29.01.03.H0.12 Internet/Intranet Use

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

Procedure Statement

Under the provisions of the Information Resources Management Act, information resources are strategic assets of Texas A&M University-Texarkana (TAMUT) that must be managed as valuable State resources. This procedure is intended to:

- ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources
- establish prudent and acceptable practices regarding the use of information resources
- educate individuals who may use information resources on their responsibilities associated with such use

Applicability
This procedure applies to all individuals granted user access privileges to TAMUT Information Resources with the capacity to access the Internet and/or Intranet.

Ownership
Electronic files created, sent, received, or stored on computers owned, leased, administered, or otherwise under the custody and control of the University are the property of TAMUT.

Privacy
Electronic files created, sent, received, or stored on Information Resources owned, leased, administered, or otherwise under the custody and control of the University, are not private and may be accessed by TAMUT Information System employees at any time without knowledge of the Information Resources user or owner in accordance with the provisions and safeguards provided in the Texas Administrative, Title 1, Part 10, Chapter 202, Information Security Standards.

Definitions

Information Resources (IR): Any computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing websites, 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, tablets, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), smartphones, telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it includes 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.

Information Resources Manager (IRM): Person responsible to the State of Texas for management of the agency's information resources. The designation of an agency information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the 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. At TAMUT, the IRM is the Associate Vice President for IT/CIO.

Information Security Officer (ISO): Person responsible to the executive management for administering the information security functions within the University. The ISO is TAMUT's internal and external point of contact for all information security matters.

Internet: A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies and colleges. The Internet is the present "information super highway."

Intranet: A private network for communications and sharing of information similar to the Internet, but accessible only to authorized users within an organization. An organization's intranet is usually protected from external access by a firewall.

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

Vendor: Someone who exchanges goods or services for money.

World Wide Web: A system of Internet hosts that supports documents formatted in HTML (HyperText Markup Language) which contains links to other documents (hyperlinks) and to audio, video, and graphic images. Users can access the Web with special applications called browsers, such as Mozilla Firefox and Microsoft Internet Explorer.

Procedures and Responsibilities

1. INTERNET AND INTRANET USAGE

1.1 Users are responsible for their account(s). Users should make appropriate use of the system and network-provided protection features and take precautions against others obtaining access to their computer resources. Individual password security is the responsibility of each user.

1.2 User accounts that are inactive for three or more months (i.e. no logins or file uploads) will be deleted as they pose a security risk and tie up valuable system resources.

1.3 Users are prohibited from using any form of electronic media (e.g. email or web pages) to harass, intimidate, or otherwise annoy another person/group.

1.4 Users must not use another user's account or password without proper authorization.

1.5 All activity may be subject to logging and review.

1.6 All authorized users of networks or systems must use the Internet/Intranet facilities in ways that do not disable, impair, or overload performance of any other computer system or network, or circumvent any system intended to protect the privacy or security of another user.

1.7 Downloading entertainment software, games, or any other non-business related software or files such as music or movies is prohibited.

1.8 Users are forbidden from using techniques designed to cause damage to access by legitimate users of computers or network components connected to the Internet.

1.9 Users are urged to report any weaknesses in TAMUT's computer security and any incidents of possible misuse or violation of this SAP to the proper authorities by contacting the Information Security Officer at itsecurity@TAMUT.edu.

1.10 All files downloaded from the Internet must be scanned for viruses using the approved INFORMATION TECHNOLOGY distributed software suite and current virus detection software.

1.11 Content on all TAMUT websites must comply with the TAMUT's 29.01.03.H0.28 Web Accessibility and Usability Procedure.

1.12 No personal or commercial advertising may be made available via TAMUT websites.

1.13 University Internet access may not be used for personal gain or personal solicitations.

1.14 No TAMUT data will be made available via TAMUT websites without ensuring that the material is available only to authorized individuals or groups.

1.15 All sensitive TAMUT material transmitted over external networks must be encrypted.

1.16 Electronic files are subject to the same records retention rules that apply to other documents and must be retained in accordance with departmental records retention schedules.

2. INCIDENTAL USE

2.1 Incidental personal use of Internet access is restricted to TAMUT approved users; it does not extend to family members or other acquaintances.

2.2 Incidental use must not result in any direct cost to TAMUT.

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

2.4 No files or documents may be sent or received that may cause legal liability for, or embarrassment to TAMUT.

2.5 Storage of personal files and documents within TAMUT's Information Resources should be nominal.

2.6 All files and documents – including personal records – stored in TAMUT's information resources are owned by TAMUT and may be subject to open records requests.

3. DISCIPLINARY ACTIONS

Violation of this procedure may result in disciplinary action which may include termination for employees, termination of business relationships for contractors or consultants, dismissal for interns and volunteers, or suspension or expulsion for students. Additionally, individuals are subject to loss of TAMUT Information Resources access privileges and civil and criminal prosecution.

Related Statutes, Policies, or Requirements

Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C, Rule § 202.75, Information Resources Security Safeguards

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 Publication

Contact Office

Information Security Officer
903-886-5425