Information Technology Services
Portable Computing Standard

Approved: February 11, 2020

Standard Statement

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

Reason for Standard

The purpose of the Tarleton State University portable computing security standard is to provide guidance on the responsibilities of information resource owners to protect data residing on portable devices. The information resource owner, or designee(s), is responsible for ensuring that the risk mitigation measures described in this internal standard are implemented. The resource owner may determine whether it would be appropriate to exclude certain risk mitigation measures provided below based on risk management considerations and business functions. The resource owner is responsible for documenting any exceptions to this standard and making it available upon request. This standard applies to the use of all portable information resources devices that process, contain or have direct access to confidential information. This standard will apply equally to all individuals who utilize portable computing devices and access Tarleton information resources.

Standards and Responsibilities

1. Whenever possible, portable computing devices must be password protected.

2. Whenever possible, sensitive or confidential Tarleton data should not be stored on portable computing devices or portable storage devices. However, in the event that there is no alternative to local storage, such data must be encrypted using university-approved encryption techniques.

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. All remote access (e.g. cable/DSL modem, dial in services, etc.) to confidential information from a portable computing device shall utilize encryption techniques, such as Virtual Private Network (VPN), Secure Socket Layers (SSL) or secure File Transfer Protocol (SFTP)

5. Unattended portable computing devices shall be kept physically secure using means appropriate to the potential risk associated with the device. Keep portable computing devices patched and updated. Install anti-virus software and a personal firewall where applicable.

6. Information resource owners will ensure that any portable computing device within their area of responsibility is being managed and used in accordance with applicable university acceptable use procedure.

Definitions

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 or Family Educational Right to Privacy Act).

Information resources: The standards, equipment and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display and transmit information or data.

Portable computing devices: 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 Tarleton infrastructure and/or data systems. These include, but are not limited to, notebook computers, handheld computers, PDAs, pagers, and smartphones.

Portable Storage Device: An easily portable device that stores electronic data which includes but is not limited to flash drives, memory cards, DVDs, CDs, iPods, USB connected storage devices, etc..

Information Resource Owner: an entity responsible for a business function and/or that determines controls and access to information resources supporting business functions.

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

Contact Office

Information Technology Services
CIO of Information Technology Services
254.968.9395