The Division of Information Technology
University Information Security Standards

Information Security Standard - Acceptable Use
Approved: April 15, 2005
Last Revised: July 23, 2017
Next Scheduled Review: August 2021

1. General

Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources, thus this procedure is established to:

1.1 Ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources;

1.2 Establish prudent and acceptable practices regarding the use of information resources; and,

1.3 Educate individuals who may use information resources with respect to their responsibilities associated with such use.

2. Applicability

This security standard applies to all University information resources. The purpose of the implementation of this security standard is to provide a set of measures that will mitigate information security risks associated with acceptable use of University information resources. There may also be other or additional measures that department heads or deans will provide to further mitigate risks The intended audience for this security standard includes, but is not limited to, all information resources owners, system administrators, and users of University information resources.

3. Definitions

3.1 Confidential Information: information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g., the Texas Public Information Act.

3.2 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.

3.3 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.

3.4 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.

3.5 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.

3.6 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.

4. Ownership of Electronic Files

Electronic files created, sent, received, and/or stored on information resources owned, leased administered, or otherwise under the custody and control of West Texas A&M University are the property of West Texas A&M University.

5. Privacy

Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of West Texas A&M University are not private and may be accessed by West Texas A&M University IT employees at any time without knowledge of the information resources user or owner. Electronic file content may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the **Texas Administrative Code 202**, Information Resource Standards.

5. Procedures

5.1 Users must report any weaknesses in West Texas A&M University's computer security, any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the appropriate management.

5.2 Users must not attempt to access any data or programs contained on West Texas A&M University's systems for which they do not have authorization or explicit consent.

5.3 Users must not attempt to access any data or programs contained on West Texas A&M University's systems for which they do not have authorization or explicit consent.

5.4 Users must not share their West Texas A&M University account(s), password(s), personal identification numbers (PIN), Buffalo Goldcard numbers, security tokens, or similar information or devices used for identification and authorization purposes.

5.5 Users must not make unauthorized copies of copyrighted software.

5.6 Users must not use non-standard shareware or freeware software without West Texas A&M University information resources management approval unless it is on the West Texas A&M University standard software list, available in the ITSC.

5.7 Users must not purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of information resources; deprive

an authorized West Texas A&M University user access to a West Texas A&M University resource; obtain extra resources beyond those allocated; circumvent West Texas A&M University computer security measures.

5.8 Users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, West Texas A&M University users must not run password cracking programs, packet sniffers, or port scanners or any other non-approved programs on West Texas A&M University information resources.

5.9 West Texas A&M University information resources must not be used for personal benefit/gain.

5.8 Users must not intentionally access, create, store or transmit material which West Texas A&M University may deem to be offensive, indecent or obscene (other than in the course of academic research where this aspect of the research has the explicit approval of the West Texas A&M University official process for dealing with academic ethical issues).

5.9 Access to the network and the Internet from a West Texas A&M University owned computer must adhere to all the same policies that apply to use from within West Texas A&M University facilities. Employees must not allow family members or other non-employees to access West Texas A&M University computer systems.

6. Incidental Use

As a convenience to the West Texas A&M University user community, incidental use of information resources is permitted. The following restrictions apply:

6.1 Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, and so on, is restricted to West Texas A&M University approved users; it does not extend to family members or other acquaintances.

6.2 Incidental use must not result in direct costs to West Texas A&M University.

6.3 Incidental use must not interfere with the normal performance of an employee's work duties.

6.4 No files or documents may be sent or received that may cause legal action against, or embarrassment to West Texas A&M University.

6.5 Storage of personal email messages, voice messages, files and documents within West Texas A&M University's information resources must be nominal.

6.6 All messages, files and documents - including personal messages, files and documents - located on West Texas A&M University information resources are owned by West Texas A&M University and may be subject to open records requests in accordance with this policy.

7. Disciplinary Actions

Violation of this policy may result in disciplinary action, which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Students are bound to the code of student conduct. Additionally, individuals are subject to loss of West Texas A&M University information resources access privileges, civil, and criminal prosecution.

8. Supporting Information

8.1 All personnel are responsible for managing their use of information resources and are accountable for their actions relating to information resources security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management.

8.2 The use of information resources must be for officially authorized business purposes only. There is no guarantee of personal privacy or access to tools such as, but not limited to; email, web browsing, and other electronic discussion tools. The use of these electronic communications tools may be monitored to fulfill complaint or investigation requirements. Departments responsible for the custody and operation of computers (custodian departments) shall be responsible for proper authorization of information resource utilization, the establishment of effective use, and reporting of performance to management.

8.3 Any data used in an information resource must be kept confidential and secure the user. The fact that the data may be stored electronically does not change the requirement to keep the information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and secure. Furthermore, if this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted, the data must still be protected as confidential and secured.

8.4 All computer software programs, applications, source code, object code, documentation and data shall be guarded and protected as if it were state property.

8.5 Custodian departments must provide adequate access controls in order to monitor systems to protect data and programs form misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorized, and controlled.

8.6 All commercial software used on computer systems must be supported by a software license agreement that specifically describes the usage rights and restrictions of the product. Personnel must abide by all license agreements and must not illegally copy licenses software. The IRM reserves the right to remove any unlicensed software from any computer systems.

8.7 The IRM reserves the right to remove any non-business related or unauthorized software or files from any computer system or network service. Examples of non-business related software or files include, but are not limited to; games, instant messengers, pop email, IMAP email, music files, image files, freeware, shareware, or other software such as Software as a Service (SaaS) systems that reside in the cloud (such services may be blocked at the firewall to prevent data leakage).

References

Copyright Act of 1976
Foreign Corrupt Practices Act of 1977
Computer Fraud and Abuse Act of 1986
Computer Security Act of 1987
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
The State of Texas Information Act
Texas Government Code, Section 441
Texas Administrative Code, Chapter 202
IRM Act, 2054.075(b)
The State of Texas Penal Code, Chapters 33 and 33A
DIR Practices for Protecting Information Resources Assets
DIR Standards Review and Recommendations Publications
System Policy 07.01, Ethics Policy
System Policy 21.04, Control of Fraud and Fraudulent Actions;
System Policy 33.04, Use of System Property;
System Regulation 21.99.10, Use of Licensed Commercial Software

OFFICE OF RESPONSIBILITY: The Division of Information Technology

CONTACT: Chief Information Officer