29.01.03.H0.17 Portable Computing

Approved: April, 2014
Revised: January 5, 2024
Next Scheduled Review: January 2029

Procedure Summary

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.

The purpose of this procedure 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 University-Texarkana (TAMUT) information. This procedure applies to all individuals who utilize portable computing devices and access TAMUT 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 TAMUT, the IRM is the CIO.

Portable Computing Devices (PCD): 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, tablets, and cell phones.

Procedures and Responsibilities

TAMUT has seen a significant increase in the use of portable computing devices such as laptops, tablets, Smartphones, and external storage media. This procedure is intended to provide guidelines for utilizing portable computing devices. The ISO will provide guidance and direction in the following areas:

1. 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 TAMUT. Authorization will need to be provided by the information owner.

1.2 Confidential information must not be shared with unauthorized parties.

1.3 Departments possessing PCD's with access to sensitive information must have all physical storage devices encrypted as stated in University Procedure 29.01.03.H0.08 *Encryption*.

1.4 No personal computers may be connected to TAMUT's wired production network without prior review and consent of the Office of Information Technology (OIT). Connecting to the wired network in the Bringle Lake Village residence hall and the E-Sports facilities in the University Center are the only.

1.5 The PCD must be password-protected using the security feature provided on the tool (most commonly a PIN or Passcode such as on an iPad), 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, the access must be removed.

1.7 Confidential, or protected, information must not be transmitted to or from a PCD unless using approved wireless transmission protocols , in addition to approved encryption techniques (i.e., VPN).

1.8 University Procedure 15.02.99.H1, *Export Control* rules must be adhered to when PCDs are identified as an export.

1.9 All users of assigned PCD(s) in any format are accountable for ensuring the safety of the assigned portable computing device and any data utilized, to prevent theft, loss, or damage. The following guidelines should be adhered to when transporting and using a portable computing device or data outside of TAMUT office space:

- When a PCD or data is not in the direct possession of the user, it must be securely stored in a locked location (e.g., desk, file cabinet, safe).
- The PCD or data should not be left unattended in a vehicle unless it is properly secured in the trunk or another fully lockable compartment within the vehicle. Such storage must be temporary and not overnight.
- When the user is traveling, either for official or personal purposes, if an issued PCD must accompany the individual, it must either remain on their person or within their carry-on luggage. The PCD should never be placed in checked baggage.

1.10 Lost or stolen PCD(s) must be reported immediately to the Office of Information Technology.

2. 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
University Procedure 29.01.03.H0.08 *Encryption*.
University Procedure 15.02.99.H1, *Export Control*
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)
Texas Administrative Code, Chapter 202
IRM Act, 2054.075(b)
The State of Texas Penal Code, Chapters 33 and 33A

Contact Office

Office of Information Technology
903-334-6603