Texas A&M University System Standard - Notification of Unauthorized Access, Use, or Disclosure of Sensitive Personal Information

Reason for Standard

This standard is to be enacted upon discovery or notification that sensitive personal information has been acquired or is reasonably believed to have been acquired by an unauthorized person, or used in an unauthorized manner.

The standards herein are in accordance Section 2054.1125 of the Texas Government Code.

Definitions

Compromised System: Any system where unauthorized access has been achieved.

Information Resources (IR): The procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

Media: Materials that hold data in any form or that allow data to pass through them, including paper, transparencies, multipart forms, hard, floppy and optical disks, magnetic tape, wire, cable and fiber.

Sensitive Personal Information: An individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:

- Social security number;
- Driver's license number or government-issued identification number; or
- Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or
- Information that identifies an individual and relates to:
  - The physical or mental health or condition of the individual;
  - The provision of health care to the individual; or
  - Payment for the provision of health care to the individual.

The term "sensitive personal information" does not include publicly available information that is lawfully made available to the public from the federal government or a state or local government.

Also refer to System Regulation 29.01.03 and the related Data Classification standard.

Unauthorized Access: Gaining access into any computer, network, storage medium, system, program, file, user area, or other private repository, without the express permission of the owner.

Official Standard

---

1. APPLICABILITY

This Standard (standard) applies to System Office (SO) information resources, including media that access or contain unencrypted sensitive personal information.

The intended audience includes, but is not limited to, System Administrators, information security personnel, and Directors.

For alternate or additional standards applicable to branch campuses, refer to section 2.5.

2. STANDARDS

2.1 Once unauthorized disclosure, access, or use has been discovered, appropriate measures are to be taken to halt any further unauthorized activity.

2.2 If a compromised system or media contained unencrypted sensitive personal information, the System Administrator/investigator must determine whether sensitive personal information was acquired or is reasonably believed to have been acquired by an unauthorized person.

2.3 If a determination is made that sensitive personal information:

- Was or is reasonably believed to have been accessed/acquired by an unauthorized person;
- Was disclosed in any manner to an unauthorized person; or
- Was used in an unauthorized manner;

The investigator (System Administrator or other responsible party) is to provide notification of the unauthorized activity and data, as soon as feasible, to SO Information Security Officer (ISO). This notification is to contain at least the following:

- A description of the file contents (e.g., field description, data type); and
- The number of persons whose information was contained in the file(s).

The Director of the department acting as custodian and/or owning the data is to be notified of the unauthorized activity as well.

2.4 SO ISO will work with all appropriate System Office and University personnel, including University Police, to ensure all required information is identified and all persons whose information may have been subject to unauthorized access, use, or disclosure are notified in accordance with applicable laws.

2.5 Refer to the instructions for any breach, data loss, hack and incident.

Contact Office

For standard interpretation and classification contact The Texas A&M University System Chief Information Officer

OFFICE OF RESPONSIBILITY: The Texas A&M University System Chief Information Officer