29.01.03.H0.18 Privacy

Approved: April, 2014
Next Scheduled Review: April, 2019

Procedure Statement

Privacy policies are mechanisms used to establish the responsibilities and limits for system administrators and users in providing privacy in university information resources. The University has the right to examine information on information resources which are under the control or custody of the University. 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.

Reason for Regulation

- Required by Texas Administrative Code Section 202
- This Standard Administrative Procedure (SAP) applies to University information resources that store or process mission critical and/or confidential information.
- The purpose of the implementation of this SAP is to provide a set of measures that will mitigate information security risks associated with privacy issues. There may also be other or additional measures that will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the information resource owner or their designee. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this SAP based on information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated Information Security Officer (ISO).
- The intended audience for this standard administrative procedure includes, but is not limited to, all information resources data/owners, users, management personnel, students and system administrators.

Procedures and Responsibilities

1. Privacy of information shall be provided to users of university 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 university 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, whether or not they are accessible by other users. The ability to read a file does not imply consent to read that file. 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 Texas A&M University-Texarkana information resources is suspected, files may be reviewed without the consent and/or knowledge of the file owner.

4. If criminal activity is suspected, the University Police Department 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.

5. 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.

6. Unless otherwise provided for, individuals whose relationship with the University 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.

7. The University 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).

8. 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.

9. Users of Texas A&M University-Texarkana information resources shall call the Information Technology Helpdesk to 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

- Texas Administrative Code Section 202

Definitions

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.

Owner of an Information Resource: an entity responsible for a business function and for determining controls and access to information resources supporting that business function.

Information Security Officer (ISO): responsible for administering the information security functions within Texas A&M University-Texarkana and reports to the Information Resources Manager (IRM).

Mission Critical Information: information that is defined by the University or information resource owner to be essential to the continued performance of the mission of the University or department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations, or closure of the University or department.

Protected information: shall be defined as data that has been designated as private, protected, or confidential by law or by the University. Protected information includes, but is not limited to, employment records, medical records, student records, education records, personal financial

records (or other individually identifiable information), research data, trade secrets, and classified government information.

Protected information shall not include public records that by law must be made available to the general public. To the extent there is any uncertainty as to whether any data constitutes protected information, the data in question shall be treated as protected information until a determination is made by the University.

Contact Office

Contact Office: Department of Information Technology, 903-223-3084