STANDARD ADMINISTRATIVE PROCEDURE

29.01.03.M1.24 Information Resources – Notification of Unauthorized Access, Use, or Disclosure of Sensitive Personal Information

Approved July 27, 2006
Revised September 15, 2010
Revised August 14, 2013
Revised November 25, 2014
Next Scheduled Review: November 25, 2019

Reason for Standard Administrative Procedure

This procedure 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 procedures 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 - 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.

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 Procedure/ Responsibilities/ Process

---

1. APPLICABILITY

This Standard Administrative Procedure (SAP) applies to University information resources, including media, which access or contain unencrypted sensitive personal information.

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

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

2. PROCEDURES

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 the Texas A&M IT: Chief Information Security Officer (ciso@tamu.edu, 979-845-0372); OR security@tamu.edu; OR itpolicy@tamu.edu; OR, after normal business hours,

call Help Desk at 979-845-8300. This notification is to contain at least the following:

2.3.1 a description of the file contents (e.g., field description, data type); and,

2.3.2 the number of persons whose information was contained in the file(s).

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

2.4 The CISO or designee will work with all appropriate university personnel and offices, 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 Reporters/investigators for branch campuses shall contact the CIO or Director of the information technology department for the reporting branch campus and inform them of the incident. The CIO, Director of information technology, or designee will coordinate with the Director or Department Head of the department which has had the incident, the Campus Police, and Texas A&M University IT CISO.

Related Statutes, Policies or Requirements

SAP *16.99.99.M0.04, Business Associates Agreement*

SAP *16.99.99.M0.26, Investigation and Response to Breach of Unsecured Protected Health Information (HITECH)*

Texas A&M Information Security Control IR-6 Incident Reporting

Contact Office

CONTACT: Office of the Chief Information Security Officer

OFFICE OF RESPONSIBILITY: Vice President for Information Technology & Chief Information Officer