Texas A&M University System Standard – Portable Devices

Standard Statement

This standard provides specific guidance on the responsibilities of information resource owners to adequately protect data residing on portable devices.

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. Refer to System Regulation 29.01.03 and the related Data Classification Standard for more information.

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.

Internet Service Provider (ISP) - A company that provides access to the internet.

Portable Computing Device - An easily portable device that is capable of capturing, processing, storing, and transmitting data to and from TAMUS information resources. This includes, but is not limited to: laptops, notebooks, Personal Digital Assistants (PDAs), tablets and smart phones.

Portable Storage Device - An easily portable device that stores electronic data. This includes, but is not limited to: flash/thumb drives, iPods, CD-Rs/CD-RWs, DVDs, and removable disk drives.

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).

Information Resource Owner - an entity responsible for:

- A business function; and,
- Determining controls and access to information resources supporting that business function.

Responsibilities and Standards

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 computing and storage devices that utilize information resources, especially those which process, store, or transmit confidential information.

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this standard are implemented. Based on risk management considerations and business functions, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures provided in this standard. All exclusions must be in accordance with standard *Exclusions from Required Risk Mitigation Measures*.

The intended audience is all users of System Office (SO) information resources.

3. STANDARDS

3.1 Portable computing and storage devices, containing confidential information, shall be protected from unauthorized access by passwords or other means.

3.2 Any confidential information stored on portable computing or storage device shall be encrypted with an appropriate encryption technique. Please see TAMU's Encryption Web page for additional information.

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

3.4 Confidential information shall 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), Wi-Fi Protected Access (WPA) or other secure encryption protocols are utilized.

3.5 Unattended portable computing or storage devices, containing confidential information, shall be kept physically secure using means appropriately commensurate with the associated risk.

3.6 Where appropriate, keep portable computing devices patched/updated, and install anti-virus software and a personal firewall.

Contact Office

Contact The Texas A&M University System Chief Information Officer for standard interpretation and clarification.

OFFICE OF RESPONSIBILITY: The Texas A&M University System Chief Information Officer