The Division of Information Technology
University Information Security Standards

Information Security Standard – Encryption (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 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 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 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.

3.4 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.

3.5 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.).

3.6 Encryption: The conversion of plaintext information into a code or cipher-text using a variable, called a "key" and processing those items through a fixed algorithm to create the encrypted text that conceals the data's original meaning.

4. Procedures

4.1 All encryption mechanisms implemented to comply with this procedure must support a minimum of, but not limited to, AES 256-bit encryption. The use of proprietary encryption algorithms is not permitted for any purpose unless reviewed and approved by the Information Security Officer.

4.2 Recovery of encryption keys will be part of business continuity planning where applicable and appropriate, except for data used by a single individual.

4.3 Sensitive or confidential data university data must not be stored on portable

computing devices. However, in the event that there is no alternative, such data must be encrypted using university-approved encryption techniques. Contact the Information Technology Service Center @ 806-651-4357 for assistance with encryption procedures.

4.4 Sensitive or confidential university information must not be transmitted via wireless, including Bluetooth, to or from a portable computing device unless approved wireless transmission protocols and encryption techniques are utilized. Contact the Information Technology Service Center @ 806-651-4357 for assistance with this procedure.

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

4.6 Any confidential or sensitive university data transmitted to or from a site not on the campus network (e.g., to and from vendors, customers, or entities doing business with the university) must be encrypted or be transmitted through an encrypted tunnel that is encrypted with virtual private networks (VPN) or secure socket layers (SSL).

4.7 Before confidential or university-sensitive data is transferred to a third party, that third party must affirm that they will protect the transferred data in accordance with the conditions imposed by the data's Owner, which conditions will contain, at a minimum, the conditions specified in this procedure. Confidential information must be encrypted if copied to, or stored on, a portable computing device, removable media, or a non-agency owned computing device.

OFFICE OF RESPONSIBILITY: Information Technology

CONTACT: Chief Information Officer