TEXAS A&M INTERNATIONAL UNIVERSITY™

Standard Administrative Procedure

29.01.99.L1.01 Acceptable Use

Approval date: 03/28/13
Revision date: 01/24/13
Next scheduled review date: 01/24/15
Author: Office of Information Technology

Standard Administrative Procedure Statement

General

Under the provisions of the Information Resources Management Act 2054.075(b), information resources are strategic assets of Texas A&M International University (TAMIU) 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 SAP applies to all individuals granted user access privileges to TAMIU Information Resources.

Ownership of Electronic Files

Electronic files created, sent, received, or stored on Information Resources owned, leased administered, or otherwise under the custody and control of the University are the property of TAMIU.

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 TAMIU Information Systems 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 Code 202, Information Resource 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 TAMIU, the IRM is the Associate Vice President for IT/CIO.

Information Security Administrator (ISA): Person responsible for monitoring and implementing security controls and procedures for a system.

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

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

Procedures and Responsibilities

1. Information Resources Acceptable Use

1.1 Users must report any weaknesses/incidents in TAMIU's computer security of possible misuse or violation of this agreement to the IT Security group at itsecurity@tamiu.edu.

1.2 Users must not attempt to access any data or programs contained on TAMIU's systems for which they do not have authorization or explicit consent.

1.3 TAMIU accounts, passwords, or similar information or devices used for identification and authorization purposes must not be shared.

1.4 Family members or other non-employees are not allowed to access TAMIU computer systems.

1.5 Unauthorized copies or illegally distributed copyrighted software are prohibited.

1.6 Users must not use non-standard software without TAMIU Information Resources management approval.

1.7 Users must not purposely engage in activity that may: harass, threaten or abuse others, degrade the performance of Information Resources, deprive an authorized user access to a TAMIU resource, obtain extra resources beyond those allocated, or circumvent TAMIU computer security measures.

1.8 Users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, TAMIU users must not run password cracking programs, packet sniffers, or port scanners or any other non-approved programs on TAMIU Information Resources. These specific acts are a violation of TAMIU's Acceptable Use.

1.9 TAMIU Information Resources must not be used for personal benefit as per TAMIU's Ethics SAP.

1.10 Users must not intentionally access, create, store or transmit material which TAMIU may deem offensive, indecent or obscene (other than in the course of approved academic research).

1.11 Access to the Internet from a TAMIU owned portable computing device must adhere to all the same policies that apply to use from within TAMIU facilities.

1.12 Users must not otherwise engage in acts against the aims and purposes of TAMIU as specified in its governing documents or in rules, regulations and procedures that are adopted from time to time.

1.13 Any data used in an IR system must be kept confidential and secure by 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. Departments' Information Security Administrator must perform a risk assessment following the 29.01.99.L1.34 Risk Assessment Guidelines SAP. 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.

1.14 All commercial software must abide by the Authorized Software SAP and must be supported by a software license agreement that specifically describes the usage rights and restrictions of the product.

1.15 The IRM reserves the right to remove any non-business related software or files from any system. Examples of non-business related software or files include, but are not limited to, games, instant messengers, pop email, music files, image files, freeware, and shareware.

1.16 Users must follow all IT SAPs.

2. Incidental Use

As a convenience to the University user community, incidental use of Information Resources is permitted. The following restrictions apply:

2.1 Incidental personal use of electronic mail, Internet access, fax machines, printers, copiers, and so on, is restricted to University approved users; it does not extend to family members or other acquaintances.

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

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 action against, or embarrassment to TAMIU.

2.5 Storage of personal email messages, voice messages, files and documents within TAMIU's Information Resources must be nominal.

2.6 All messages, files and documents (including personal messages) located on TAMIU Information Resources are owned by TAMIU, may be subject to open records requests, and may be accessed in accordance with this SAP.

Disciplinary Actions

Violation of this SAP 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 TAMIU Information Resources access privileges as well as civil and criminal prosecution.

Related Statutes, Policies, Regulations, Rules or Requirements

TAC 202.75 Security Standards for Institutions of Higher Education

29.01.99.L1.09 Internet/Intranet Standard Administrative Procedure

Appendix

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

Contact Office

Office of Information Technology Hotline: (956) 326-2310 Killam Library 257	**Information Security Officer** Cuauhtemoc Barrios cbarrios@tamiu.edu
Office Hours Monday - Friday: 7:30 AM - 6:00 PM Saturday - Sunday: Closed	**ITSecurity Group** itsecurity@tamiu.edu