

TEXAS A&M
INTERNATIONAL
UNIVERSITY™
Standard Administrative Procedure

29.01.99.L1.15 Portable Computing
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

Portable computing devices are becoming increasingly powerful and affordable. Their small size and functionality are making these devices ever more desirable to replace traditional desktop devices in a wide number of applications. However, the portability offered by these devices may increase the security exposure to groups using the devices.

Applicability

The purpose of this SAP is to establish the rules for the use of mobile computing devices and their connection to the network. These procedures are necessary to preserve the integrity, availability and confidentiality of Texas A&M International University (TAMIU) information. This SAP applies to all individuals who utilize portable computing devices and access TAMIU Information Resources.

Definitions

External storage media: Portable devices that are not permanently fixed inside a computer and are used to store data. These include, but are not limited to, USB thumb drives, CDs, DVDs, external hard drives, memory cards, etc.

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.

Portable Computing Devices: Any easily portable device that is capable of receiving and/or transmitting data to and from IR. These include, but are not limited to, notebook computers, handheld computers and cell phones.

Procedures and Responsibilities

TAMIU has seen a significant increase in the use of portable computing devices such as laptops, tablets, Smartphones and external storage media. This SAP is intended to provide guidelines for utilizing portable computing devices.

Security Guidelines

Portable computing devices are inherently at risk for theft and security vulnerability. In cases where there is a justifiable business need or requirement for confidential information such as confidential student information, grades, etc., to be stored or transferred to a portable computing device, appropriate security measures must be implemented as listed below.

- 1.1 Confidential information must not be stored, downloaded, or taken off the University grounds unless there is a need to access this information away from TAMIU. Authorization will need to be provided by the information owner.
- 1.2 Confidential information must not be shared with others who do not have a job-related need for this information.
- 1.3 Departments possessing portable computing devices with access to sensitive information must have all physical storage devices encrypted as stated in TAMIU's 29.01.99.L1.25 Encryption SAP.
- 1.4 No personal computers may be connected to TAMIU's wired network without prior review and consent of OIT.
- 1.5 The portable computing device must be password-protected using the security feature provided on the tool, and there should be no sharing of the password.
- 1.6 Whenever there is no longer a job related need to access or store this confidential information, it must be deleted.
- 1.7 TAMIU data must not be transmitted via wireless network to or from a portable computing device unless approved wireless transmission protocols along with approved encryption techniques are utilized.
- 1.8 Unattended portable computing devices must be physically secured. This means they must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.

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 and civil and criminal prosecution.

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