who do not have a valid need to know without prior written approval of an authorized PANYNJ official. The attached document must be controlled, stored, handled, transmitted, distributed and disposed of according to PANYNJ Information Security Policy. Further reproduction and/or distribution outside of the PANYNJ are prohibited without the express written approval of the PANYNJ.

At a minimum, the attached will be disseminated only on a need to know basis and, when unattended, will be stored in a locked cabinet or area offering sufficient protection against theft, compromise, inadvertent access and unauthorized disclosure.

#### **(b) Sensitive Security Information Requirements**

Pursuant to the federal regulations governing SSI, Port Authority Confidential Privileged Information that has been designated SSI by the Federal government must be conspicuously marked with its respective protective marking “SENSITIVE SECURITY INFORMATION” on the top and the distribution limitation statement on the bottom of each page of the document

including, if applicable, the front and back covers, the title page, and on any binder cover or folder. The protective marking must be in bolded Arial 16-point font size and the distribution limitation statement must be in an 8-point font size. All copies of SSI documents must also bear the required markings.

The distribution limitation statement is:

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the TSA or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

**(c) Critical Infrastructure Information**

Pursuant to the federal regulations governing CII, Port Authority Confidential Privileged Information that has been marked PCII by the Department of Homeland Security PCII Program Manager or the manager's designee will be marked as follows:

This document contains PCII. In accordance with the provisions of 6 CFR Part 29, this document is exempt from release under the Freedom of Information Act (5 U.S.C. 552 (b)(3)) and similar laws requiring public disclosure. Unauthorized release may result in criminal and administrative penalties. This document is to be safeguarded and disseminated in accordance with the CII Act and the PCII Program requirements.

**(d) Document Control Number for Confidential Privileged Information**

Documents that have been identified as Confidential Privileged Information will be given a control number, which shall consist of the category of information followed by an acronym for the transmitting department, followed by the last 2 digits of the year, followed by a number that is sequential and, finally, followed by the copy number.

Examples:

C&P – LAW – 05 – 1 – 1

C&P – PMD – 07 – 10 – 2

The front page (or front and back cover, if appropriate) and all pages of Confidential Privileged Information shall be marked with the control number. The control number must also be visible from the exterior container of the material, e.g., the spine of a binder, or compact disc container or cover.

## 4.2 Handling Confidential Information

Handling refers to the physical possession of, and includes working on or with, Confidential Information to perform job duties or complete tasks or projects. This includes, but is not limited to, reading, copying, editing, creating, or correcting the material. Confidential Information in any form, including physical or electronic, must be under constant surveillance by an authorized individual to prevent it from being viewed by, or being obtained by, unauthorized persons. Confidential Information is considered to be in use when it is not stored in an approved security container.

The following is a chart of the minimum-security requirements for handling Confidential Information, and certain requirements that apply only to Confidential Privileged Information:

Minimum Security Requirements for Handling	Confidential Privileged Information	Confidential Information
Must never be left unattended outside of storage location.	X	
Must be under the direct and constant supervision of an authorized person who is responsible for protecting the information from unauthorized disclosure.	X	
Must be turned face down or covered when an unauthorized person is in the vicinity. Be cognizant of others in area that can view your computer screen.	X	X
When leaving a computer unattended ensure that the screen is locked.	X	
Attach an information cover sheet when removing materials from their place of storage.	X	
Use all means to prevent unauthorized public disclosure of information.	X	X

## 4.3 Transmittal of Confidential Information

Transmission refers to the sharing among individuals and/or entities, and/or the transfer or movement of Confidential Information from one location to another using either physical or electronic means. The following chart sets forth the methods by which Confidential Information should be transmitted. In all instances, Confidential Information must at all times be safeguarded and transmitted in a manner and method designed to insure that it is not disclosed, or otherwise compromised, and it should be appropriately marked with the proper identifying marking.

In general, all Confidential Privileged Information must be signed in and out, and, in certain situations as determined by the SIM or SPM, Confidential Information may be signed in and out as well. A cover sheet must be attached to the Confidential Privileged or, in certain situations as determined by the SIM, to Confidential Information and it should be marked appropriately. With respect to Confidential Privileged Information, the coversheet attached as Appendix "E" is to be utilized to draw emphasis to the fact that a document contains Confidential Privileged Information and to limit visual exposure to unauthorized individuals in near proximity. Confidential Privileged Information and, where appropriate, Confidential Information, must be wrapped and sealed. The exterior of the wrapping should not indicate that it is sensitive material, or its category, or level. Confidential Information transmitted by email must state at the top of the email in bold uppercase letters "CONFIDENTIAL INFORMATION."

Confidential Privileged Information may be transported using public modes of transportation, and a courier service may also be utilized; provided, however, that the sign in and sign out procedures will apply, as well as wrapping and sealing procedures. All packages must be sealed in a manner that easily identifies whether the package has been opened prior to delivery to the intended recipient. The use of a double wrapped/enveloped package or a tamper resistant envelope must be used to fulfill this requirement. Protective markings are not to be placed on the outer visible envelope. If using a double wrapped package or two envelopes, the inner wrapping or envelope should be marked in accordance with appropriate category designation. The package must be addressed to an individual who is authorized to receive it or, preferably, to the SIM. All packages must contain a specific individual's name on the shipping label. Where appropriate any of the foregoing requirements may also be required in handling Confidential Information and can be provided for generally in the department's CIPP, or as required by the DISO and/or SIM with respect to handling such information in specific instances.

Minimum Security Requirements for Transmission	Confidential Privileged Information	Confidential Information
Verbally at a meeting, conference or briefing where all attendees have the appropriate security clearance	X	X
Electronic Systems: restrict to the Livelink <sup>2</sup> network or a similar secure repository	X	
Electronic Mail: restricted from using e-mail accounts to transmit unless expressly permitted by the SIM in writing	X	
Hand Carried or delivered in the personal custody of Port Authority employee: (a) request return receipt (b) place in sealed envelope, and (c) name of recipient, department, address and phone number must be written on face of envelope	X	
Approved Commercial Delivery Service (e.g., DHL, FedEx, UPS): (a) request return receipt, (b) verify recipient name and mailing address, (c) place in a sealed envelope, and (d) the exterior of a		

---

<sup>2</sup> Livelink is a secure repository for the records of a project.

mailing document shall not indicate the security category of the material contained therein	X	X
Use of USPS Certified Mail: (a) request return receipt, (b) verify recipient name and mailing address, and (c) the exterior of a mailing document shall not indicate the security category of the material contained therein	X	X
Intra-agency Mail System (a) request return receipt (b) place in sealed envelope, (c) name of recipient, department, address and phone number must be written on face of envelope, and (d) the exterior of a mailing document shall not indicate the security category of the material contained therein	X	X (b, c, d only)
Telephone: restricted from using a telephone to transmit, unless expressly permitted by SIM in writing. If approved: (a) use all means to prevent unauthorized public disclosure, and (b) may not use cell phone	X	
Fax Machine: restricted from using fax machine to transmit unless expressly permitted by the SIM in writing. If approved: (a) prior coordination with recipient required, (b) verify recipient fax number, (c) receipt of successful transmission, and (d) follow-up contact required	X	X(a,b,c only)

Steps for transmittal of a “hard copy” of all Confidential Privileged Information and, when required, for Confidential Information:

- Step 1. Make certain that documents are properly marked: “CONFIDENTIAL PRIVILEGED” or “CONFIDENTIAL,” according to its designated category.
- Step 2. Prepare Transmittal Receipt (Appendix “F”).
- Step 3. Place document in envelope with the Transmittal Receipt, seal envelope, mark the inner envelope CONFIDENTIAL PRIVILEGED or CONFIDENTIAL, place envelope in second envelope (outer), this envelope shall not contain any protective markings.
- Step 4. Address envelope to an individual who is authorized to receive it.
- Step 5. Mail document.
- Step 6. The Transmittal Receipt shall be returned to the party who initially sent the item.

When hard copies of 8 1/2 " X 11" multi-page documents include threat scenarios, asset criticality information, identification of security vulnerability details, risk assessments, design

basis threats and concepts of operations are distributed, this information is to be bound using heat sensitive binding to prevent individual sheets from being removed from a set.

#### **4.4 Storage of Confidential Information**

Steps should be taken to prevent unauthorized access to Confidential Information. Confidential Information should be kept in a locked storage room or a locked security container, such as a drawer, cabinet or safe-type file that has a locking mechanism, and must be vandalism resistant. The DISO will periodically review the departmental storage vehicles and mechanisms and determine their appropriateness for the information being stored. Confidential Information should be gathered and stored in a minimum number of office locations and Confidential Privileged Information must never be left unattended outside its storage location. A storage space or security container/receptacle may not be left open and unattended at any time. At no time should Confidential Information be stored, even for short periods, in unauthorized desk drawers, file cabinets, or other unsecured locations. The CISO may require that certain information be kept in a safe in a designated central location(s).

Combinations or locks for each security container must be changed or replaced when a person having knowledge of the combination or possession of a lock key no longer requires it, or there is reason to suspect that the combination has been tampered with, or that an unauthorized person may have acquired knowledge of the combination, or that a lock key is in the possession of an unauthorized person. Keys and combination locks protecting Confidential Information must be protected at the same level of protection as paper documents. The "Guidelines for the Storage of Confidential Information" attached as Appendix "G" provides further detailed information and instructions.

Confidential Privileged Information and, where appropriate Confidential Information, may not be stored at any individual's home overnight for a meeting the following day without prior authorization of the SIM or DISO.

Downloading of any Confidential Privileged Information and Confidential Information carries with it the responsibility to protecting that information in accordance with the procedures identified in this Handbook. The possessor of the electronic file assumes full responsibility for the proper handling, storage and transmittal of this Confidential Privileged Information and Confidential Information.

#### **4.5 Document Accountability Log**

All entities, Port Authority Departments and third-parties having Confidential Information in their possession will have a system in place that will account for the material in such a manner that retrieval is easily accomplished for inspection. The accountability log shall be maintained by the DISO, or the SPM, or SIM, where applicable, and include:

- The date that a document was received or created
- The identity of the sender or creator
- A brief description of the document
- The Control Number, if Confidential Privileged Information
- Number of copies

- Transmission history (sent to whom, when)
- If applicable at the time of the inspection, a Port Authority Records Destruction Certification (PA Form #283) stating that the document has been destroyed (including, when, by whom and the method), or a Certification that the document has been returned to the Port Authority.

#### **4.6 Reproduction**

Confidential Information should only be reproduced to the minimum extent necessary to carry out an individual or entity's responsibilities. However, the reproduced material must be marked and protected in the same manner and to the same extent as the original material. Authorized individuals must perform all reproduction work. Print and reproduction locations are limited to Port Authority sites, or, when appropriate, to authorized consultant and/or third-party contractor work site equipment. The CISO may require that the work site should limit reproduction of Confidential Information to a particular copying machine with technological capabilities limited to copying (not scanning or storing etc.). Service providers, authorized by the responsible SIM or DISO where appropriate, may be used for this task if the information remains safeguarded throughout the process. Each reproduction of Confidential Information shall contain all security markings, instructions, etc., as set forth in Section 4.1. All scraps, over-runs, and waste products resulting from reproduction shall be collected and processed for proper disposal.

#### **4.7 Destruction of Confidential Information**

All Confidential Information that is no longer needed shall be disposed of as soon as possible, consistent with the Port Authority's Record Retention Policy, by any method that prevents its unauthorized retrieval or reconstruction. The individuals who had been granted access to Confidential Information must perform the actual destruction. Authorized service providers may be used for this task provided that the information remains safeguarded until the destruction is completed. Paper products must be destroyed using a cross cut shredder located in the office. As previously noted in Section 4.5, a Port Authority Records Destruction Certificate (PA Form #283) must be provided to the DISO, SPM or SIM for any document being destroyed, including original or copies thereof, and provided to the CISO for final approval by the Secretary or her/his designee. In addition to the requirements in this Handbook, all Departments shall continue to comply with the Port Authority Records Program (A.P. 15-2.02). Where Confidential Information is no longer needed, but the Port Authority Records Program requires retention of the original, the original Confidential document shall be retained by the CISO and all copies are to be destroyed in accordance with this section. The "Guidelines for the Disposal and Destruction of Confidential Privileged Information" attached as Appendix "H" provides further detailed information and instruction.

Since deleted electronic files can be recoverable by utilizing software tools, Confidential Information stored in electronic form needs to be erased and destroyed with methods that comply with the US Department of Defense standards for file secure erasure (DoD 5220.22). Therefore, CyberScrub or a similar software shall be used to prevent discovery by a computer technician or other unauthorized person. With respect to Port Authority staff, individual staff shall contact the Technology Services Department ("TSD") to make a request that Confidential Information be permanently removed from a computer. This request shall be made by providing relevant information on a TSD form through the Internet or by email.

## **CHAPTER 5 – AUDITING AND MONITORING**

### **5.1 Purpose**

The ISSC, Audit and/or OIG may conduct random or scheduled examinations of business practices under the Policy in order to assess the extent of compliance with the Policy. The Policy's self-assessment and audit processes enable management to evaluate the Policy's uniformity throughout the Port Authority and of third parties' practices, in order to identify its strengths and potential exposures, and to help guide evolving policy objectives.

### **5.2 Audits and Investigations**

Audits conducted by the ISSC and/or Audit may be scheduled in advance. The chief, department director, project manager, company liaison or contract representative of the organization being assessed should receive prior notice of the date of the assessment and also be advised as to what the assessment will consist of. A copy of the current version of the Audit Procedures guidelines, attached as Appendix "H", should be provided to the particular entity(ies) in order to allow adequate time to undertake appropriate pre-review and preparation action. The Audit Procedures guidelines should guide the ISSC and/or Audit through the assessment process. This Guideline is not all-inclusive and may be amended, as necessary. Organizations, departments, units, or third parties, preparing for an ISSC and/or Audit visit are encouraged to contact the CISO prior to the scheduled visit date in order to inquire and obtain additional information about the process.

The ISSC and/or Audit may also conduct information security assessments without prior notice and/or unannounced investigations coordinated through the Office of the General Counsel and the Office of Inspector General, as it may deem necessary and appropriate. Where appropriate, the CISO should be advised of the existence of such an investigation and, if appropriate, its nature.

The ISSC and/or Audit approach to conducting an assessment should consist of three phases (i) personnel interviews, (ii) site assistance visits, and (iii) corrective action follow-up.

#### **(i) Personnel Interviews**

The interview(s) should focus on the department, business unit, organization or third party's compliance with the Policy, how engaged the interviewee is with the Policy, and the level of education and awareness the interviewee has about the Policy. Employees, consultants, third-party contractors, and other individuals and/or entities should be included as potential interviewees. Personnel interviews should encompass a wide range of individuals who are regularly engaged with the Policy, as well as those having less involvement in it. This allows the ISSC to develop a balanced understanding regarding Policy compliance and effectiveness, as well as its impact on the organization and enable it both to identify concerns and issues regarding the Policy, and to solicit recommendations for possible improvements to the Policy.

**(ii) Site Assistance Visits**

The ISSC and/or Audit site visit should focus on a hands-on review of the following processes and procedures: document safeguards, handling protocols, transmission practices, control number usage, document marking, receipt and copying practices, and disposal of Confidential Information procedures. The visit should also include compliance reviews of the security clearance access criteria, document accountability audits, conditions regarding information access, background check processes, Authorized Personnel Clearance Lists updates, Confidential Information material sign out and sign in records, and the information security education awareness training program.

**(iii) Follow-up**

Policy compliance deficiencies noted during the assessments should be provided by the ISSC and/or Audit through the CISO to the department head, chief, project manager, consultant, third-party contractor liaison/representative, other agency staff, and the respective DISO, SPM, or SIM for corrective action. The ISSC, through the CISO, may also follow-up on investigation results to determine corrective actions and Policy compliance. The ISSC may also recommend the imposition of any penalties or disciplinary action that are described in Chapter 6.

With the assistance of the respective DISO, SPM, or SIM, a plan with milestones should be developed with the intention of correcting any identified deficiencies. A return site assistance visit may be scheduled in order to re-assess earlier identified deficiencies. The respective DISO, SPM, or SIM should forward a periodic corrective action progress report to the CISO as part of the milestone monitoring.

**5.3 Self-Assessment**

Department heads, chiefs, managers, supervisors, DISOs, SPMs or SIMs should conduct an annual self-assessment of their unit's Policy compliance using the Audit Procedures Guidelines. The results will not be forwarded to the CISO, Audit or ISSC, but should be used as a tool to gauge compliance before regular assessments are conducted. The results should be available for inspection and any serious findings should be forwarded to the CISO.

## **CHAPTER 6 – POLICY VIOLATIONS AND CONSEQUENCES**

### **6.1 Responsibilities**

Anyone having knowledge of any infraction, violation or breach of the Policy is required to report it to the OIG and to their supervisor, who shall in turn report the same to the DISO. The CISO shall have the final decision with respect to the violation determinations and/or the recommended course of action to be taken, consistent with Port Authority policy, practices and legal requirements referenced in this section.

All individuals who have been reported as having violated the Policy may be temporarily denied access to Confidential Information and/or have their security clearance suspended until an investigation is completed.

### **6.2 Violations, Infractions, or Breach of Information Security Protocols**

Due to any number of unintended circumstances or, other conditions beyond the control of an individual, Confidential Information could be subject to compromise or loss. For example, an individual may unintentionally discard Confidential Information, mislabel Confidential Information, sent through the internal mail routing system, or drop or inadvertently leave Confidential Information in a public place. Intentional disclosure of Confidential Information to unauthorized individuals for personal gain, or to otherwise make available for unauthorized public release, may also occur. Violations, infractions and breaches of the Policy will be reviewed on a case-by-case basis to determine the facts and circumstances surrounding each incident.

### **6.3 Violation Reporting, Investigation and Fact Finding**

Individuals must report alleged or suspected violations, infractions or breaches of the Policy to the OIG and to their supervisor or manager. The supervisor or manager must refer the issue and/or the individual to the DISO. The DISO, in consultation with the CISO and OIG, will determine whether an investigation into the allegations or other appropriate action is warranted. The CISO will consult with the OIG on these matters and the OIG will determine whether to undertake its own separate investigation into the matter. Individuals and/or entities must cooperate with all authorized investigations of any act, omission or occurrence relating to Port Authority property, information, materials, and, in the case of Port Authority employees, and if applicable, must comply with the Agency General Rules and Regulations. (See *“General Rules and Regulations for all Port Authority Employees.”* Port Authority of New York and New Jersey. April 1990.)

### **6.4 Disciplinary Action**

The following is a list of Policy violations and the respective disciplinary actions that may be taken against any individual and/or entity, having authorized access to Confidential Information, who violates their responsibilities in handling such information:

- a) Non-deliberate violations involving negligence and/or carelessness, such as leaving Confidential Information unattended.

First Offense: Verbal reprimand and security briefing.

Second Offense: Written reprimand and/or a security briefing and possible suspension or termination of access privileges, depending on the circumstances.

Third Offense - Termination of access and possible imposition of civil penalties. Where the offense involves a Port Authority employee, disciplinary action may also be taken.

- b) Non-deliberate violation involving negligence and/or carelessness such as misplacing or losing a document.

First Offense - Written reprimand and/or a security briefing, and possible suspension or termination of access privileges, depending on the circumstances, and possible imposition of a civil penalty. Where the offense involves a Port Authority employee, disciplinary action may also be taken.

Second Offense - Dismissal or termination of access privileges, and, depending on the circumstances, the imposition of a civil penalty, and possible legal action against the violator. Where the offense involves a Port Authority employee, disciplinary action may also be taken including suspension with forfeiture of up to one year's personal and vacation time allocation.

- c) For cases of deliberate disregard of security procedures or gross negligence in handling Confidential Information.

First Offense – Suspension or termination of access privileges, termination of an agreement or contract, written reprimand, imposition of a civil penalty depending on the circumstances, and possible legal civil and/or criminal action against the violator. Where the offense involves a Port Authority employee, disciplinary action may be taken up to and including termination of employment. Termination of access privileges will be for a period of one year at minimum and may be permanent, subject to review by the CISO.

The Port Authority may also impose investigation costs and/or a monitor to oversee future compliance with its security policies and practices at the violator's expense, when the violation is by a consultant, vendor contractor or other third party. Nothing herein is construed to limit the Port Authority's right to exercise or take other legal rights and remedies including terminating agreements with a third party violator and/or refusing to enter into future business relationships with the violator and/or seeking such legal action, as it may deem appropriate, including injunctive, civil actions for monetary damages and/or seeking criminal prosecution of the violator(s).

In addition, any violation relating to SSI or CII will be reported to the TSA, the OIG, and/or, if applicable, DOT, USCG or DHS. Penalties and other enforcement or corrective action may be taken as set forth in relevant statutes, rules and regulations, including, without limitation, the issuance of orders requiring retrieval of Sensitive Security Information and Critical Infrastructure Information to remedy unauthorized disclosure and directions to cease future unauthorized disclosure. Applicable Federal Regulations, including, without limitation, 49 C.F.R. § 15.17 and 1520.17 and 6 CFR Part 29, provide that any such violation thereof or mishandling of information therein defined may constitute grounds for a civil penalty and other enforcement or corrective action being taken by the DOT, TSA and/or DHS.

## **CHAPTER 7 – INFORMATION SECURITY EDUCATION AND AWARENESS TRAINING**

### **7.1 Purpose**

Information security education and awareness training ensures that all personnel requiring access to Confidential Information, regardless of position or grade level, have an appropriate understanding of the need to adhere to security procedures in order to protect Confidential Information. The goal of the training program is basically to provide that all such employees, consultants, third-party contractors, other individuals, entities and/or, where appropriate, third parties develop essential security habits and thereby ensure that all personnel handling Confidential Information understand and carry out the proper handling protocols for those materials.

### **7.2 Overview**

The CISO is responsible for implementing the Information Security Education and Awareness Training Program (the “Training Program”). The Training Program, with assistance from the Office of Inspector General, DISO, SPM and SIM, should be provided to all employees, consultants, third-party contractors, and other agency personnel requiring access to Confidential Information. These individuals, regardless of rank or position in a particular organization, must complete initial indoctrination and annual refresher training. The CISO, with the concurrence of the Law Department, may waive this requirement for certain individuals. A current list containing the names of all persons who completed training will be developed and retained by the CISO. The CISO shall ensure that all employees have complied with the requisite Training Program.

### **7.3 Training Program Elements**

The Training Program consists of three interconnected elements: (a) indoctrination training, (b) orientation training, and (c) annual refresher training. Each element provides employees, consultants, third-party contractors, and other agency personnel with a baseline of knowledge, as well as periodic updates, about the existing and current Policy. Each element of the Training Program contributes another level of information to the individual. At a minimum, all individuals must receive the indoctrination training and the annual refresher training.

#### **(a) Indoctrination Training**

Indoctrination Training provides personnel with the fundamentals of the Training Program. It should be completed when beginning employment or assignment to a project for the Port Authority, but no later than sixty (60) days after initial hire, or after commencing work on a project. It may be combined with other types of new employee indoctrination programs. Individuals completing this level of training should understand the basic organization of the Policy, the Policy definitions, what materials are defined as Confidential Information under the Policy, how to identify Confidential Information (security category levels and markings), the general criteria and conditions required in order to be granted a security clearance, procedures for categorizing documents, the obligation to report suspected and alleged policy violations, and the penalties for non-compliance with the policy and for unauthorized disclosure of Confidential Information.

**(b) Orientation Training**

Orientation Training focuses on the more specific protocols, practices and procedures for individuals whose roles and responsibilities involve reading, using, safeguarding, handling, and disposing of Confidential Information. Individuals assigned such responsibilities should complete this level of training. Orientation training should be conducted prior to assignment to a department, project, task, or other special assignment, where the individual is expected to become involved with receiving and handling Confidential Information. Individuals completing this level of training should be introduced to the DISO, SPM, or SIM, understand the organizational elements of the Policy, know how to process Confidential Information, know the different security categories under their control or within their assigned work environment, know how to identify proper safeguarding protocols, including hardware needs, and understand the differences between general access privileges and the need to know requirement for access to particular information. Individuals should also read and acknowledge their understanding of the requirements.

**(c) Annual Refresher Training**

Once a year, during the anniversary month of the individual's start date on a project, or initial access to Confidential Information, all employees, consultants, third-party contractors, and other individuals and/or entities, who continue to have access to sensitive materials, should receive an information security education and awareness training refresher briefing to enhance their information security awareness. At a minimum, the annual refresher training should include indoctrination and orientation topic training, as well as key training on recent Policy changes or other appropriate information. Also, this milestone may be used to reaffirm the individual's need for a security clearance or to determine whether the individual requires a periodic update of their background check.

**(d) Other Circumstances and Special Briefings**

If a Port Authority employee, consultant, third-party contractor, or other individual and/or entity transfers to another department, is promoted within his or her department, or changes employers on the same project without a break in service, and can provide a record of completion of indoctrination training within the previous twelve months, only annual refresher training may be required. All other situations demand that an individual requiring access to Confidential Information fulfill the conditions for information security education and awareness training under this Policy.

In addition to reading and signing a NDA or an Acknowledgment of an existing NDA, or, alternatively, being subject to a NDI, temporary or one-time access individuals should be fully briefed on the limitations on access to Confidential Information and the penalties associated with the unauthorized disclosure, before being granted access to such information.

Special briefings may be provided on a case-by-case basis, as circumstances may require.