Information Security Standard (ISEC S-06.)

Sensitive Regulated Data: Permitted and Restricted Uses

Standard number:	ISEC- S-06-1
Date issued:	2/3/17
Date last reviewed:	2/22/17
Version:	1.0
Approval authority:	Internal Services Director
Responsible office:	Information Security Office

1. **Purpose**

   The City of Tempe engages in business activities that encompass a variety of sensitive regulated data. This standard defines permitted and restricted uses of such city-owned data, including the IT environments in which these data are maintained by staff.

   This standard is governed by the following Personnel Rules:

   Rule 405.A Use of Technology

   By implementing this standard, Tempe establishes a city-wide framework to comply with federal, state, and local law, and/or contractual agreements that require the city to implement specific privacy and security safeguards.

2. **Scope and Authority**

   This standard applies to all City of Tempe employees and workforce members.

   Information Technology, a division of Internal Services, is responsible for the maintenance and interpretation of this standard.

3. **Standard**

   City employees have individual and shared responsibilities to:

   - process, handle and maintain city-owned sensitive regulated data in accordance with federal, state, and local law, and/or city policy or agreement;
   - implement specific privacy and security safeguards as mandated by federal, state, local law, including, if any, additional department-specific safeguards;

- maintain city-owned sensitive regulated data on personally owned devices in compliance with the provisions of the Guidelines for Securing Sensitive Data on Personally Owned Devices, including, if any, additional department-specific restrictions;
- report a violation of this standard, whether intentional or unintentional, as an information security incident to security@tempe.gov or by calling 480-350-2900 within 24 hours.

4. **Violation of the Standard - Misuse of Information**

   In accordance with Rule 405 A, Responsible Use of Technology, the city characterizes certain activities related to misuse of regulated data as unethical and unacceptable. Violations of this standard may result in disciplinary action up to and including termination, and/or legal action. (Rule 406.C35)

5. **Definitions**

   Sensitive Regulated Data: For purposes of this standard, "sensitive regulated data" is defined as data that requires the city to implement specific privacy and security safeguards as mandated by federal, state, local law, and/or city policy or agreement. Regulations or categories of data most applicable to the City include:

   1. Health Insurance Portability and Accountability Act (HIPAA)
   2. Family Medical Leave Act (FMLA)
   3. Personally Identifiable Information (PII)
   4. Payment Card Industry Data Security Standards (PCI-DSS)
   5. Critical Infrastructure Information Presidential Policy Directive 21 (PPD-21)
   6. Sensitive Security Information (SSI) and IT System Configuration Information
   7. Sensitive Law Enforcement and Criminal Justice System Information (CJIS)
   8. Attorney/Client Privilege Information (defined)

6. **References**

   1) Handbook for Safeguarding Sensitive Personally Identifiable Information
   2) Security Laws and Regulations Related to Handling Sensitive Data
   3) Maintaining Payment Security
   4) Presidential Policy Directive 21 (PPD-21)

Appendix A

Personally Identifiable Information (PII)

Personally Identifiable Information (PII) is a category of sensitive information that is associated with an individual person, such as an employee, resident, or patient. PII should be accessed only on a strict need-to-know basis and handled and stored with care.

PII is information that can be used to uniquely identify, contact, or locate a single person. Personal information that is "de-identified" (maintained in a way that does not allow association with a specific person) is not considered sensitive. Note that employee ID numbers by themselves are not considered sensitive or private personal information.

City policies, contractual obligations, and federal and state laws and regulations require appropriate protection of PII that is not publicly available. These regulations apply to PII stored or transmitted via any type of media: electronic, paper, microfiche, and even verbal communication.

PII does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

PII pertaining to the Public:

- Social Security number (There are additional restrictions on where Social Security numbers can be stored and shared.)
- National ID number
- Passport number
- Visa permit number
- Driver's license number
- Bank and credit/debit card numbers
- Tax information (e.g., W-2, W-4, 1099)
- Disability information
- Ethnicity
- Gender
- The location of an individual at a particular time
- Web sites visited
- Materials downloaded
- Any other information reflecting preferences and behaviors of an individual
- Internet Protocol (IP) address (source and destination) in conjunction with other PII. IP address may identify an individual originating a transaction as well as the recipient.

PII pertaining to Employees:

- Biographic/demographic data
    - Date and location of birth
    - Country of citizenship
    - Citizenship status
    - Marital status
    - Military status
- Criminal record

- Home address
- Grievance information
- Discipline information
- Leave-of-absence reason
- Health information (There are additional restrictions on where Protected Health Information can be stored and shared).

Additional Resources:

Handbook for Safeguarding Sensitive Personally Identifiable Information

Appendix B

Security of Personally Owned Devices that Access or Maintain Sensitive Restricted Data

I. Overview

When conducting City business, it may at times be necessary for employees, agents, affiliates or workforce members to access or maintain *sensitive data* on *personally owned devices*. There is often risk of data loss or unauthorized access when sensitive data is accessed or maintained via self-managed personally owned devices.

This policy directs employees who access or maintain sensitive institutional data to meet their shared obligation and responsibility to secure such data by properly self-managing the privacy and security settings on their personally owned device.

II. Policy

Sensitive data shall be accessed or maintained on personally owned devices only when necessary for the performance of City-related duties and activities. Employees shall take all required, reasonable, and prudent actions necessary to ensure the security and retention of sensitive data.

A. Permission to Use Personally Owned Devices

Department Directors shall decide on a department-by-department basis whether to allow employees, agents, affiliates or workforce members to use personally owned devices to access or maintain sensitive data.

B. Device Security

City employees, agents, affiliates and workforce members shall maintain up-to-date, device-appropriate security safeguards and follow the policies, standards, and guidance provided by the City's IT Division, as well as comply with appropriate safeguards required by state and federal regulations. In addition, the City or individual departments may require that specific security settings and/or software to protect sensitive data be put in place and maintained on the device. It is the responsibility of the employee to check with their department Director for specific requirements.

C. Data Return/Deletion

Users shall return or delete sensitive data maintained on personally owned devices upon request from the City or when their role or employment status changes such that they are no longer an authorized user of that data.

D. Incident Reporting

Personally owned devices that access or maintain sensitive data and that are lost, stolen, have been subject to unauthorized access, or otherwise compromised must be reported within 24 hours to both their department Director and the IT Security Office at: security@tempe.gov.

E. Device Inspection

In the course of an incident investigation, the City reserves the right to inspect a personally owned device that accesses or maintains sensitive data. Any access to a personally owned device will be carried out in accordance with Tempe rules regarding Privacy and the Need to Monitor and Access Records, as well as follow other relevant City protocols, and legal or law enforcement requirements.

F. Response to Document Requests and Production

Records or data maintained by the City or employees, agents, workforce members, and affiliates may be the subject of document requests (e.g., Freedom of Information Act) or document production (e.g., warrants, subpoenas, court orders, etc.). City employees, agents and affiliates must produce these records or data (or the devices on which they are stored) upon request of the City.

III. Applicability

This policy is applicable to all City employees, agents and workforce members. In accordance with Rule 405 A, Responsible Use of Technology, the City characterizes certain activities related to misuse of sensitive data as unethical and unacceptable. Violations of this policy may result in disciplinary action up to and including restricting the ability to use a personally owned device for work-related activities, termination, and/or legal action

IV. Definitions

Device: For purposes of this guide, a device is defined as an object with the ability to engage in computational operations, including the accessing or storing of electronic data.

Record: For purposes of this guide a Record is data that satisfies one or more of the following criteria:

- It is relevant to planning, managing, operating, controlling, or auditing administrative functions of an administrative or operational department of the City;
- It is created, received, maintained, or transmitted as a result of planning, managing, operating, controlling, or auditing administrative functions of an administrative or operational department of the City;
- It is generally referenced or required for use by more than one organizational unit;
- It is included in an official City administrative report;
- It is used to derive an element that meets the criteria above;
- It is generated by a City workforce member or agent using any of the above data.

Sensitive data: Sensitive data is defined as information whose unauthorized disclosure may have serious adverse effect on the City's reputation, resources, services, or individuals. It includes information protected under federal or state regulations or subject to proprietary, ethical, or privacy considerations.

Personally owned: For purposes of this guide, *personally owned* includes devices for which a user receives a city subsidy or stipend as well as those wholly owned by the employee.

Appendix C

Sensitive Security Information (SSI)

The SSI regulation lists 16 categories of affected information, and allows the Secretary of Homeland Security and the Administrator of the Transportation Security Administration to designate other information as SSI.

The 16 SSI categories as listed in Code of Federal Regulations - CFR 49 §1520.5(b) are:

1. Security programs and contingency plans.
2. Security Directives.
3. Information Circulars.
4. Performance specifications.
5. Vulnerability assessments.
6. Security inspection or investigative information.
7. Threat information.
8. Security measures.
9. Security screening information.
10. Security training materials.
11. Identifying information of certain transportation security personnel.
12. Critical aviation or maritime infrastructure asset information.
13. Systems security information.
14. Confidential business information.
15. Research and development.
16. Other information. (Determined in writing by DHS or DOT; rarely used.)

For example, SSI includes airport and aircraft operator security programs; the details of various aviation, maritime or rail transportation security measures including perimeter security and access control; procedures for the screening of passengers and their baggage; the results of vulnerability assessments of any mode of transportation; the technical specifications of certain screening equipment and the objects used to test such equipment; and, training materials that could be used to penetrate or circumvent security.

An agency Final Order on SSI can only be challenged in the United States court of appeals.