Texas A&M University System Standard – Privacy

Standard Statement

This standard establishes responsibilities and limits for system administrators and users in providing privacy for System Office (SO) information resources.

Reason for the Standard

The SO has the right to examine information on information resources which are under the control or custody of the SO. The general right to privacy is extended to the electronic environment to the extent possible.

However, there should be no expectation of privacy beyond that which is expressly provided by applicable privacy laws. Privacy is limited by the Texas Public Information Act, administrative review, computer system administration, and audits.

Definitions

Confidential - Information that must be protected from unauthorized disclosure or public release based on state or federal law (e.g. the Texas Public Information Act and other constitutional, statutory, judicial, and legal agreements). See System Regulation 29.01.03 and the related Data Classification Standard for more information.

Examples of "Confidential" data may include but are not limited to the following:

- Personally Identifiable Information, such as: a name in combination with Social Security number (SSN) and/or financial account numbers
- Student Education Records
- Intellectual Property, such as: certain intellectual property as set forth in section 51.914 of the Texas Education Code
- Medical Records

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.

File Owner: Holder (assignee) of the computer account which controls a file. Not necessarily the owner in the sense of property.

Information Resource Owner: An entity responsible:

1) For a business function; and,
2) For determining controls and access to information resources supporting that business function.

Applicability

This standard applies to electronic information created, transmitted, received, or stored on information resources owned, leased, administered, donated to or otherwise under the custody and control of the SO.

The information resource owner, or their designee, is responsible for ensuring that the risk mitigation measures described in this standard are implemented. Based on risk management considerations and business functions, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures provided in this standard. All exclusions must be in accordance with standard *Exclusions from Required Risk Mitigation Measures*.

The audience for this standard is *all users and administrators* of SO information resources.

Standards

1. Privacy of information shall be provided to users of SO information resources consistent with obligations of Texas and Federal law and/or secure operation of university information resources.

2. In the normal course of their duties, system administrators may examine user activities, files, electronic mail, and printer listings to gather sufficient information to diagnose and correct problems with system software or hardware.

   2.1 In order to protect against hardware and software failures, backups of all data stored on SO information resources may be made. System administrators have the right to examine the contents of these backups to gather sufficient information to diagnose and correct problems with system software or hardware. It is the user's responsibility to find out retention policies for any data of concern.

   2.2 The organization unit head may designate certain individuals or functional areas that may monitor user activities and/or examine data solely to determine if unauthorized access to a system or data is occurring or has occurred. If files are examined, the file owner will be informed as soon as practical, subject to delay in the case of an on-going investigation.

2.3 Files owned by individual users are to be considered as private to the degree noted herein, whether or not they are accessible by other users. The ability to read a file does not imply authorization to read the file exclusive of the standards set forth in this standard. Under no circumstances may a user alter a file that does not belong to him or her without prior consent of the file's owner. The ability to alter a file does not imply consent to alter that file.

2.4 Some individually owned files are by definition open access. Examples include Unix plan files, Web files made available through a system-wide facility and files made available on an anonymous ftp server. Any authorized user that can access these files may assume consent has been given.

3. If access to information is desired without the consent and/or knowledge of the file owner or if inappropriate use of SO information resources is suspected, files may be reviewed without the consent and/or knowledge of the file owner if that review is part of the process of Rule 32.01.99.S1, Complaint Procedures for Electronic Information.

4. If data or files are needed by a SO organizational unit to continue to conduct normal SO business and the file owner is unable to provide access to the data/files, the data/files may be accessed by unit personnel with the documented consent of the organizational unit head. The file owner is to be notified of such access as soon as practical, subject to delay in the case of an on-going investigation.

5. If criminal activity is suspected, the UPD or other appropriate law enforcement agency must be notified. All further access to information on university information resources must be in accordance with directives from law enforcement agencies.

6. Information resource owners or custodians will provide access to information requested by auditors in the performance of their jobs. Notification to file owners will be as directed by the auditors.

7. Other than exceptions in 2, 3, 4, 5, and 6, access to information by someone other than the file owner requires the owner’s explicit, advance consent.

8. Unless otherwise provided for, individuals whose relationship with the System Office is terminated (e.g., student graduates; employee takes new job; visitors depart) are considered to cede ownership to the information resource custodian. Custodians should determine what information is to be retained and delete all other.

9. The SO collects and processes many different types of information from third parties. Much of this information is confidential and shall be protected in accordance with all applicable laws and regulations (e.g., Gramm-Leach-Bliley Act, Texas Administrative Code 202).

10. Individuals who have special access to information because of their position have the absolute responsibility to not take advantage of that access. If information is

inadvertently gained (e.g., seeing a copy of a test or homework) that could provide personal benefit, the individual has the responsibility to notify both the owner of the data and the organizational unit head.

11. SO web sites available to the general public shall contain a Privacy Statement.

Users of SO information resources shall report any compromise of security which could lead to divulging confidential information including, but not limited to, posting social security numbers to the internet.

Related Statutes, Policies, or Requirements

Supplements: *SO Rule 29.01.99.S1*

Contact Office

For interpretation or clarification, contact The Texas A&M University System Chief Information Officer.

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