

INFORMATION TECHNOLOGY STANDARD ADMINISTRATIVE PROCEDURES

SAP No. 24.99.99.W1.30

Information Resources – Notification of Unauthorized Disclosure of Sensitive Personal Information

Approved: April 15, 2005

Last Revised: August 30, 2011

Next Scheduled Review: August 2012

Supplements [University Rule 24.99.99.W1](#)

1. General

This procedure is to be enacted upon discovery or notification that as a result of a breach of system security (unauthorized access) or unintentional disclosure, sensitive personal information has been acquired or is reasonably believed to have been acquired by an unauthorized person.

The procedures herein are in accordance with Article 2.29 of the Texas Code of Criminal Procedure, Chapter 48 of Title 4 of the Texas Business & Commerce Code.

2. Applicability

This Standard Administrative Procedure (SAP) applies to university 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, Department Heads and Directors.

3. Definitions

3.1 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

(1) Social security number

(2) Driver's license number or government-issued identification number or

(3) 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.

- 3.2 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.
- 3.3 Compromised System: Any system where unauthorized access has been achieved.
- 3.4 Information Resources: Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.
- 3.2 Media: Materials that hold data in any form or that allow data to pass through them, including paper, transparencies, multipart forms, hard drives, floppy and optical drives, magnetic tape, wire, cable, and fiber.
- 3.3 Information Security Officer (ISO): Responsible to the executive management for administering the information security function within the agency. The ISO is the university's internal and external point of contact for all information security matters.

4. Procedures

- 4.1 Once a compromised system or unauthorized access has been discovered, appropriate measures are to be taken to halt any further unauthorized access.
- 4.2 If the 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.
- 4.3 If the determination is that sensitive personal information was or is reasonably believed to have been acquired by an unauthorized person, the System Administrator/investigator is to provide notification of the disclosure, as soon as feasible, to the information security officer (ISO) (security@wtamu.edu or 806-651-7919 during business hours, Monday through Friday, or 806-651-4357 during nights and weekends). The division/department head or director of the department acting as custodian and/or owning the disclosed data is to be notified as well. This notification

is to contain at least the following information:

- 4.3.1 A description of the file contents that may have been disclosed (e.g. field description, data type); and
 - 4.3.2 The number of persons whose information was contained in the file(s) that were disclosed.
- 4.2 The information security officer (ISO) will work with all appropriate university personnel and offices, including university police, to ensure that all required information is identified and that all persons whose information may have been disclosed are notified in accordance with applicable laws.

OFFICE OF RESPONSIBILITY: Information Technology

CONTACT: Chief Information Officer