West Texas A&M UNIVERSITY™

The Division of Information Technology
University Information Security Standards

Information Security Standard – Privacy (Legacy TAC 202)
Approved: April 15, 2005
Last Revised: July 26, 2017
Next Scheduled Review: August 2018

1. General

Privacy policies are mechanisms used to establish the limits and expectations for the users of University information resources. The general right to privacy is extended to the electronic environment to the extent possible**.** Privacy is mitigated by the Texas Public Information Act, administrative review, computer system administration, and audits. Contents of electronic files will be examined or disclosed only when authorized by their owners, approved by an appropriate University official, or required by law.

2. Applicability

This information security standard applies to electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of the University.

The purpose of this information security standard 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 department heads or deans will provide to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures is to be determined by the department heads and their identified information security administrators. 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 is based on documented information security risk management decisions and business functions. Such risk management decisions must be documented and approved by the designated Information Security Officer (ISO).

3. Definitions

3.1 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 Information Resources Manager (IRM): Responsible to the State of Texas for management of the agency/university's information resources. The designation of an agency/university information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state agency's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the agency. If an agency does not designate an IRM, the title defaults to the agency's Executive Director, and the Executive Director is responsible for adhering to the duties and requirements of an IRM.

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.

3.4 User: An individual or automated application or process that is authorized to the resource by the owner, in accordance with the owner's procedures and rules.

4. Procedures

4.1 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.

4.2 Electronic files created, sent, received, or stored on university owned, leased, administered, or otherwise under the custody and control of West Texas A&M University are not private and may be accessed by authorized West Texas A&M information technology employees at any time without knowledge of the information resource owner or owner.

4.3 To manage systems and enforce security, West Texas A&M University may log, review, and otherwise utilize any information stored on or passing through its information systems in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Security Standards. For these same purposes, West Texas A&M University may also capture user activity such as telephone numbers dialed and web sites visited. 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.

4.4 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, hardware, or performance. It is the user's responsibility to find out retention policies for any data of concern.

4.5 A wide variety of third parties have entrusted their information to West Texas A&M University for business purposes, and all workers at West Texas A&M University must do their best to safeguard the privacy and security of this information. The most important of these third parties is the individual customer; customer account data is accordingly confidential and access will be strictly limited based on business need for access.

4.6 The organization 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.

4.7 To manage the efficient operation of information systems, appropriate security practices, and issues relating to inappropriate or illegal use of information resources, the University may log, review, and otherwise utilize any information stored on, or passing through, its information resource systems. All such actions shall be in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Security Standards, and other applicable rules and laws.

4.8 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.

4.9 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.

4.10 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.

4.11 Unless otherwise provided for, individuals whose relationship with the university is terminated (e.g. student graduates, employee takes new job; termination; 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.

4.12 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 206).

4.13 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.

4.14 Users of West Texas A&M University 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 and credit card numbers to the Internet.

4.15 Users shall not attempt to access any University data or systems that they do not have authorization or explicit consent from the owner or appropriate University employee to access.

4.16 University websites available to the general public shall contain a Privacy Statement.

OFFICE OF RESPONSIBILITY: Information Technology

CONTACT: Chief Information Officer