TEXAS A&M INTERNATIONAL UNIVERSITY™

Standard Administrative Procedure

29.01.00.L1.16 Information Resources Privacy

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
Privacy policies are mechanisms used to establish the responsibilities and limits for system administrators and users of Texas A&M International University (TAMIU) Information Resources.

Applicability
This SAP applies to all users and administrators of TAMIU Information Resources. TAMIU has the right to examine data on Information Resources which are under the control or custody of the University. 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.

Definitions

Custodian: Guardian or caretaker; the holder of data; the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. For server applications, Information Services is the custodian; for micro and mini applications, the owner or user may retain custodial responsibilities. The custodian is normally a provider of services.

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 Resource Owner: An entity responsible for:

1. a business function, and
2. determining controls and access to Information Resources supporting that business function.

Office of Information Technology (OIT): The name of the TAMIU department responsible for computers, networking and data management.

Web browser: A software application for retrieving, presenting, and traversing information resources on the World Wide Web. The major web browsers are Internet Explorer, Mozilla Firefox and Google Chrome.

Web page: A document on the World Wide Web. Every Web page is identified by a unique URL (Uniform Resource Locator).

Web server: A computer that delivers (*serves up*) web pages.

Web site: A location on the World Wide Web accessed by typing its address (URL) into a Web browser. A Web site always includes a home page and may contain additional documents or pages.

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, Navigator and Microsoft Internet Explorer.

Procedures and Responsibilities

This Standard Administrative Procedure applies to electronic information created, sent, received, or stored on Information Resources owned, leased, administered, or otherwise under the custody and control of TAMIU.

The information resource owner, or his or her designee, is responsible for ensuring that the risk mitigation measures described in this SAP are implemented. Based on risk management consideration and business functions, the resource owner may deem it appropriate to exclude certain risk mitigation measures provided in this SAP.

Procedures

1. Privacy of information must be provided to users of TAMIU Information Resources consistent with obligations of Texas and Federal law and/or secure operations.
2. In the normal course of their duties, custodians 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 TAMIU Information Resources may be made. Custodians 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 be aware of retention policies for any data of concern.

2.2 The organization unit head may designate certain individuals who may monitor user activities and/or examine data solely to determine if unauthorized access to a system or data is occurring or has occurred.

2.3 Files owned by individual users are to be considered private to the degree noted herein, whether or not they are accessible by other users. The ability to read a file does not imply authorization to read or alter the file. Under no circumstances may a user alter a file that does not belong to him or her, unless given consent by the file's owner.

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 who can access these files may assume consent has been given.

3. If data or files are needed by a TAMIU organizational unit to continue to conduct normal University business and the file owner is unable to provide access to the data/files, the data/files may be accessed by unit personnel with the documented consent of the organizational unit head. The file owner is to be notified of such access as a soon as possible.
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 TAMIU 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) on the performance of their jobs. Notification to file owners will be sent as directed by the auditors.
6. Unless otherwise provided for, individuals whose relationship with TAMIU is terminated (i.e. student graduates, employees taking a new job, visitors departing) are considered to cede ownership to the information resource custodian. Custodians should determine what information needs to be retained and must delete all other unnecessary data.
7. TAMIU collects and processes many different types of information from third parties. Much of this information is confidential and must 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 of not abusing 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. TAMIU websites available to the general public must contain a Privacy Statement such as the one found at Texas A&M International University Privacy Statement.
10. Users of TAMIU Information Resources are urged to contact OIT at itsecurity@tamiu.edu 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, grades, DOBs, etc.

Related Statutes, Policies, Regulations, Rules or Requirements

TAC 202.75 Security Standards for Institutions of Higher Education

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