Information Security for Portable Devices

Original Implementation: October 18, 2011
Last Revision: April 24, 2018

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this policy are implemented. All Users are responsible for safeguarding university data.

Definitions:

Confidential Information – Information that is protected from disclosure requirements under the provisions of applicable state or federal law, e.g., Family Educational Rights and Privacy Act (FERPA), The Texas Public Information Act.

Information Resources (IR) - The procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

Information Resource Owner– an entity responsible for:

- a business function; and,
- determining controls and access to information resources supporting that business function.

Portable Computing Device –Any portable device that is capable of capturing, processing, storing, and transmitting data to and from the SFA information resources.

Portable Storage Device –Any portable device that stores electronic data.

Remote Access – The act of using a computing device to access another computer/network from outside of its established security realm (e.g, authentication mechanism, firewall, or encryption).

Risk Mitigation Measures:

- Portable computing devices, containing confidential information will be protected from unauthorized access by passwords or other means.
- Any confidential information stored on portable computing or storage devices will be encrypted with an appropriate encryption technique.
- All remote access to confidential information from a portable computing device will utilize encryption techniques, such as virtual private network (VPN), secure file transfer protocol (SFTP), or secure sockets layer (SSL).

- Confidential information will not be transmitted via wireless connection to, or from, a portable computing device unless encryption methods that appropriately secure wireless transmissions, such as virtual private network (VPN), encrypted Wi-Fi, or other secure encryption protocols are utilized.
- Unattended portable computing or storage devices, containing confidential information, will be kept physically secure using means appropriately commensurate with the associated risk.
- Where appropriate, keep portable computing devices patched/updated, and install anti-virus software and a personal firewall.

Cross Reference: Family Educational Rights and Privacy Act of 1974 (FERPA), 20 U.S.C. § 1232g; Tex. Gov't Code Ch. 552; 1 Tex. Admin. Code §§ 202.1-.2, .70-.76; Information Security Management (14.1)

Responsible for Implementation: Vice President for University Affairs

Contact for Revision: Information Security Officer

Forms: None

Board Committee Assignment: Academic and Student Affairs