


Kenneth E. Hill, P.E.  
Planning & Coordination Manager  
2317 South Jackson, Room 312  
Tulsa, Oklahoma 74107  
Phone: 918.596.9240

**PUBLIC WORKS & DEVELOPMENT DEPARTMENT  
ENGINEERING SERVICES DIVISION**

# Memo

**To:** Charles Hardt  
**From:** Kenneth Hill   
**CC:** Paul Zachary  
**Date:** January 29, 2004  
**Re:** Information Protection Protocol

---

Attached is an RFA and 'Information Protection Protocol' document to present to the Mayor for adoption as policy by Executive Order. This 'Information Protection Protocol' is developed to safeguard vulnerability assessments, security plans, record drawings of public facilities, and any information derived from them. This document describes the policies and security procedures that will be put in place by the City of Tulsa to protect from unlawful access and use the copies of vulnerability assessments and other sensitive information. The Public Facilities Security Manager will administer the policy.

Development of a policy to protect sensitive information was identified as an action item in the findings of Internal Audits (IA) review of the City's security programs. The draft document was submitted to Internal Audit for review on August 27, 2003. I received an email from Cathy Criswell, IA, on August 28, 2003 approving the plan (document).

The Mayor's Homeland Security Technical Advisory Group (HLS-TAG) reviewed and approved this document on December 15, 2003.

Staff recommends approval.

---

# Information Protection Protocol

City of Tulsa, Oklahoma

---

Adopted this \_\_\_\_\_ day of FEB 16 2004, 2004  
by Executive Order No. 2004-01 establishing an administrative procedure to  
safeguard sensitive information for the City of Tulsa, Oklahoma.

  
Mayor

  
ATTEST: City Clerk



APPROVED AS TO FORM:

By: MDS  
ASST. CITY ATTORNEY

## EXECUTIVE SUMMARY

This "information protection protocol" describes the policies and security procedures to manage vulnerability assessments of critical City facilities and other sensitive information, including emergency operational plans and protective measures, under strict security arrangements and to develop the necessary protocols to protect copies of the assessments and other sensitive information described herein. ***The applicable assessments and sensitive information may be kept confidential as provided for in Section 24A.27 of Title 51 of the Oklahoma Statutes.***

This Information Protection Protocol is developed to safeguard vulnerability assessments, security plans and any information derived from them. This protocol ensures that all assessments are kept in a secure location. Only the individual designated by the department head, the Public Facilities Security Manager and Public Works Planning & Coordination Manager will have access to these documents. No assessment or "information derived from" a completed vulnerability assessment will be available to anyone other than those persons designated.

This protocol establishes a number of protective measures. The protocol ensures that vulnerability assessments are stored behind closed doors, filed under lock at all times, and accessed only by designated persons under strict security procedures. A master copy of the vulnerability assessments will be housed in the office of the Planning & Coordination Manager of the Public Works Department. A document tracking system will allow the vulnerability assessments to be traceable at all times to a single person. Documents will be labeled as sensitive and covered to show that they must be protected. Copying, faxing and loaning of vulnerability assessments will be prohibited except on a rare, case-by-case basis as authorized by the department head.

The department head, or his/her designee, will oversee the protection of the information, manage the day-to-day implementation of the protocol and conduct routine security check-ups. Access will be withdrawn when a designated person terminates employment or no longer requires access because of a change in duties or position. The City will develop and maintain a stringent training program for protection of such data and will perform audits and inspections to ensure accountability. Each designated person must receive annual refresher security training.

**Unauthorized copying and/or distribution of or the dissemination of any sensitive information by a City employee or contractor may result in disciplinary action up to and including dismissal or termination of contract.**

## **CHAPTER 1: PURPOSE AND DEFINITIONS**

---

### **1.1 Authority**

Vulnerability assessments, information technology, response plans, and other sensitive information may be kept confidential as provided for in Section 24A.27 of Title 51 of the Oklahoma Statutes.

### **1.2 Purpose of this Protocol**

This "Information Protection Protocol" describes the policies and security procedures put in place by the City of Tulsa to protect from unlawful access and use the copies of vulnerability assessments.

This protocol is intended to serve as the security manual for individuals to be designated by the department head to have access to the vulnerability assessments.

### **1.3 Definitions**

**Authorized Access List:** A list of those persons who the department heads have designated for access to vulnerability assessments. Includes the names of the designated individuals, the date of designation, and the date their annual refresher training is due.

**Designated Person or Designee or otherwise authorized individuals:** In addition to the department head, a designated person or designee is an individual designated by the department head to have access to vulnerability assessment(s). An otherwise authorized individual is a person to whom a designated individual is authorized to provide access to vulnerability assessment information.

**Information contained in or derived from a vulnerability assessment:** Information originating from a submitted vulnerability assessment or information generated by the department as a result of reviewing and analyzing submitted vulnerability assessments.

**Public Facilities Security Manager:** Employee assigned to oversee the protection of vulnerability assessment information and implementation of this protocol.

**PW Planning Manager:** The manager, or person-in-charge, of the Planning & Coordination Section of the Public Works Department.

**Vulnerability Assessment or VA:** A review of certain specified items to assess the vulnerabilities of critical facilities to natural, technological and manmade hazards, including terrorist attack or other intentional act, that may substantially disrupt the ability of the facility to continue normal operations.

Vulnerability Assessment Information: Used to refer to both vulnerability assessments submitted to the department and information contained in or derived by the department from a submitted vulnerability assessment.

## **CHAPTER 2: MANDATORY PROTECTIVE MEASURES**

---

The department will observe the following protective measures in location(s) where vulnerability assessments are kept and secured.

### **2.1 Copies of Vulnerability Assessment Information**

Three (3) copies of the reports developed for the vulnerability assessments of critical City facilities, also identified as Priority 1 Buildings, are maintained in the offices of the Public Facilities Security Manager, PW Planning Manager, and a person in each department designated by the department head to be responsible for the report. Each report will be numbered for tracking purposes. The department will receive document number "1"; the Public Facilities Security Manager will receive number "2"; and the PW Planning Manager will maintain document number "3".

The vulnerability assessments conducted of the water and wastewater systems under the Federal Bioterrorism Act of 2003 and the Wastewater Security Act of 2003 provide six (6) copies of each report. The Public Facilities Security Manager will maintain a distribution list of persons provided copies of these reports. The Environmental Protection Agency (EPA) in Washington, D.C also maintains a copy. Each report is numbered for tracking purposes.

### **2.2 Tracking System**

A designated individual in each department will monitor the vulnerability assessment for management and tracking of the document. The Public Facilities Security Manager will maintain a master list of designated persons reported by the department heads.

### **2.3 Markings to identify Vulnerability Assessment Information**

All vulnerability assessments, and any sensitive documents produced in the course of analyzing the vulnerability assessments will be marked, with a stamp ("CONFIDENTIAL") to identify the sensitivity of the information. The stamp must be placed on the front of the first page (or on the cover, if the document has one) and on the back of the last page (or back cover, if the document has one). Other pages may be marked, as necessary.

### **2.4 Secure File and Review Area**

The designated person will maintain the vulnerability assessment in a secure locked cabinet. As much as possible, the cabinet will be located within an already-existing protected area. The area will have a secure door with a secure doorframe and doorjamb. This provision also applies to the Public Facilities Security Manager and PW Planning Manager.

A review area will be provided, as necessary. Removal of the vulnerability assessment from the office of the designee shall be discouraged.

## **2.5 Custody Rules**

The designated person responsible for the vulnerability assessment will maintain a "Document Activity Log" (Exhibit A). Individuals, other than the designated person, must provide a printed name, signature, date removed and time of removal. The designated person must also acknowledge removal of the document by initials. When returning the document to the cabinet, the recipient must indicate the date returned and initial the entry. An activity log is attached for use. When the document is not being used, the document must be returned to the locked cabinet.

## **2.6 Copying Restrictions and Numbering**

The vulnerability assessments shall **not** be copied, in part or in whole, except on a rare, case-by-case basis as authorized by the department head. If and when the department head authorizes copying, it shall be for the purpose of design and construction of recommended physical security measures or for the purpose of developing and implementing operating procedures.

**Unauthorized copying and/or distribution of or the dissemination of any sensitive information by a City employee or contractor may result in disciplinary action up to and including dismissal or termination of contract.**

## **2.7 Fax Transmissions**

Transmission of vulnerability assessments by fax is strictly prohibited.

## **2.8 Use of Electronic Mail (E-Mail)**

The use of email or any other electronic mail system to transmit vulnerability assessment information is strictly prohibited.

## **2.9 Protecting Information Derived from Vulnerability Assessments**

The department will protect information derived from submitted vulnerability assessments in the same fashion as submitted vulnerability assessments.

## **2.10 Use of Computers**

There will be no electronic version of vulnerability assessments, and no information derived from vulnerability assessments will be kept in electronic systems with public access or maintained on other than a secure server.

## **2.11 Discussing Sensitive Vulnerability Assessment Information in Meetings**

A check to determine that all meeting participants have been designated will precede any discussion of information pertaining to vulnerability assessments. The chair of any meeting that involves a discussion of vulnerability assessment information must ensure that only designated or otherwise authorized individuals are present. At the close of the meeting, the chair of the meeting must ensure all sensitive information, including materials produced at the meeting, is secure.

## **2.12 Periodic Security Reviews**

The Technical Advisory Group of the Mayor's Homeland Security Task Force will conduct periodic security inspections/reviews to ensure security practices are being followed. Those conducting the security reviews will promptly document the findings and report the findings to the Mayor's office and the department head.



## **CHAPTER 3: DESIGNATIONS AND AUTHORIZED ACCESS PROCEDURES**

---

### **3.1 Selection of Designated Persons**

The department head will designate those individuals determined to need access to the vulnerability assessments. The following criteria shall be used to identify designated individuals.

- Role in conducting and reviewing the vulnerability assessments, and implementing security measures;
- Knowledge of department facilities and conducting vulnerability assessments; and
- Knowledge of implementing protective measures, structural and non-structural (i.e. CIP's, SOP's, ERP's).

### **3.2 Basic Responsibilities of Designees**

Designated persons must protect and safeguard any vulnerability assessment information at all times and in compliance with this protocol, not discuss sensitive information with anyone who is not a designated individual and promptly report any apparent violation of access to the department head or Public Facilities Security Manager.

It is recognized that situations not covered by this protocol may arise. In such cases, the Public Facilities Security Manager will be available for guidance, and each designated person will ensure through personal conduct and accountability that he or she will act consistently within these guidelines to protect, to the best of his or her ability, all vulnerability assessment information.

### **3.3 Public Facilities Security Manager**

The "**Public Facilities Security Manager**" will oversee the protection of vulnerability assessment information and the implementation of this protocol. The Public Facilities Security Manager will:

- Be the focal point for protection of vulnerability assessment information.
- Maintain the Vulnerability Assessment Tracking System.

### **3.4 Use of Contractors**

If the City enters into a contractual relationship in order to carry out recommendations contained in the vulnerability assessments, and contract employees need to be designated, these employees will be required to follow the City's policy and procedures and implement this protocol as any designated individual. An *"Access and*

*Confidentiality Agreement*" (Exhibit B) must be executed in full prior to the release of information.

### **3.5 Removal of Designation or Termination of Access**

The department head will withdraw designations when an individual no longer requires access to vulnerability assessments because of a change in duties or position. An individual may also be withdrawn if found not to be adhering to security procedures.

Upon completion of work by a contracted firm or employee, a "*Confidentiality Agreement for Termination of Designation*" (Exhibit C) shall be executed.

## EXHIBIT A

### DOCUMENT ACTIVITY LOG

**VA TRACKING/FACILITY:** \_\_\_\_\_

Printed Name	Dept., Agency, Firm	Signature	Date Removed	Time Removed	Designee (Initial)	Date Returned	Returned By

This sheet is to remain on the file drawer, visible while the document is in use. It is meant to identify which files have been removed and to assist with re-filing. Thank you.



**EXHIBIT C**

**CONFIDENTIALITY AGREEMENT FOR TERMINATION OF DESIGNATION**

In accordance with my official duties, I have had access to information contained in vulnerability assessments. Because of a change in duties or position, or completion of work under contract to the City of Tulsa, I no longer require access to this information.

I understand that vulnerability assessment information may not be disclosed except as authorized by the City of Tulsa.

I certify that I have returned all vulnerability assessment information in my custody to the Public Facilities Security Manager as specified in the "Information Protection Protocol for Vulnerability Assessments."

I certify that I have not reproduced any documents from the vulnerability assessments or other sensitive information derived from the vulnerability assessments.

I further agree that I will not disclose any vulnerability assessment information to any person upon completion of my duties or contracted services and am subject to the following action.

- I understand that as a person who has had access, I am subject to disciplinary action, including termination of employment, if I knowingly or recklessly disclose this information.
- I understand that as a person who has had access that revealing this information may lead to debarment from performing future contracts with the City of Tulsa.

<hr/>	
<b>Full Name (print)</b>	
<hr/>	<hr/>
<b>Department</b>	<b>Contractor Name and No. (if applicable)</b>
<hr/>	<hr/>
<b>Signature</b>	<b>Date</b>
<hr/>	<hr/>
<b>Signature Security Manager</b>	<b>Date</b>
<hr/>	<hr/>



[Home](#) [Courts](#) [Court Dockets](#) [Legal Research](#) [Calendar](#) [Help](#)

[Previous Section](#) [Top Of Index](#) [This Point in Index](#) [Citationize](#) [Next Section](#)

Title 51. Officers

## Oklahoma Statutes Citationized

### Title 51. Officers

#### Section 24A.27 - Confidential Vulnerability Assessments

Cite as: 51 O.S. § 24A.27 (OSCN 2004)

---

A. Any state environmental agency or public utility shall keep confidential vulnerability assessments of critical assets in both water and wastewater systems. State environmental agencies or public utilities may use the information for internal purposes or allow the information to be used for survey purposes only. The state environmental agencies or public utilities shall allow any public body to have access to the information for purposes specifically related to the public bodies function.

B. For purposes of this section:

1. "State environmental agencies" includes the:

- a. Oklahoma Water Resources Board,
- b. Oklahoma Corporation Commission,
- c. State Department of Agriculture,
- d. Oklahoma Conservation Commission,
- e. Department of Wildlife Conservation,
- f. Department of Mines, and
- g. Department of Environmental Quality;

2. "Public Utility" means any individual, firm, association, partnership, corporation or any combination thereof, municipal corporations or their lessees, trustees and receivers, owning or operating for compensation in this state equipment or facilities for:

- a. producing, generating, transmitting, distributing, selling or furnishing electricity,
- b. the conveyance, transmission, reception or communications over a telephone system,
- c. transmitting directly or indirectly or distributing combustible hydrocarbon natural or synthetic natural gas for sale to the public, or
- d. the transportation, delivery or furnishing of water for domestic purposes or for power.

#### **Historical Data**

---

Added by Laws 2003, HB 1146, c. 166, § 1, emerg. eff. May 5, 2003.

---

#### **Citationizer® Summary of Documents Citing This Document**



[Home](#) [Courts](#) [Court Dockets](#) [Legal Research](#) [Calendar](#) [Help](#)  
[Previous Section](#) [Top Of Index](#) [This Point in Index](#) [Citationize](#) [Next Section](#)

Title 51. Officers

## Oklahoma Statutes Citationized

### Title 51. Officers

#### Section 24A.28 - Confidentiality of Information Relating to Terrorism

Cite as: 51 O.S. § 24A.28 (OSCN 2004)

---

The following information may be kept confidential:

- A. Investigative evidence of a plan or scheme to commit an act of terrorism;
- B. Assessments of the vulnerability of government facilities or public improvements to an act of terrorism and work papers directly related to preparing the assessment of vulnerability;
- C. Plans for deterrence or prevention of or protection from an act of terrorism;
- D. Plans for response or remediation after an act of terrorism;
- E. Information technology of a public body or public official but only if the information specifically identifies:
  - 1. Design or functional schematics that demonstrate the relationship or connections between devices or systems;
  - 2. System configuration information;
  - 3. Security monitoring and response equipment placement and configuration;
  - 4. Specific location or placement of systems, components or devices;
  - 5. System identification numbers, names, or connecting circuits;
  - 6. Business continuity and disaster planning, or response plans; or
  - 7. Investigative information directly related to security penetrations or denial of services; or
- F. Investigation evidence of an act of terrorism that has already been committed.

For the purposes of this section, the term "terrorism" means any act encompassed by the definitions set forth in Section 1268.1 of Title 21 of the Oklahoma Statutes.

#### **Historical Data**

---

Added by Laws 2003, SB 395, c. 175, § 2, emerg. eff. May 5, 2003.

---

#### **Citationizer® Summary of Documents Citing This Document**

---