Information Resources - Portable Devices: Information Security

Approved January 20, 2004
Revised November 21, 2006
Revised July 10, 2007
Revised September 17, 2009
Revised June 5, 2013
Next Scheduled Review: June 5, 2016

Supplements TEES Rule 29.01.99.E1

Standard Administrative Procedure Statement
The scope of this procedure is to minimize the security exposure with the transport of portable computing and storage devices.

Reason for Standard Administrative Procedure
The purpose of this portable computing procedure is to provide guidance on the responsibilities of information resource owners to adequately protect data residing on portable devices.

Procedures and Responsibilities

1. CONTROLS AND RESPONSIBILITIES

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

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

1.3 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).

1.4 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.
1.5 Unattended portable computing or storage devices, containing confidential information, shall be kept physically secure using means appropriately commensurate with the associated risk.

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

Related Statutes, Policies, or Requirements

Encryption Web page


TEES Rule 29.01.99.E1, Security of Electronic Information Resources

Contact Office

Information Technology Services
(979) 847-8585