STANDARD PROCEDURES
OF THE
WASHINGTON SUBURBAN SANITARY COMMISSION

ORIGINATOR & POSITION	SP NUMBER	APPROVE BY/DATE	EFFECTIVE DATE	PAGE 1
Roscoe Wade, Logistics Director 6/22/12 Christopher Brous, Group Leader 6/22/12	SEC-12-01 SUPERSEDES N/A	General Manager/CEO	6/25/12	OF 7

SUBJECT

ACCESS TO SENSITIVE ENGINEERING RECORDS

1.0 PURPOSE

1.1 This procedure describes the Washington Suburban Sanitary Commission's (WSSC) procedure for responding to requests for access to Sensitive Engineering Records. Access to these records must be controlled as necessitated for protection of critical infrastructure in a post 9/11 environment.

WSSC finds that the disclosure or inspection of Sensitive Engineering Records, as defined herein, without appropriate controls, could:

- Jeopardize the security of structures owned or operated by the WSSC;
- Facilitate the planning of a terrorist attack; or
- Endanger the life or physical safety of WSSC employees, customers and the public at large.

WSSC further finds that unrestricted disclosure or inspection of these records would be contrary to the public interest, and thus hereby determines that such disclosure or inspection shall be denied, except as otherwise specified herein. These restrictions are permitted under Md. State Government Code Ann., §10-618 (j)(2), which allows denial of access to records of water or wastewater systems should such access be contrary to the public interest. Note also this Procedure is an exception to WSSC Standard Procedure L-07-01- REQUESTS FOR WSSC RECORDS UNDER THE MARYLAND PUBLIC INFORMATION ACT.

2.0 AUTHORITY

The General Counsel's Office certifies that the statutory authority for the adoption of this regulation is Md. Public Utilities Code Ann., §17-403 and Md. State Government Code Ann., §10-618 (j)(2), which permits the denial of access to records of water or wastewater systems should such access be contrary to the public interest.

3.0 DEFINITIONS

3.1 "Agent" is defined as an employee or representative of a Company.

3.2 "Clearance" is defined as when an Individual, Company or its Agent has been approved by the Commission to access sensitive documents as defined in this regulation.

3.3 "Company" is defined as any business entity, including by not limited to a private firm,

partnership, sole proprietorship or government agency.

3.4 "ERISA" is defined as WSSC's Engineering Records Information Secured Access database

3.5 "External" is defined as any non-WSSC employee document user.

3.6 "Facility" is defined as any WSSC building or treatment site, including but not limited to the following: dam; water treatment plant; water pumping station; water storage facility; wastewater treatment plant; wastewater pumping station; Richard G. Hocevar Building (RGH); or depot/maintenance shop. The facility includes related piping and appurtenances (such as vaults and valves) contained within its property lines.

3.7 "Individual" is defined as any person whether representing themselves or a Company

3.8 "Internal" is defined as any WSSC employee document user.

3.9 "Internal Security Task Force ("ISTF") is defined as the standing committee of WSSC staff responsible for understanding, assessing, and addressing security vulnerabilities

3.10 "Principal" is defined as an authorized officer of a Company or an authorized representative of a government agency.

3.11 "Requestor" is defined as an Individual or Company seeking access to Sensitive Engineering Records as defined in this Procedure.

3.12 "Safety and Security Services Group ("SSSG")" is defined as the WSSC Safety and Security Service Group (SSSG), which implements the recommendations of WSSC's Internal Security Task Force, and is located in the Richard G. Hocevar Building located at 14501 Sweitzer Lane, Laurel, Maryland 20707.

3.13 "Sensitive Engineering Records" are defined as plans, drawings or documents relating to WSSC facilities or systems that could reasonably be used to aid in or plan for contaminating or damaging the WSSC system. Such records are limited to:

- Plans, blueprints, drawings, operational manuals, map books, or other records including threat assessments, disaster response plans, and contract documents relating to WSSC Water or Wastewater Facilities and Water Transmission Mains over 24" in diameter;
- Plans, blueprints, drawings, operational manuals, 200-foot sheets, map books, or other records, including contract documents, of the WSSC Water Distribution System; and
- Plans, blueprints, drawings, operational manuals, 200-foot sheets, or other records, including contract documents, of Sensitive On-Site Systems within the Washington Sanitary Suburban District.

3.14 "Sensitive on-site system" is defined as an on-site distribution or collection system owned or occupied by a federal, State or local government agency, to the extent such ownership or occupancy is known or satisfactorily proven to WSSC.

3.15 "Water Distribution System" is defined as the piping and appurtenances (except those covered under facilities) constituting the distribution network for the potable water system.

3.16 "WERI" is defined as WSSC's Engineering Records/Information system

4.0 RESTRICTIONS ON ACCESS TO RECORDS

4.1 Distribution and access to Sensitive Engineering Records varies depending on the type of asset for which they provide information. For the purposes of this policy, three classes are defined

4.1.1 Facilities and Transmission Mains over 24" in Diameter
4.1.2 Water Distribution System; and
4.1.3 Sensitive On-Site Systems.

4.2 The following restrictions apply:

4.2.1 Facilities and Transmission Mains over 24" in Diameter - Access is denied, however, engineers, contractors, and/or subcontractors working for WSSC on specific projects may request access as specified in the contract solicitation documents. Such access must also be approved by the SSSG Leader, and should access be approved, Sensitive Engineering Facility and Transmission Main Records will not be distributed to any Individual or Company until that Individual or Company has been approved to receive them in accordance with the procedures described in Section 5.0.

4.2.2 Water Distribution System Records - Access is denied, however, Requestors may be granted limited access to WSSC's Web Map or provided paper copies if approved under the procedures described in Section 5.0, below.

4.2.3 Sensitive On-Site System Records - Access is denied. Sensitive on-site documents will be provided only to the property owner or their designated agent of the particular on-site system. *There are no exceptions to this requirement.*

4.2.4 Note that these restrictions do not apply to records relating to inspections by or citations issued by the federal, State or local governments, or records relating to any of the above classes of facilities or infrastructure that have experienced a catastrophic or emergency event.

4.3 Approval of Requestor for either of the first two classes of information will be based upon proof of legitimate business purposes. Proof must be provided by the Requestor and confirmed by references as described in Section 5.0. Legitimate business purposes may include:

- Engineers or contractors involved in installation or repair of new or existing portions of the WSSC Facilities, Water Transmission Mains or Water Distribution System;
- Developers or engineers involved in identification of water and sewer system availability for new development;
- County governments using information for zoning, category changes, etc.;
- Potential bidders and subcontractors involved in work on distribution/collection

system and/or facilities;
- Engineers or contractors performing or bidding on on-site work, as authorized by on-site owner;
- Plumbers working on renovations/tie-ins to existing systems;
- Other utility companies' work requiring the use of sensitive documents; and/or
- Other business usages which are expressly authorized by the General Manager.

5.0 EXCEPTION REQUEST PROCEDURES

5.1 Application: In order to qualify for any of the exceptions to denial of access listed in Section 4.0 and receive any WSSC Sensitive Engineering Records, a Requestor must first submit an online application. The online application may be found on WSSC's Internet Page under "Businesses", "Development Services", "W.E.R.I.".

5.1.1 The application requires the following Requestor information:

- Full Name
- Driver's License Number and State of Origin
- Contact Information:
  - Home Information (required if the Requestor is self-employed or unemployed):
    - Address (including Number and Street, City, State, Zip and Country);
    - Telephone Number;
    - Fax Number (optional); and
    - E-Mail Address (required if internet access is requested).
  - Company Information (if applicable):
    - Address (including Number and Street, City, State, Zip and Country);
    - Telephone Number and Extension;
    - Fax Number (optional);
    - E-Mail Address (required if internet access is requested);
    - Name, telephone number, extension and fax number of Principal of

- Company authorizing access to WSSC records, if applicable. A Company Principal must confirm Requestor's employment, length of employment, position, and related business purpose.
- Description of Intended Business Use of WSSC Sensitive Engineering Records;
- Authorized WSSC Contact (required if Requestor is working on a project for WSSC); and
- Records/Information Requested (at least one box must be checked):
  - ☐ Paper or Electronic Copy
  - ☐ Internet Access to WSSC Web Map or eGIS system
- Requested User ID: (required for internet access only)

5.1.2 Applications may be submitted from any personal computer having internet access or at the WSSC's Security Desk counter located in the lobby of the RGH building in

Laurel, Maryland. Upon successful submission of the application, the Requestor will be provided with an application number for tracking purposes.

5.1.3 To complete the application process, the Requestor must personally appear at WSSC's Security Desk counter within 30 days of submitting the electronic application and provide a current, valid driver's license for validation of the application. If the Requestor does not complete the process within 30 days, their application will be deleted from the system and they will have to reapply for access. On a case-by-case basis, Individuals from a distant, out-of-state location or with a legitimate reason for not personally appearing may be allowed, at the discretion of the SSSG Leader, to mail in a signed copy of the application form with a copy of their current, valid driver's license to the SSSG at 14501 Sweitzer Lane, Laurel, Maryland 20707. The driver's license copy and signature on the application form must be notarized before mailing.

5.2 Validation: SSSG personnel at the Security Desk will access the Requestor's online application to confirm that the information provided on the application matches the information on the Requestor's driver's license and validate that the person presenting the driver's license is the same person pictured on the driver's license. Once the validation process is complete, the Requestor will be required to provide an electronic signature certifying that the information provided on the application is complete and accurate, acknowledging that providing false information could be cause for refusal, and agreeing to comply with specified renewal and non-disclosure terms (see Attachment – Application Form for Requesting Sensitive Engineering Records, for terms and conditions). The Requestor's driver's license will be scanned. Once the Requestor's signature and driver's license information have been captured electronically, the updated application will be submitted electronically for review and approval by the SSSG.

5.2.1 In the case of a notarized application submitted by a distant Requestor, SSSG will confirm the Requestor's signature, driver's license copy and notarization, scan in the driver's license and fill in the electronic signature with the words "OUT-OF STATE". The notarized application form will be forwarded, and the application status will change electronically, making it available for the SSSG to proceed with the Background Review.

5.3 Background Review: Upon receipt of a validated application, SSSG will conduct a background review. The background review may consist of personal contact with the Requestor, reference checks, and criminal history checks. The purpose of these checks is to verify the following information:

- Requestor's identity;
- Requestor's home address and telephone number;
- Requestor's business affiliation;
- Requestor's business address and telephone number;
- Legitimate business need (as defined previously in Section 4.3) for access to WSSC's Sensitive Engineering Records; and
- Lack of notable criminal history.

5.4 Requestors may be refused access to WSSC's Sensitive Engineering Records for the following reasons:

- Providing false identity, address, telephone number or other personal information;
- Providing false business information;
- Lack of legitimate need to access WSSC's Sensitive Engineering Records;
- Appearance on any Federal, State, or local terrorist watch list;
- Affiliation with terrorist, criminal, or subversive organizations;
- Violent criminal history;
- Criminal history that indicates extensive drug possession;
- Criminal history that indicates possession of drugs with the intent to distribute; and/or
- Other extensive criminal history.

6.0 APPROVAL

If approved, SSSG will change the status of the Requestor to Approved, and the system will automatically generate an email to notify the Requestor of the approval with a user Login ID and an initial password. The Requestor must login within 30 days of the origination date of the notification e-mail and change their initial password; if the Requestor fails to do so, their Login ID will become invalid and they will be required to re-apply for access to the system. If the login failure is due to a system error or a WSSC related circumstance out of their control, the Requestor may contact SSSG employees for assistance. If WSSC is found to be at fault, additional time may be provided for the required login.

7.0 DENIAL

Should the background review not be approved and access denied, the SSSG Leader will notify the Requestor by email and first class mail of the denial and the reasons for same. The Requestor may, within 30 calendar days after receipt of the notice of denial, request an administrative hearing pursuant to the procedures set forth in Section 12 of WSSC Standard Procedure L-07-01.

8.0 WSSC DISTRIBUTION OF SENSITIVE DOCUMENTS

WSSC employees (in any business unit) may NOT distribute Sensitive Engineering Records to External Users unless they have been approved through this process. This includes the following:

- An individual requesting a hard copy drawing(s);
- Contractors and subcontractors purchasing or obtaining bid documents containing Sensitive Engineering Records;
- Other government agencies requesting Sensitive Engineering Records; and/or
- Engineers/Consultants requesting Sensitive Engineering Records for projects for WSSC.

Any questions or concerns an employee has regarding an approved Individual, Company and/or Company Agent and the level of access granted must be addressed to the SSSG Leader.

The WSSC employee distributing Sensitive Engineering Records must confirm the Requestor's

identity (through checking photo ID), their approved status (using the ERISA system accessible from the WSSC intranet), and the legitimate business purpose. WSSC employees shall provide only the information needed to accomplish the legitimate business purpose. When possible, the Employee should transmit the necessary information without the disclosure of Sensitive Engineering Records (e.g., providing text description of requested information rather than a drawing.) Any applicable fees for copying would apply.

9.0 DISTRIBUTION OR DISCLOSURE OF RECORDS PROVIDED UNDER THIS PROCEDURE

Distribution or disclosure of Sensitive Engineering Records by approved Requestors to other individuals or entities is governed by the terms of the Non-Disclosure Agreements signed (or accepted) by the Individual during the registration/application process. The intent of the Non-Disclosure Agreement is to prevent any unauthorized exchange, distribution, or disclosure of Sensitive Engineering Records by approved Requestors to other individuals or entities. The degree of exchange, distribution, or disclosure will be limited based on the class of documents and the projects or business purpose involved. A copy of the Non-Disclosure Agreement is attached.

DISTRIBUTION:

Commission Wide

MASTER VOLUME LIST:

General Manager/CEO
Corporate Secretary
Human Resources
Internal Audit

OTHER DISTRIBUTION:

Chief of Staff
Deputy General Manager
Staff Offices
Team Chiefs
Directors
Group Leaders

ATTACHMENT –

Terms and Conditions and Non-Disclosure Agreement on Application Form for requesting Sensitive Engineering Documents

By signing this application, I certify that this application is complete and accurate to the best of my knowledge and that I have not made any attempt to conceal information. I understand that falsification could be cause for refusal. I also agree to the following terms:

- WSSC reserves the right to require occasional renewal of this application. If the application is not renewed when required, documents will not be released until application renewal is completed.
- I will abide by the terms of non-disclosure listed below. Failure to do so may result in permanent revocation of my right to access WSSC records/information. In such case, WSSC also reserves the right to demand immediate delivery or return of all WSSC records/information, documents, and files.

Non-disclosure Agreement - As a condition to allowing me access to WSSC engineering records/information or Internet access to such, I, the Requestor, agree to the following:

- The records/information provided by WSSC shall not be used by me other than for the legitimate business purpose provided to WSSC.
- The records/information will be treated as belonging to WSSC, and shall not, without WSSC's prior written consent, be disclosed in any manner, in whole or in part, to anyone.