29.01.03.R0.01 Information Security Standards Portable Computing

Approved June 2, 2010
Revised December 19, 2011
Next Schedule Review December 19, 2016

Procedure Statement

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.

Reason for Procedure

This procedure provides guidance and security standards for the use of portable computing devices.

Procedures and Responsibilities

1. APPLICABILITY

This procedure 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 procedure is to provide a set of measures that will mitigate information security risks associated with portable computing. The intended audience is all users of university information resources.

2. 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.

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.

3. PROCEDURES

3.1 Portable computing devices shall be protected from unauthorized access by passwords or other means, where appropriate.

3.2 No sensitive or confidential university data should be stored on portable computing devices without prior approval of the Chief Information Officer. All sensitive or confidential university data stored on portable computing devices shall be encrypted. Information Technology will maintain a list of suitable encryption mechanisms.

3.3 All remote access (VPN, Remote Desktop, etc.) to the university shall utilize encryption techniques when connecting from an Internet Service Provider (ISP).

3.4 University data or information shall not be transmitted via wireless connection to, or from, a portable computing device unless encryption methods that appropriately secure wireless transmissions are utilized (i.e., secured socket layer (SSL) or Remote Desktop Protocol over SSL/TLS).

Related Statutes, Policies, or Requirements

System Policy *29.01 Information Security Standards*

System Regulation *29.01.03 Information Security*

University Procedure *29.01.03.R0.02 Electronic Information Security*

Contact Office

Information Technology, Information Security Officer
903-886-5425