The Division of Information Technology
University Information Security Standards

Information Security Standard – Portable Computing (Legacy TAC 202)
Approved: April 15, 2005
Last Revised: July 26, 2017
Next Scheduled Review: August 2018

1. General

Portable computing devices are becoming increasingly powerful and affordable. Their small size and functionality are making these devices 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 individuals using the devices.

2. Applicability

This information security standard applies to all portable information resource devices that process, contain, or have direct access to mission critical and/or confidential information.

The purpose of this information security standard is to provide a set of measures that will mitigate information security risks associated with portable computing. There may also be other or additional measures that department heads or deans will provide to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures is to be determined by the department heads and their identified information security administrators.   In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided is based on documented information security risk management decisions and business functions. Such risk management decisions must be documented and approved by the designated Information Security Officer (ISO).

The intended audience is all users of University information resources.

3. Definitions

> 3.1   Confidential Information: information that is excepted from

disclosure requirements under the provisions of applicable state or federal law, e.g., the Texas Public Information Act.

3.2   Information Resources: Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, 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, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is 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.

3.3   Information Resources Manager (IRM): Responsible to the State of Texas for management of the agency/university's information resources. The designation of an agency/university information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state 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. If an agency does not designate an IRM, the title defaults to the agency's Executive Director, and the Executive Director is responsible for adhering to the duties and requirements of an IRM.

3.4   Information Security Officer (ISO): Responsible to the executive management for administering the information security function within the agency. The ISO is the university's internal and external point of contact for all information security matters.

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

3.6   Internet Service Provider (ISP): a company that provides access to the internet.

3.7   Portable Computing Device: Any easily portable device that is capable of receiving, transmitting, and/or storing data, and that can connect by cable,

telephone wire, wireless transmission or via any Internet connection to the West Texas A&M University infrastructure and/or data systems. These include, but are not limited to, notebook computers, handheld computers, PDA's, pagers, cellphones, and portable storage devices (such as flash drives, memory cards, USB-connected storage devices, etc).

4. Procedures

4.1 Where possible and/or appropriate, portable computing devices shall be protected from unauthorized access by passwords or other means.

4.2 Whenever possible, sensitive or confidential West Texas A&M University data should not be stored on portable computing devices. However, in the event that there is no alternative to local storage, such data must be encrypted using university-approved encryption techniques. Contact the Information Technology Service Center or the Information Security Officer @ 806-651-4357 for assistance with encryption.

4.3 Sensitive or confidential information must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols and encryption techniques are utilized.

4.4 Remote access to West Texas A&M University systems must utilize approved encryption techniques when transmitting or receiving sensitive or confidential information.

4.5 Unattended portable computing devices shall be kept physically secure using means appropriate to the potential risk associated with the device. This may include storing the device in a locked office, desk drawer, or filing cabinet, or attaching the device to a desk or chair via a cable lock systems.

4.6 All portable devices, such as laptops, must utilize current anti-virus software, such as Trend Micro or Symantec, especially when connected to a network outside of the West Texas A&M University infrastructure.

4.7 Device and information resource owners will ensure that any portable computing device within their area of responsibility is being managed and used in accordance with all applicable university acceptable use policies.

OFFICE OF RESPONSIBILITY: Information Technology
CONTACT: Chief Information Officer