

THE PORT AUTHORITY OF NY & NJ

PROCUREMENT DEPARTMENT
2 MONTGOMERY STREET, 3RD FL.
JERSEY CITY, NJ 07302

March 6, 2014

ADDENDUM #2

TO PROSPECTIVE BIDDER(S) ON **BID #36617 - WORLD TRADE CENTER (WTC)
CCP LOCKER ROOM AND ELEVATOR REPAIRS**

Due back on March 27, 2014 no later than 11:00AM

The following changes are hereby made to the solicitation document:

I. BID SOLICITATION DOCUMENT

A. Invitation for Bid:

1. In the Part II Table of Contents, delete “7. Contract Documents” and replace with “7. Reference Documents”.
2. Delete Part II, Section 7 in its entirety and replace with the following:

7. Reference Documents

A. Confidential and Privileged Information

Upon request to Joann Spirito, 212-435-5640 or jspirito@panynj.gov, a copy of the non-confidential portion of the Reference Documents listed below will be made available to all bidders on a set of DVDs.

A portion of the Reference Documents is Confidential and Privileged Information. In order to receive this portion of the Documents, each bidder firm must assign an individual to serve as its Security Information Manager (SIM) and must assume responsibility for the firm’s compliance with the Port Authority’s Information Security Handbook.

If your firm already has a qualified and trained SIM, upon request to Joann Spirito, a copy of the Confidential and Privileged (C&P) portion of the Reference Documents will be made available on a set of DVDs. To be qualified, a SIM must have received training after January 1, 2013. With your request for C&P documents, please provide the date that your SIM received SIM Training.

If your firm does not already have a qualified and trained SIM, an individual, to be considered qualified and trained, must:

1. Undergo a background check through the Secure Worker Access Consortium (SWAC) Process and obtain a SWAC credential verifying that the individual has passed the background check; and
2. Sign Non-Disclosure Agreements (NDAs), or an Acknowledgment of an existing NDA, provided by the Authority.

To begin the SWAC process, go to the website:

<http://www.secureworker.com/>. Click on “Enroll or Renew Now” and follow the procedure on the website. The cost for the SWAC credential will not be reimbursed by the Authority.

Following receipt of the Reference Documents, the SIM must receive training in person from the Authority regarding the requirements for handling, receiving and controlling Confidential and Privileged information received from the Authority, as outlined in the “Information Security Handbook” as outlined in Section 34 of the Authority’s Standard Contract Terms and Conditions, regarding nondisclosure/confidentiality agreements. See Attachment C.

The next SIM training is scheduled for Wednesday, March 19, 2014 at 12:00 noon in the Authority offices at 115 Broadway. Please contact Malik Goodson at 212-435-5185 or mgoodson@panynj.gov to confirm your attendance at this training and/or to receive information on other SIM training sessions.

A copy of the Non-disclosure Agreements, instructions for their completion and a copy of the Training Materials that will be used at the March 19th Training Session are attached to this Notice to Bidders. For your reference, a copy of the Authority’s Information Security Handbook is attached to the Contract Documents as Attachment D.

B. List of Reference Documents

- 1) A complete set of the World Trade Center Central Chiller Plant & River Water System – CCP Package 1 (Conformed)
- 2) Specific Drawings that may aid in the understanding of the scope of work include:
 1. A101 – Floor Plan Level 242
 2. A401 – Reflected Ceiling Plan – Level 242
 3. A601 – Enlarged Locker Room Plans and Elevations
 4. A602 – Enlarged Locker Room Plans and Elevations
 5. M107 – Chiller Plant HVAC Plan – Level 242
 6. EP101 – Power Plan – Level 242

- 3) The rooms where the majority of the work will occur are:
 1. 109/109A – Female Locker Room & Vestibule
 2. 110/110A – Male Locker Room & Vestibule
 3. 111 – Storage
 4. 117 – Tool Storage
 5. 114--Machine Room
- 4) Exhibit C—CCP—SK-1—Photographic Views of Existing Conditions

II. BIDDER’S QUESTIONS AND ANSWERS

The following information is made available in response to questions submitted by prospective Bidder(s). It should not be deemed to answer all questions that have been submitted by Bidder(s) to the Port Authority. It addresses only those questions which the Port Authority has deemed to require additional information and/or clarification. The fact that information has not been supplied with respect to a question asked by a Bidder(s) does not mean or imply, nor should it be deemed to mean or imply, any meaning, construction, or implication with respect to the terms.

The Port Authority makes no representations, warranties or guarantees that the information contained herein is accurate, complete or timely or that such information accurately represents the conditions that would be encountered during the performance of the Agreement. The furnishing of such information by the Port Authority shall not create or be deemed to create any obligation or liability upon it for any reason whatsoever and each Bidder, by submitting its proposal, expressly agrees that it has not relied upon the foregoing information, and that it shall not hold the Port Authority liable or responsible therefor in any manner whatsoever. Accordingly, nothing contained herein and no representation, statement or promise, of the Port Authority, its directors, officers, agents, representatives or employees, oral or in writing, shall impair or limit the effect of the warranties of the Bidder(s) required by this Proposal or Agreement and the Bidder(s) agrees that it shall not hold the Port Authority liable or responsible therefor in any manner whatsoever.

1	<i>Question</i>	Will there be another walk through scheduled?
	<i>Answer</i>	Yes, an additional Site Inspection has been scheduled for March 13, 2014 at 10:00AM. See Addendum #1.
2	<i>Question</i>	Are there drawings and specifications available for this? I do not see any on the website.
	<i>Answer</i>	See Bid Solicitation Document changes above.

3	<i>Question</i>	Do you happen to know what the estimated \$\$ value for this project is?
	<i>Answer</i>	The estimate range is \$1 million to \$2 million.
4	<i>Question</i>	Do you have a list of attendees from the facility inspection?
	<i>Answer</i>	See attached sign-in sheet.

This communication should be initialed by you and annexed to your response to the above-referenced Bid 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.

QUESTIONS CONCERNING THIS ADDENDUM MAY BE ADDRESSED TO JOANN SPIRITO, WHO CAN BE REACHED AT (212) 435-5640 or at jspirito@panynj.gov.

THE PORT AUTHORITY OF NY & NJ

RICHARD PEREZ
PROCUREMENT MANAGER
FTA/WTC SITE PROJECTS

RESPONDENT'S FIRM NAME: _____

INITIALED: _____

DATE: _____

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

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).

Field Form Number	Description of Data to be Entered
[1]	Insert Name of Your Company (All caps)
[2]	Insert Calendar Date
[3]	Insert Month
[4]	Insert Year
[5]	Insert Name of Your Company (All caps)
[6]	Insert Company's full street address (no P.O. boxes) – city, state, and zip code
[7]	Insert Agreement No. or Awarded Contract, Duration of Agreement or Contract, and Official Title of Agreement or Project.
[8a], [8b] & [8c]	Insert Name and address of Port Authority contact
[9]	Print Your Name (Signatory must be a Principal of the Company)
[10]	Print Your Title – (Signatory must be a Principal of the Company)
[11]	Insert Date Signed (Should match date on Page 1)

The NDA signor must also sign an Exhibit A Related Party Individual Acknowledgment. All Prime employees that will come in contact with information must sign an Exhibit A Related Party Individual Acknowledgment.

EXHIBIT A

Port Authority Acknowledgment by Related Party Individual Instructions:

Please fill in the Exhibit A 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.

Field Form Number	Description of Data to be Entered
[1]	Insert Your Name
[2]	Insert Your Working Title (i.e. Project Manager, Field Inspector, Civil Engineer, etc.)
[3]	Insert Name of Your Company
[4]	Insert Name of Your Company OR if employed by for Sub-consultant/Sub-contractor insert the Prime Company's Name . (All caps)
[5a], [5b] & [5c]	Insert Month, Date, and Year of the Prime's Company NDA (page1) ,
[6]	Insert "Port Authority" OR if you are an employee of Sub-Consultant/Sub-Contractor, insert the Prime's Company Name .
[7]	Print Your Name
[8]	Insert Date Signed

EXHIBIT B

Port Authority Acknowledgment by Related Party Entity Instructions
(For use by Sub-Consultants or Sub-Contractors ONLY)

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

Field Form Number	Description of Data to be Entered
[1]	Insert Your Name – (Signatory must be a Principal of the Company)
[2]	Insert Your Title
[3]	Insert Name of Entity (Company Name)
[4]	Insert Type of Entity (Corp., LLC, etc.) and Jurisdiction of Formation (State)
[5]	Insert Full Address of Entity (Company Address)
[6]	Describe Scope of Work of Related Party (Work performing for Prime)
[7]	Describe Project (include Prime's Agreement Number or Awarded Contract Number and Official Title)
[8a], [8b] & [8c]	Enter Month, Date and Year of the <u>Prime's Company NDA</u> (page 1).
[9]	Insert Name of <u>Prime Company</u>
[10]	Print Your Name – (Signatory must be a Principal of the Company)
[11]	Insert Date Signed

Sub-Consultant or Sub-contractor that signs Exhibit B must also sign an Exhibit A Acknowledgment. All Sub-Consultant or Sub-contractor employees must sign Exhibit A Acknowledgment.

**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], [4], 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 [5] having an office and place of business at [6] (“**Recipient**”).

WHEREAS, the Port Authority desires, subject to the terms and conditions set forth below, to disclose to Recipient Protected Information (as defined below) in connection with [7] (collectively, the “**Project(s)**”, or “**Proposed Project(s)**”); and

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

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

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

WHEREAS, Recipient recognizes and acknowledges that providing unauthorized access to, or disclosing such information to third parties in violation of the terms of this Agreement could compromise or undermine the existing or future guidelines, techniques and procedures implemented for the protection against terrorist acts or for law enforcement, investigation and

prosecutorial purposes, and accordingly could result in significant irreparable harm and injury; and

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

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

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

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

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

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

(c) **“Protected Information”** means and includes collectively, Confidential Information, Confidential Privileged Information, Sensitive Security Information (SSI), Critical Infrastructure Information (CII) or Health Insurance Portability and Accountability Act (HIPPA) Information and Information that is labeled, marked or otherwise identified by or on behalf of the Port Authority so as to reasonably connote that such information is confidential, privileged, sensitive or proprietary in nature. The term Protected Information shall also include all work product that contains or is derived from any of the foregoing, whether in whole or in part, regardless of whether prepared by the Recipient, the Port Authority or others, or when the Port Authority receives such information from others and agrees to treat such information as Protected. The following Information shall not constitute Protected Information for the purpose of this Agreement:

- (i) Particular Information, other than Confidential Privileged Information, that is provided to the Recipient by a source other than the Port Authority, provided that such source is not subject to a confidentiality agreement, or similar obligation, or understanding with or for the benefit of the Port Authority, with respect to such Information and that the identity of such source is not itself part of such Protected Information.
- (ii) Information that is or becomes generally available to the public other than as a result of a disclosure by the Recipient or a Related Party in violation of this Agreement.
- (iii) Information that is known to or was in the possession of the Recipient or a Related Party on a non-confidential basis prior to the disclosure of such Information by the Port Authority.

(d) **“Confidential Information”** means and includes collectively, any and all Information, documents and materials entitled to protection as a public interest privilege under New York State law and as may be deemed to be afforded or entitled to the protection of any other privilege recognized under New York and/or New Jersey state laws or Federal laws. It also includes information that contains sensitive financial, commercial or other proprietary business information concerning or relating to the Port Authority, its projects, operations or facilities that would be exempt from release under the Port Authority Freedom of Information Code.

(e) **“Confidential Privileged Information”** means and includes collectively, (i) Information that reveals security risks, threats, vulnerabilities, documentation that identifies specific physical security vulnerabilities or revealing specific security vulnerabilities details related to emergency response protocols, egress plans, flow paths, egress capacities, (diagrams, codes, standards) etc., which is not publicly available.” and any and all Information, documents and materials entitled to protection as a public interest privilege under New York State law and as may be deemed to be afforded or entitled to the protection of any other privilege recognized under New York and/or New Jersey state laws or Federal laws, and (ii) certain Critical Infrastructure Information.

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

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

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

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

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

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

(k) **"Project Purposes"** means the use of Protected Information strictly and only for purposes related to Recipient's and its Related Parties' participation and involvement in the Project, and only for such period of time during which Recipient and its Related Parties are involved in Project related activities.

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

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

(a) All Protected Information shall be held in confidence and shall be processed, treated, disclosed and used by the Recipient and its Related Parties only for Project Purposes and in accordance with the Confidentiality Control Procedures established pursuant to Paragraph 2(c), below, including, without limitation, the Port Authority Handbook, receipt of which is acknowledged by Recipient and shall be acknowledged in writing by each Related Party by signing the Acknowledgment attached hereto as Exhibit A or Exhibit B, as applicable, and

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

(b) Recipient and each Related Party acknowledges and agrees that (i) any violation by the Recipient or any of its Related Parties of the terms, conditions or restrictions of this Agreement relating to Protected Information may result in penalties and other enforcement or corrective action as set forth in such statutes and regulations, including, without limitation, the issuance of orders requiring retrieval of Sensitive Security Information and Critical Infrastructure Information to remedy unauthorized disclosure and to cease future unauthorized disclosure and (ii) pursuant to the aforementioned Federal Regulations, including, without limitation, 49 C.F.R. §§ 15.17 and 1520.17, any such violation thereof or mishandling of information therein defined may constitute grounds for a civil penalty and other enforcement or corrective action by the United States Department of Transportation and the United States Department of Homeland Security, and appropriate personnel actions for Federal employees.

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

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

(e) The Port Authority may request in writing that the Recipient or any Related Parties apply different or more stringent controls on the handling, care, storage and disclosure of particular items of Protected Information as a precondition for its disclosure. The Port Authority may decline any request by the Recipient or any of its Related Parties to provide such item of Protected Information if the Recipient or any of the Related Parties do not agree in writing to apply such controls.

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

(g) The Recipient and each Related Party agrees to be responsible for enforcing the provisions of this Agreement with respect to its Related Parties, in accordance with the Confidentiality Control Procedures. Except as required by law pursuant to written advice of

competent legal counsel, or with the Port Authority's prior written consent, neither the Recipient, nor any of the Related Parties shall disclose to any third party, person or entity: (i) any Protected Information under circumstances where the Recipient is not fully satisfied that the person or entity to whom such disclosure is about to be made shall act in accordance with the Confidentiality Control Procedures whether or not such person or entity has agreed in writing to be bound by the terms of this Agreement or any "Acknowledgement" of its terms or (ii) the fact that Protected Information has been made available to the Recipient or such Related Parties, or the content or import of such Protected Information. The Recipient is responsible for collecting and managing the Acknowledgments signed by Related Parties pursuant to this Agreement. Recipient shall, at the Port Authority's request, provide the Port Authority a list of all Related Parties who have signed an Acknowledgment, and copies of such Acknowledgments.

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

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

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

continues to abide by the requirements of this Agreement with respect to the protection of such Protected Information.

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

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

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

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

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

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

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

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

If to the Recipient: _____

with a copy to: _____

10. **Entire Agreement.** This Agreement contains the complete statement of all the agreements among the parties hereto with respect to the subject matter thereof, and all prior agreements among the parties hereto respecting the subject matter hereof, whether written or oral, are merged herein and shall be of no further force or effect. This Agreement may not be changed, modified, discharged, or terminated, except by an instrument in writing signed by all of the parties hereto.

11. **Counterparts.** This Agreement may be executed in one or more counterparts, each of which shall be deemed to be an original, but all of which shall be one and the same document.

12. **Parties Bound.** This Agreement shall be binding upon the Recipient and its respective successors. The foregoing shall not be affected by the failure of any Related Party to join in this Agreement or to execute and deliver an Acknowledgement hereof.

13. **Authority.** The undersigned individual(s) executing this Agreement on behalf of the Recipient below represent(s) that they are authorized to execute this Agreement on behalf of the Recipient and to legally bind such party.

14. **Disclosure of Ownership Rights or License.** Nothing contained herein shall be construed as the granting or conferring by the Port Authority of any rights by ownership, license or otherwise in any Information.

15. **No Liability.** Neither the Commissioners of the Port Authority, nor any of them, nor any officer, agent or employee thereof, shall be charged personally by the Recipient with any liability, or held liable to the Recipient under any term or provision of this Agreement, or because of its execution or attempted execution or because of any breach, or attempted or alleged breach thereof.

16. **Construction.** This Agreement is the joint product of the parties hereto and each provision of this Agreement has been subject to the mutual consultation, negotiation, and agreement of the parties hereto, and shall not be construed for or against any party hereto. The captions of the various sections in this Agreement are for convenience only and do not, and shall not be deemed to, define, limit or construe the contents of such Sections.

RECIPIENT:

Signature: _____

Print Name: [9]

Title: [10]

Date: [11]

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, protected or confidential information. If it is required for me to review or receive Protected Information, as it is defined in the aforementioned Agreement, I acknowledge that I will be bound by each and every term and provision contained therein, and that failure to do so may include, but is not limited to, the imposition of disciplinary action and sanctions, and/or the institution of legal action seeking injunctive relief, monetary and/or criminal penalties for violation of law and/or Port Authority policies and procedures, as well as for violation of federal and/or state regulations.

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

Signature: _____

Print Name: [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.

Signature: _____

Print Name: [10]

Date: [11]

The Port Authority Information Security Handbook Training

*Security Information Manager Training and
Refresher Course*

Revision 7 – 02/28/2014

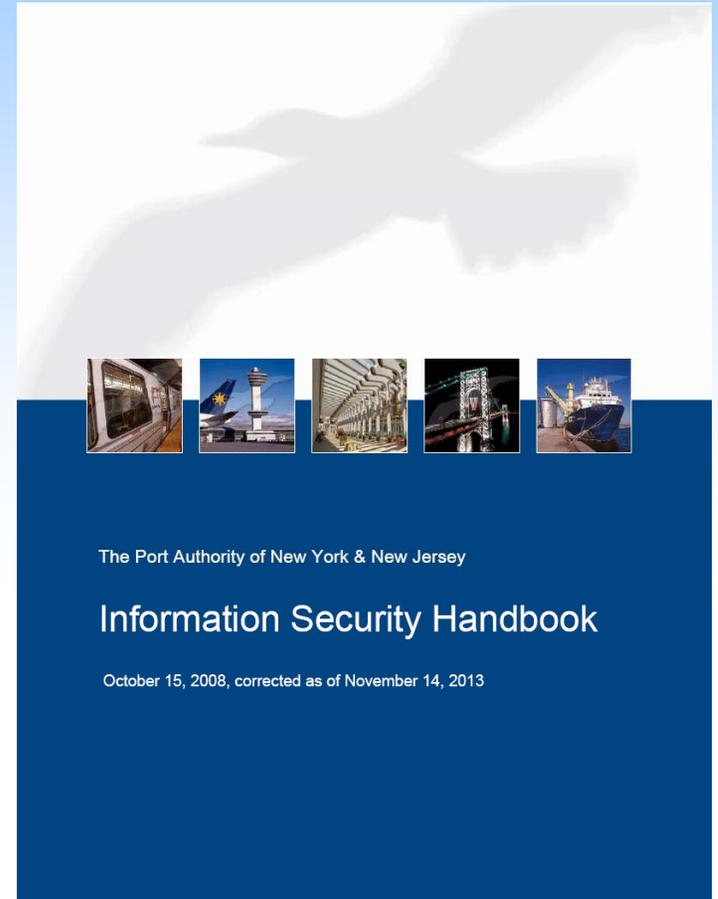


Table of Contents

- **The Information Security Handbook – corrected as of 11/14/2013**
- **Port Authority Information Security Organizational Structure**
- **Categories of Secure Information**
- **The Port Authority Freedom of Information Policy**
- **Training and Information Review**
- **Access to Confidential & Privileged Information**
- **Labeling Secure Documents**
- **Handling Secure Documents**
- **Transmitting Secure Documents**
- **Storage of Secure Documents**
- **Receiving of Secure Documents**
- **Reproduction of Secure Documents**
- **Disposal of Confidential & Privileged Information**
- **Audits / Violations**

Information Security Handbook

- “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.”
- Use the Handbook as a guide to answer most of your questions regarding handling C&P information.
- If there is additional clarification needed, contact a SIM.
- The Information Security Handbook can be downloaded from Livelink from the following location for those with access:
 - ◆ Livelink/DRP (online)/Enterprise Workspace/SECURITY HANDBOOK



Port Authority Information Security Organizational Structure

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

- **Corporate Security Officer (CSO)**
- **Corporate Information Security Officer (CISO)**
- **Departmental Information Security Officer (DISO)**
- **Security Information Manager (SIM)/Deputy 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)**
- **Chief Technology Officer (CTO)**
- **Office of Inspector General (OIG)**
- **Information Security Subcommittee (ISSC)**
- **Non-Port Authority entities should have a SIM and Deputy SIM, at a minimum.**

Categorization of Information

- **Confidential Information**
- **Confidential and Privileged Information (C&P)**
- **Confidential Proprietary Information**
- **Critical Infrastructure Information**
- **Information (Unrestricted Information)**
- **Limited Access Safety and Security Information**
- **Sensitive Information**
- **Non-Disclosure and Confidentiality Agreement**
- **Non-Disclosure Instructions**

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 PA-DISO concurrence and approval.
3. Obtain PA-CISO final approval.
4. If approved, mark and label the information, and, if appropriate, apply a cover sheet.
5. If a document is produced, and is derived from a C&P document, the new document will also be C&P if the content dictates such classification.

Categories of C&P Information

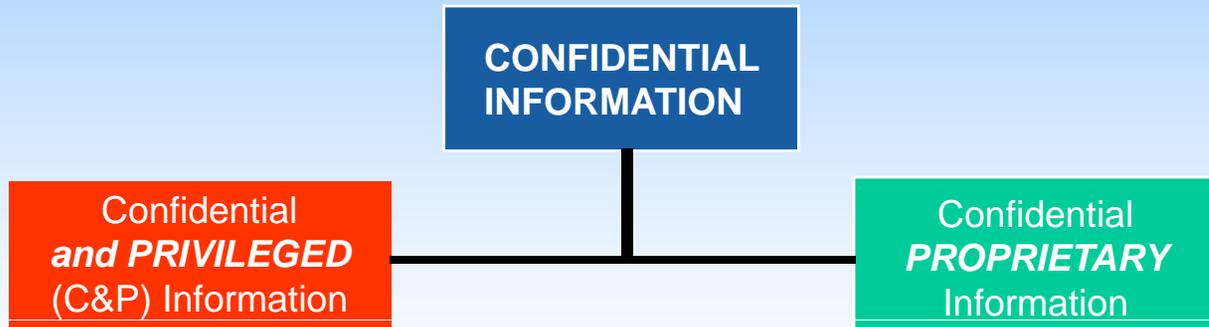
- ◆ Vulnerability Studies
- ◆ Risk Assessments
- ◆ Countermeasures
- ◆ Existing Engineering & Facility Data
- ◆ Emergency Response Protocols
- ◆ Security Design Criteria
- ◆ Cumulative Information



- ***Any information that if discovered and used by terrorist could render a security system inoperable?***

Categories of Secure Information

Secure information shall be classified as information falling in any of the below mentioned categories:



- **CONFIDENTIAL** *Highly sensitive information, if lost or made public, could seriously damage or compromise the Port Authority and/or public safety and security. Information includes, but is not limited to, methods utilized to mitigate vulnerabilities and threats, such as identity, location, design, construction and fabrication of security systems.*
- **CONFIDENTIAL and PRIVILEGED (C&P)** *Extremely sensitive security or public safety information, if lost or made public, could gravely damage or compromise the Port Authority and/or public safety and security. Information includes, but is not limited to Security Risk and Threat Assessments, Design Basis Threats and Concept of Operations documents. Any information identifying vulnerabilities, capabilities, threats, operational methodologies, and/or security related design criteria.*
- **CONFIDENTIAL PROPRIETARY** *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. Information includes sensitive financial, commercial and other business information received from third parties under Non-Disclosure and Confidentiality Agreements.*

Reasons For Keeping Documents Secure

- Britain's most senior counter terrorism officer, Assistant Commissioner Bob Quick, was photographed carrying sensitive documents as he arrived at Downing St to meet with Prime Minister Gordon Brown and Home Secretary Jacqui Smith.

Among the bundle of papers under his arm was a document marked "secret" that outlined an ongoing counter-terrorism operation.

The names of several senior officers, locations and details about the nature of the overseas threat were included on the briefing paper. The operation was forced to be shut down and Quick was forced to resign.

- **THIS IS AN EXAMPLE OF WHAT WE ARE TRYING TO AVOID!!!**
- **Use better judgment as we are all the first line of defense in keeping documents secure.**
- **There are cameras everywhere we go and pictures being take with and without our knowledge.**



Invoking FOI Exemptions Requires

- Evaluation and identification of information assets
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.
- Restricting access to this information
Another important principle of the Handbook is that access to properly designated sensitive information is premised on a strict "need to know" basis.
- Safeguarding
Marking, handling, storage, transmittal and destruction



Port Authority Freedom of Information Code

RESOLVED, that any paper, written or printed book, document, drawing, map, plan, photograph, microfilm, data processed or imaged processed document, information stored or maintained electronically or by sound-recording or in a similar device, or any copy thereof, that has been made, generated, maintained, received in the course of transacting official business and kept on file (collectively, "Records") of the Port Authority shall be made available for public inspection and/or copying, except that such access or copying may be denied as to Records or portions of Records which:

1. federal or state law or regulations or rules or decisions of court render confidential or privileged or exempt from disclosure, including any Record within the attorney-client privilege, or Records which, if disclosed, would constitute an unwarranted invasion of personal privacy of an individual or individuals, including lists of names and addresses to be used for profit or financial gain, sexual harassment complaints, grievances involving individual employees (filed by or against an employee), personnel, medical or disciplinary records (with Records or portions of Records indicating a Port Authority employee's compensation, pension, employment and salary history and qualifications as shown on résumés, for example, not exempted), and financial account numbers, including, in addition to Social Security Numbers, bank account, credit card, personal or cell telephone, or driver's license numbers, and electronic mail addresses; or
2. a. if disclosed, would impair, or give a competitive advantage in connection with, present or imminent awards or negotiation of collective bargaining agreements, leases, permits, contracts or other agreements, open procurement matters, contracts not yet awarded, unexecuted leases or permits, and portions of scoring or evaluation documents not constituting a part of a final agency action document; or
b. are trade secrets, or are submitted by or derived from information obtained from a commercial enterprise and which, if disclosed, would cause injury to the competitive position of the subject enterprise, including résumés of individuals submitted by unsuccessful bidders, internal business protocols, systems or strategies specific to the commercial enterprise or to the project, as well as technology or equipment that the unsuccessful bidder has developed;

Port Authority Freedom of Information Code

3. are compiled for public safety, law enforcement or official investigatory (internal or external) purposes, when their disclosure may affect public safety, interfere with investigations, audits, law enforcement investigations, or judicial or disciplinary proceedings, or deny or prejudice a right to a fair trial or impartial adjudication, or identify a confidential source or disclose confidential information relating to an audit or an ongoing civil, criminal, or internal or external disciplinary investigation, including any reports, statements, transcripts or recordings related to an ongoing investigation, audit or proceeding; or
4. **if disclosed, could endanger the life or safety of any person or jeopardize the safety and/or security of any facility or information technology system, including drawings, maps, or sketches of non-public areas, administrative or technical information regarding computer networks, hardware or software related to security systems, emergency or security plans or procedures for any building or facility, or security or safety procedures or surveillance techniques or details; or**
5. are inter-agency or intra-agency advisory, consultative or deliberative Records, such as recommendations and communications to or from, and discussions among the members of the Board of Commissioners, the Governors of the States of New York and New Jersey and the Port Authority (or the staffs of the foregoing); and inter-agency or intra-agency memoranda, draft reports and presentations, or e-mail messages, which are not statistical or factual tabulations of data, with instructions to staff that affect the public or final agency policy or determinations not exempted; or
6. are examination questions or answers which are requested prior to final administration of such questions;

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.

Access to Secure Information

- Access to Confidential Information shall be on a **need to know basis** only.
- In certain instances access privileges may be conditioned on the satisfactory completion of a background investigation
- Non-Disclosure Agreements must be executed by:
 - ◇ Firms – General Company NDA (completed by an Executive)
 - ◇ All Non-PA Individuals - (“Exhibit A” acknowledgement form only)
 - ◇ PA Employees – PA NDA form only

***All NDA forms should be accompanied by instructions on how to complete.
- US Citizenship or Permanent Residency is required
- Each internal and external organization is to have a dedicated SIM & Deputy SIM
- **Only SIM transmits NDA package to requestor**

Access to Secure Information

- In certain instances access privileges may be conditioned on the satisfactory completion of a background investigation
- ♦ For all organizations & non Port Authority employees requiring access to secure information the following are required:
 - ◇ **Secure Worker Access Consortium (S.W.A.C.) Clearance**
visit <http://www.secureworker.com/> and enroll. Complete all online requirements and contact S.W.A.C. customer service at **877-522-7922** for next steps.
*The closest S.W.A.C. office to the WTC site is located at 116 Nassau Street.
 - ◇ **Upon receipt of you S.W.A.C. card, please provide a color photo copy to the CM SIM who will in turn submit to the WTCC SIM to be filed with you NDA form.**
 - ◇ **If clearance is not obtained, access to all secure documents will be denied.**

Access to Secure Information

- Each Firm that is provided access to Secure Information shall prepare an Authorized Personnel Project List to their CM for submission to the Port Authority.

The list will include:

- ◇ *Firm's name and address*
 - ◇ *Name and contact information for the firm's Security Information Manager*
 - ◇ *A list of employees authorized to access Confidential Information; and their most recent SIM training date*
- A copy of this list should be provided to the PANYNJ or CM semi-annually (**every six months**). This list will be used as a method for authenticating that individuals are authorized access to Confidential Information.
 - Security Information Managers are responsible for the accuracy of this list.

Labeling Confidential & Privileged Documents

- Confidential & Privileged Information needs to be marked as such in a particular way:
 - ◇ Appropriate protective marking: **CONFIDENTIAL & PRIVILEGED**
 - ◇ The markings must be conspicuous and in bolded Arial type and in red.
 - ◇ The front page (or front and back cover, if appropriate) shall be marked at the top and bottom of the page.
 - ◇ *All interior pages within the document must also be marked at the top and the bottom of the page.*
 - ◇ Certain documents will be given a control number, which shall consist of the category of information followed by an acronym for the transmitting department or company, followed by the last 2 digits of the year followed by a number that is sequential and finally, followed by, the copy number. CP-XXX-14-0001-X
 - Insert company initials for the transmitting department for a number unique to your company for easy recognition of documents issued.
 - ◇ 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.
 - ◇ For compact discs, DVDs or other smaller materials, the warning statement may be printed on an adhesive label and affixed to the material. It should be in 8-point font size.

CONFIDENTIAL & PRIVILEGED

CONFIDENTIAL & PRIVILEGED

Confidential and Privileged	
Document Control #	CP-PCP-06-
Identifier:	
Agency:	
Recipient:	
Transmittal Approved by:	
Date:	
 THE PORT AUTHORITY OF NY & NJ	



Labeling Confidential & Privileged Documents

- Confidential Information Warning Statement

"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.

Labeling Confidential & Privileged Documents

- Ensure that the C&P Documents are labeled correctly, however, do not use the C&P labels on every document as a default. Not every document generated is C&P.
- Ensure that if information is removed from a document/drawing, the documents is reviewed by the SIM for proper re-classification if necessary.

Handling of Confidential & Privileged Information

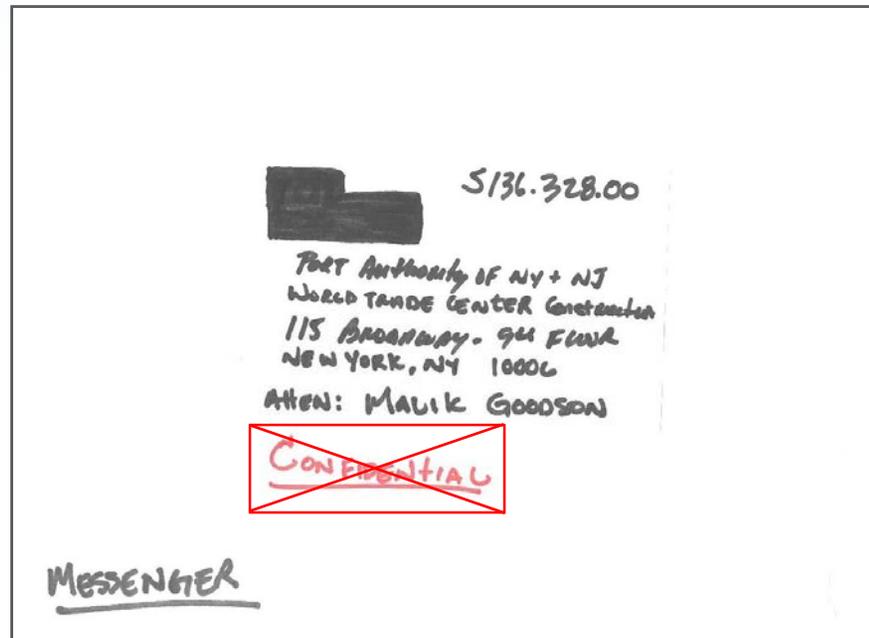
Handling refers to the physical possession of, and includes working on or with, Confidential Information to perform job duties or complete tasks or projects. This includes, but is not limited to, reading, copying, editing, creating, or correcting the material. Confidential Information in any form, including 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

Transmitting Confidential & Privileged Documents

- **EMAIL NOT AUTHORIZED TO DISTRIBUTE INFORMATION**
- **Approved Commercial Delivery Service:** FedEx, UPS, DHL
- **US Postal Service:** Certified Mail only
 - (a) request return receipt
 - (b) verify recipient name and mailing address
 - (c) place in a sealed envelope, and
 - (d) the exterior of a mailing document shall **not** indicate the security category of the material contained therein



Transmitting Confidential & Privileged Documents

- **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
 - (e) Be sure to gather the original fax and all transmittal sheets made by the fax machine.

TRY TO AVOID USING THE FAX MACHINE TO TRANSMIT INFORMATION

Transmitting Confidential & Privileged Documents

- 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.

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

Transmitting Confidential & Privileged Documents

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 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)

Storage of Confidential & Privileged Information

- Confidential & Privileged information MUST be kept securely stored in a locked location when not in use.
- Confidential & Privileged information should be kept/stored separate from Unrestricted information. Do not mix drawings together that are of different security classifications.
- Confidential Information should be gathered and stored in a *minimum number* of office locations.
- A storage space or security container/receptacle *may not be left open and unattended at any time.*
- 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 the Handbook.
- Any steel file cabinet that has four sides and a top and bottom (all permanently attached by welding, rivets or pined bolts so the contents cannot be removed without leaving visible evidence of entry) and is secured by a rigid metal lock bar and an approved key operated or combination padlock.

Storage of Confidential & Privileged Information

- If you have an office, lock your office at the end of the day.
- Do not leave C&P information unattended at any time.
- If you do not have sufficient storage space, please let your SIM or Document Control know.
- Do not store C&P information on an unrestricted server.
- If you have C&P information stored electronically on your computer, it should be on a secure server only accessible to staff who have signed the proper NDA form and have received clearance to access the information.
- Do not loan your C&P information to anyone for their use, have a copy of the document requested for them instead.
- Do not store/accept information that is not assigned to you.
- You should not have C&P material in your possession unless it is assigned to you. No exceptions!!!

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)

A simple Word or Excel document should suffice.

INVENTORY OF CONFIDENTIAL PRIVILEGED DOCUMENTS WORKSHEET

Date received or created	Sender or creator	Title and brief description	Control Number	Number of copies	Transmission history (sent to whom, when)	Date destroyed (when, by whom and the method) or date returned to the Port Authority



Reproduction / Printing of C&P Documents

- 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.
- Staff should not print or make copies of any document or parts of any document containing C&P information.
- Do not request extra/additional copies of C&P documents be made if there are no intended recipients.

Disposal of Secure Documents

- When do you need to dispose of secure documents?

- ♦ Drawings in your possession are no longer valid.
- ♦ You have completed the task for which the documents were needed.
- ♦ You are no longer a member of the project or department:

When any employee, consultant, third-party contractor or other agency personnel either leave the project or the Agency, they must destroy all Secure Information that has been issued to them during their tenure or return these documents to the Security Information Manager or Document Control for destruction. Until either of the above has been completed, the individual remains accountable for the Confidential Information they have been issued and may be subject to Audit and subsequent penalties pursuant to Chapters 5 and 6 of the Handbook.

- ♦ Do not pass along your material to someone taking over for you. Documents should be returned and closed out and can be reissued to a new recipient if needed.
- ♦ Close out your book on all C&P material if you are leaving the project.

Disposal of Secure Documents

Individuals granted access to Confidential Information must perform the actual destruction.

Paper products must be destroyed using a cross cut shredder located in the office.

Authorized service providers may be used for this task provided that the information remains safeguarded until the destruction is completed.

If documents are destroyed, a letter certifying this destruction is to be provided to the Port Authority including the document control number.

Oversize material shall not be placed or accumulate adjacent to secure receptacles while awaiting destruction.

Oversize materials awaiting destruction must be stored in a protected manner.

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).

CyberScrub or a similar software shall be used to prevent discovery by a computer technician or other unauthorized person.



Compliance Audits

- The Information Security Subcommittee and the Office of Inspector General may conduct random or scheduled inspections of business practices in order to assess compliance.

- These audits will include



- Interviews with staff



- Hands-on review of security practices

- Suggested corrective action if deficiencies are identified

Suggested Questions When Interviewing Employees Authorized Access to Confidential Information:

What is your job title/responsibility?

Which contract or program requires you to access this information?

How do you access the information?

How long have you been authorized access?

When was your last access to Confidential Information?

Have you ever had access to Confidential Information outside of PATC?

Did anyone else from the office accompany you?

Did you take any Confidential notes or Confidential Information back with you?

What procedures were followed to protect this information?

Where is this information now?

Have you ever provided access to Confidential Information to visitors?

How did you determine their need-to-know?

When was the last time that you had a security briefing?

Have you ever been cited for a security violation?

What would YOU do if YOU committed a security violation or discovered one?

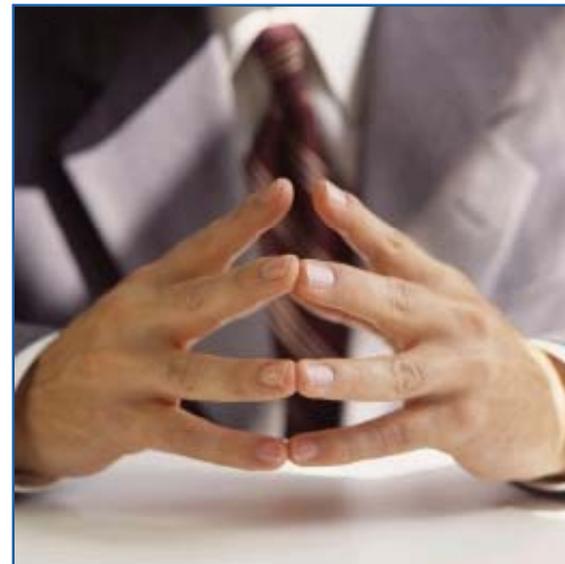
Do you have the combination to any storage containers?

Who other than yourself has access to these containers?

Is a record maintained of the safe combination? If so, where?

Violations

- 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.
- Reporting and Investigation
 - ◆ *Individuals must report alleged or suspected violations, infractions or breaches of the Policy to the Office of Inspector General and to their supervisor or manager.*
- Disciplinary Actions
 - ◆ Carelessness **vs.** Deliberate
 - ◇ *Verbal or Written Reprimand*
 - ◇ *Re-training*
 - ◇ *Suspension*
 - ◇ *Termination*
 - ◇ *Legal or Civil Action*



Violations

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.

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.

Violations

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).

Training Program Elements

- **The Training Program consists of three interconnected elements: (a) indoctrination training, (b) orientation training, and (c) 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.**
 - ◆ **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.
 - ◆ **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.
 - ◆ **Required Refresher Training**
 - ◇ Once every three (3) years, 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.
 - ◆ **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.

Questions

Should you have any questions that arise after completion of this training/refresher course, please contact your SIM:

WTCCSIM Name: **Malik Goodson**

SIM E-mail: **mgoodson@panynj.gov**

SIM Phone: **(212) 435-5185**

WTCC Handling of Secure Documents Issues For Information Handling Specific to the Workplace

*Staff Level Training
WTCC-TRAIN-006
Revision #6*

Confidential & Privileged Issues Specific to the Workplace

- **Reasons for Keeping C&P Documents Secure**
- **Identification of Security Information Managers (SIM)**
- **The Non-Disclosure Agreement Form (NDA)**
- **The Information Security Handbook**
- **Document Security Review Process – Handling Procedure**
- **Requesting Confidential & Privileged Information**
- **Transmitting Confidential & Privileged Information**
- **Reproduction / Printing Confidential & Privileged Information**
- **Receiving Confidential & Privileged Information**
- **Storage of Confidential & Privileged Information**
- **Handling of Confidential & Privileged Information**
- **Disposal of Confidential & Privileged Information**
- **What ifs**
- **Questions**

Reasons For Keeping Documents Secure

- To Protect OUR Security and OUR Families
 - ◆ Our families will be coming to visit the WTC site and you want to ensure their safety from any threats, as best as possible. We are building the future that other want to destroy.
- To Prevent Unauthorized Access to Secure Information
 - ◆ All parties working on WTC projects are not authorized to view secure information.
 - ◆ Our office have visitors and staff from outside of our organization coming to our floors who do not need to be aware of the content of confidential & privileged information.
- To Prevent the Misuse of Sensitive & Secure Information
 - ◆ Unauthorized copying.
 - ◆ Borrowing of information.
 - ◆ Information getting into the news.

Reasons For Keeping Documents Secure



Secure documents should be treated in the same fashion that you would treat your social security card or bank card.

WTCC Information Security Officers

The WTCC Department has four Information Security Officers:

- ◆ **Carla Bonacci, DISO**
 - ◇ Department Information Security Manager (DISO)
 - ◇ External SIM – Outside agencies: LMDC, SPI, SAIC, Etc.
- ◆ **Malik Goodson, SIM**
 - ◇ Internal SIM - PA including Law, DDP, CM, CM/GC
 - ◇ WTC Hub Projects & Non-Hub Projects
- ◆ **Tom Grassi, SIM**
 - ◇ Internal SIM - PA including Law, DDP, CM, CM/GC
 - ◇ WTC Hub Projects
- ◆ **Doug Blais, SPM**
 - ◇ Security Project Manager
 - ◇ Non-WTC Hub Projects

Include your company SIM and Deputy SIM here

Non-Disclosure Agreement Form

- NDA forms can be accessed from any SIM.
- Must be signed and returned prior to gaining access to ANY & ALL secure documents.
- There are three (3) different NDA forms:
 - ◊ **PA Employee NDA (includes interns)**
 - ◊ **Non-PA company/organization General NDA - To be completed by organization executive**
 - ◊ **Exhibit A Related Party Individual NDA –
To be completed by all employees of non-PA organization (Exhibit A)**
- **Original signed & completed NDA forms should be returned to Malik Goodson at**
The Port Authority of NY & NJ
115 Broadway, 7th floor
New York, NY 10006
- Keep a copy of your NDA form on file for future verification if needed.
- NDA forms need to be completed once, and are valid for work on all PA projects.



Non-Disclosure Agreement Form

- General NDA form to be completed by a company or organization executive. (9 pages)
- Note: Executive must also complete Exhibit A NDA form

NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT
BETWEEN

AND

THE PORT AUTHORITY OF NEW YORK AND NEW JERSEY

THIS NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT (this "Agreement") is made as of this _____ day of _____, _____, by and between THE PORT AUTHORITY OF NEW YORK AND NEW JERSEY (the "Port Authority") a body corporate and politic created by Compact between the States of New York and New Jersey, with the consent of the Congress of the United States, and having an office and place of business at 225 Park Avenue South, New York, New York, 10003, and _____ having an office and place of business at _____ ("Recipient").

WHEREAS, the Port Authority desires, subject to the terms and conditions set forth below, to disclose to Recipient Confidential Information (as defined below) in connection with _____ (collectively, the "Project(s)", or "Proposed Project(s)"); and

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

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

WHEREAS, the Port Authority and Recipient (collectively, the "Parties") acknowledge that in order for Recipient to undertake its duties and/or obligations with regard to its involvement in the Project, the Port Authority may provide Recipient or certain of its Related Parties (as defined below) certain information in the possession of the Port Authority, which may contain or include 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

Port Authority Handbook NDA 062711



Non-Disclosure Agreement Form

- Exhibit A NDA form to be completed by all non-PA employees
- Note: The date referenced in the body of the Exhibit A NDA refers to the date which the General/Company NDA was completed by the executive.

EXHIBIT A

ACKNOWLEDGMENT BY RELATED PARTY INDIVIDUAL

I, _____ ("Related Party"), am employed as a(n) _____ by _____. I have been provided with and have read the Non Disclosure and Confidentiality Agreement between _____ (the "Recipient") and The Port Authority of New York and New Jersey (the "Port Authority") dated _____, _____ (hereinafter the "Agreement"), and the Port Authority Handbook attached to the Agreement. I understand that because of my employer's relationship with _____, both my employer and I may be provided with access to, and/or copies of, sensitive security materials 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: _____

Date: _____

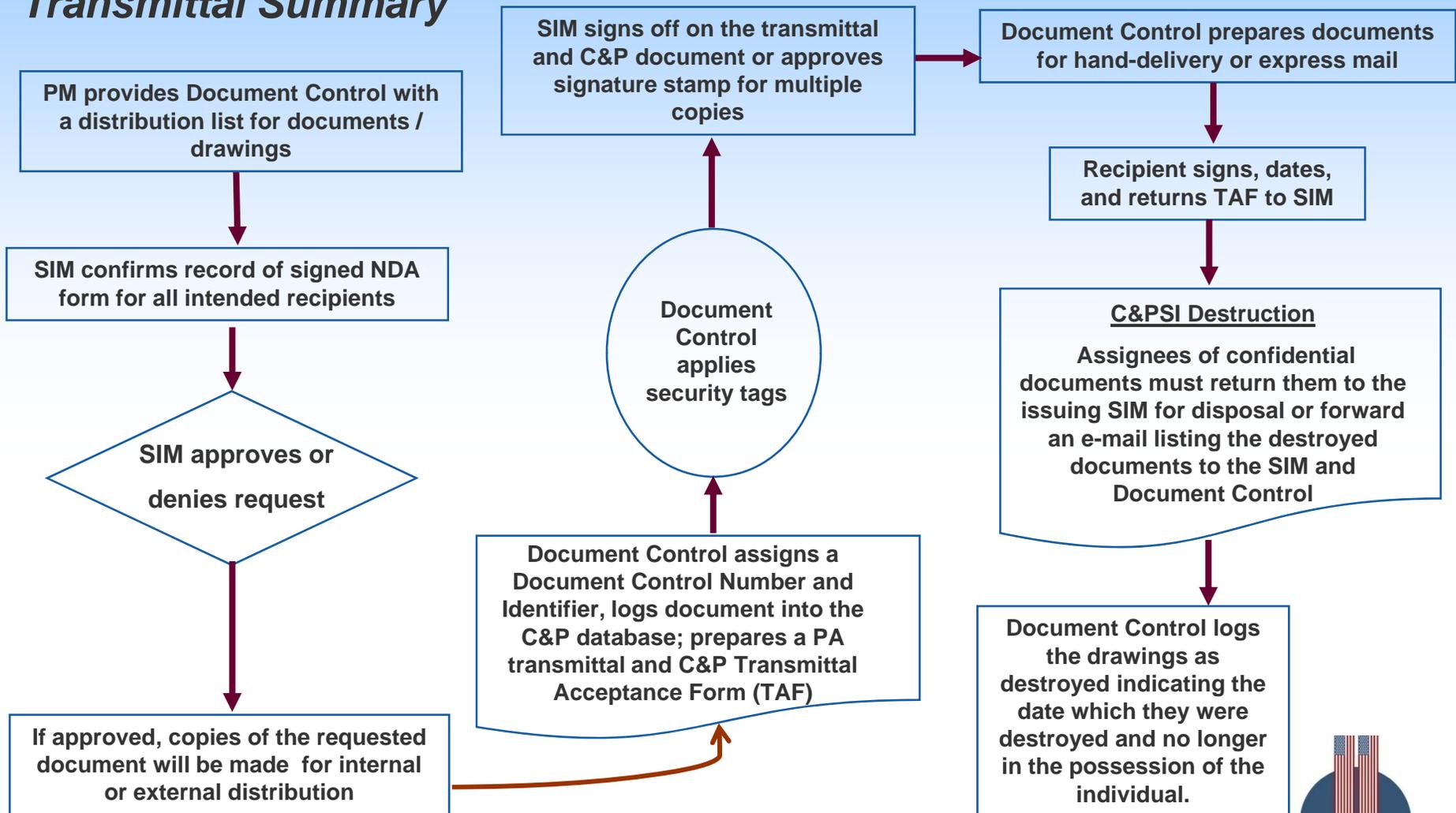
Port Authority Handbook NDA 062711

10



Document Security Review Process Handling Procedure for WTC Construction

Transmittal Summary



Requesting Confidential & Privileged Documents

- Do not request a document for an individual who has not signed the NDA form. Only share with other authorized individuals.
- Do not request additional copies to be made without intended recipients. There is no storage space for extra sets to be stored. Provide a name per copy request.
- **Request should be made electronically on the Downtown Restoration Program Intranet by Document Control ONLY.**
- Prior to requesting a document as a "New" document, be sure that it has not been previously requested with an existing document control number. Use the search function.
- For documents being issued, they should be requested in the name of the SIM of the department or organization where the documents are being sent.
- One copy per person. Individuals may not receive more than ONE copy of a secure document.
- Multiple request should not be made for any individual, but may be made for a department/organization if the listed recipient is the SIM. (The SIM may then distribute copies to the intended recipients of department or organization)
- Keep a copy of what you have requested to be distributed, and the document control numbers.

Requesting Confidential & Privileged Documents

Transmittal: **Keep for Your Records**

Transmittal Acceptance Form: **Complete & Return**

 **THE PORT AUTHORITY OF NY & NJ**

Date: Monday, February 09, 2009
 Contract:
 Reference: From

To: /
 ()

Copy: T. Grassi, File,

We are sending you the following items: Attached Under Separate
 Specifications Copy of Letter
 Drawings

Via: Hand Delivered DHL
 UPS Courier Service

No	Document Tracking #	Dated	WTC Downtown Restoration Program
1	----		

For your use As requested Copies for Distribution
 For review & comment Approved as submitted Copies for Approval

Remarks:
 Please be reminded that, as this set of drawings is being provided to you, and it has been marked "Confidential and Privileged", you are responsible for its safeguarding. Please ensure that it is protected at all times by either appropriate storage or having it under your personal observation and control. All persons working with Confidential and Privileged information are personally responsible for taking the proper procedures to ensure that unauthorized persons do not gain access to it. Further reproduction and/or distribution outside the contract team is prohibited without the express written approval of: The Port Authority of NY & NJ.

Malik G. Goodson
 Project Manager
 WTC Construction
 115 Broadway, 7th Floor
 New York, NY 10006
 mgoodson@panynj.gov
 (212) 435-5185

Confidential and Privileged

Document Control #: ----
 Identifier: _____
 Agency: _____
 Recipient: _____
 Transmittal Approved by: _____
 Date: 09/20/09

 **THE PORT AUTHORITY OF NY & NJ**

 **THE PORT AUTHORITY OF NEW YORK AND NEW JERSEY**
CONFIDENTIAL AND PRIVILEGED TRANSMITTAL ACCEPTANCE FORM
 SECURITY WARNING:

THE MATERIAL CONTAINED HEREIN IS CONFIDENTIAL AND PRIVILEGED AND MAY INCLUDE SENSITIVE SECURITY, CRITICAL INFRASTRUCTURE AND/OR PROPRIETARY INFORMATION PROTECTED AS A PUBLIC INTEREST PRIVILEGE, UNDER STATE AND/OR FEDERAL RULES AND REGULATIONS. UNAUTHORIZED TRANSMISSION, REPRODUCTION OR DISSEMINATION IS STRICTLY PROHIBITED.

By signing below I acknowledge that I have signed a Port Authority Confidentiality and Non-Disclosure Agreement and/or the corresponding Acknowledgment thereof. I recognize that I am a person with the requisite "need to know" and that I will conform my handling, distribution, reproduction and safeguarding of the attached Confidential and Privileged, Sensitive Security, Critical Infrastructure and/or Proprietary Information in accordance with the Confidentiality and Non-Disclosure Agreement signed between the parties.

Document Name/Title: _____ PCP Document Control #: _____
 /
 /
 Printed Name: _____ SIM/Recipient/Company: _____
 Signature: _____ Date: _____

WTC Construction

Sign & Return to: Malik Goodson (PANYNJ)
 115 Broadway - 7th Floor
 New York, NY 10006
 Last Revised Date: 03/18/2005

You may want to replace the images of the PA transmittal and TAF with your transmittal and TAF when your SIM conducts additional training of subcontractors.



Reproduction / Printing of C&P Documents

- All reproduction should be done by Document Control with the permission of the SIM.
- Staff should not print or make copies of any document or parts of any document containing C&P information.
- Do not request extra/additional copies of C&P documents be made as there is no space for storage. (Document Control is consistently overflowing with unnecessary additional copies of C&P documents)

Receiving Confidential & Privileged Documents

- When you receive a secure document or drawing:
 - ♦ Make sure you receive a Transmittal and a Transmittal Acceptance Form (TAF).
 - ♦ Sign, print and date the TAF and return to Document Control immediately.
 - ♦ Add the document control number to your person accountability log.
 - ♦ Ensure that the document control number on the Transmittal, TAF and documents all match.
 - ♦ Ensure that you are receiving and signing for documents that are relevant to your work.
 - ♦ Do not accept documents that you do not need or did not request.

Receiving Confidential & Privileged Documents

- Confidential & Privileged Information needs to be marked as such in a particular way:
 - Appropriate protective marking:

Confidential and Privileged	
Document Control #	CP-ENG-10-XXXX
Identifier:	1
Agency:	Bidder Organization
Recipient:	Bidder SIM
Transmittal Approved by:	PA SIM
Date:	01/04/2010
 THE PORT AUTHORITY OF NY & NJ	
BID DOCUMENT	
NOT FOR CONSTRUCTION	

For pre-award C&P drawings and specifications issued to bidders.

Confidential and Privileged	
Document Control #	CP-ENG-09-XXXX
Identifier:	X
Agency:	Bidding Company
Recipient:	SIM
Transmittal Approved by:	Malik Goodson
Date:	11/20/2009
 THE PORT AUTHORITY OF NY & NJ	
FOR REVIEW & COMMENT ONLY	
NOT FOR CONSTRUCTION	

For pre-award C&P drawings and specifications issued to non-bidders.

Confidential and Privileged	
Document Control #	CP-ENG-10-XXXX
Identifier:	1
Agency:	Agency Name Here
Recipient:	SIM/Recipient
Transmittal Approved by:	PA SIM
Date:	01/04/2010
 THE PORT AUTHORITY OF NY & NJ	

For post-award C&P drawings and specifications issued to set distribution list.

Note: Unrestricted drawings issued post award will not receive any classification label.

BID DOCUMENT
NOT FOR CONSTRUCTION

For pre-award unrestricted drawings and specifications issued to bidders.

FOR REVIEW & COMMENT ONLY
NOT FOR CONSTRUCTION

For pre-award unrestricted drawings and specifications issued to set distribution list.



Receiving Confidential & Privileged Documents

- Electronic distribution of C&P information should be via Livelink.
- In a case where C&P information may need to be distributed via CD/DVD, the following should occur:
 - ♦ Approval from the appropriate SIM prior to producing the CD/DVD.
 - ♦ The information on the CD/DVD MUST be password protected.
 - ♦ The CD/DVD must be labeled properly:

CD/DVD Case Cover

CONFIDENTIAL & PRIVILEGED

WORLD TRADE CENTER CONSTRUCTION
WORLD TRADE CENTER TRANSPORTATION HUB
PATH Hall & Transit Hall Construction
CONTRACT No. WTC-214.582
SPECIFICATIONS

CONFIDENTIAL & PRIVILEGED

CD/DVD Case Interior

“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.

CD Label

WTC TRANSPORTATION HUB

PHTHC
Contract No. WTC-214.582
Revision 0
Dated 2009-07-20

Confidential & Privileged

Confidential and Privileged	
Document #	CP-PJP-06
Issued	
Agency	
Recipient	
Transmitted	
Approved by	
Date	

THE PORT AUTHORITY OF NY & NJ

- ♦ **C&P information MUST be placed on a separate CD/DVD from any Unrestricted information. C&P information only on C&P CDs/DVDs.**

Storage of Confidential & Privileged Information

Avoid storing secure documents/information on the following media or accessing secure documents in the following fashions:



Secure documents should be transmitted electronically via the Livelink secure serve which the Port Authority has established, or an approved FTP site. For information on getting an FTP site approved, contact the PA-WTCC SIM.

Disposal of Confidential & Privileged Documents

- How Do You Dispose of Secure Documents?
 1. Identify the individual document control number (each document has a specific number).
 2. Place document(s) into secure shredding bin.



3. Notify the SIM who approved the distribution and issued the document via e-mail.
 - A. Include the complete document control number (CP-XXX-XX-XXXX-~~X~~).
 - B. Indicate where & how you have disposed of the document(s).
 - C. For documents issued by WTC Construction, notify Document Control at dcandpdocs@panynj.gov or Destroyed_C_and_P_Documents@panynj.gov

What ifs?

- **What if I Lose a Confidential & Privileged document?**
 - ◆ Notify your SIM immediately!!!
 - ◆ Identify the document control number of the document.
 - ◆ Indicate the last time you were familiar with the documents' location.
 - ◆ Check your storage locations to ensure that it is not in your possession.
 - ◆ A replacement document will not be issued unless approved by the SIM.
- **What if I request a document for someone and the document is not distributed?**
 - ◆ Notify document control and/or your project SIM.
 - ◆ The document may not have been approved for distribution.
- **What if I only need part of a C&P document?**
 - ◆ Inform document control which sections of the document you need to have reproduced. If it ends up being most of the document, the entire document may be reproduced depending on the difficulty of separation.



What ifs?

- **What if I need another copy of a document that I have already destroyed?**
 - ◆ Provide proof or destruction notification e-mail.
 - ◆ Depending on the document, an additional copy may be provided with the permission of the SIM.
- **What if I forget to inform the SIM and document control that I have destroyed a document?**
 - ◆ You are still held accountable for those documents until you are able to identify the document control number and inform document control and the SIM of the destruction.

Questions

Should you have any questions that arise after completion of this training/refresher course, please contact your SIM:

WTCCSIM Name: **Malik Goodson**

SIM E-mail: **mgoodson@panynj.gov**

SIM Phone: **(212) 435-5185**

