

**PRAIRIE VIEW A&M UNIVERSITY
UNIVERSITY ADMINISTRATIVE PROCEDURE**

29.01.03.P0.16 Information Resources – Portable Computing

Approved (May 26, 2009)

Revised (August 25, 2011)

Next Scheduled Review (August 2012)

1. PURPOSE

- 1.1 This University Administrative Procedure (UAP) provides specific guidance on the responsibilities of information resource owners to adequately protect data residing on portable devices. 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.
- 1.2 This UAP applies to all portable computing and storage devices that utilize information resources, especially those which process, store, or transmit confidential information. The purpose of this procedure is to have a set of measures that will mitigate information security risks associated with portable computing.

2. DEFINITIONS

- 2.1 **Confidential Information** - Information that is exempted from disclosure requirements under the provisions of applicable state or federal law, e.g., the Texas Public Information Act.
- 2.2 **Sensitive Personal Information** – An individual's first name or first initial and last name in combination with any one or more of the following items:
 - 2.2.1 Social Security Number;
 - 2.2.2 Driver's license number or government-issued identification number (including UIN or Student ID);
 - 2.2.3 Account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account.
- 2.3 **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.
- 2.4 **Owner of an Information Resource** - a person responsible for a business function; and for determining controls and access to information resources supporting that business function.
- 2.5 **Encryption (encrypts, encipher, or encode)** - the conversion of plain text information into a code or cipher-text using a variable, called a "key" and

processing those items through a fixed algorithm to create the encrypted text that conceals the data's original meaning.

- 2.6 **Internet Service Provider (ISP)** - A company that provides access to the internet.
- 2.7 **Portable Computing Device** - An easily portable device that is capable of capturing, processing, storing, and transmitting data to and from PVAMU information resources. This includes, but is not limited to laptops, personal digital assistants (PDAs), and iPads.
- 2.8 **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.
- 2.9 **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).

3. PROCEDURES AND RESPONSIBILITIES

- 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 or sensitive personal information stored on portable computing or storage device shall be encrypted with an appropriate encryption technique (See UAP 29.01.03.P0.22 – Encryption of Confidential and Sensitive Information). It is highly recommended that no confidential or sensitive personal information be stored on any portable computing or storage device but to a PVAMU network share for which this data can be accessed through VPN if required.
- 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 and sensitive personal 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 The purchase of all portable devices not listed on the University Standard Specifications will require a business plan supporting the purchase to be submitted and approved by the Information Resources Manager, the Chief Information Officer, and the Information Security Officer. A business plan form is located in the University policy library (*insert web address*) under Information Resources.
- 3.6 The University will not purchase data plans. However, an employee who has purchased a data plan may submit a request for a communication allowance.

- 3.7 All portable storage devices are required to be ordered with encryption if the device supports it, and it is available for the device.
- 3.8 Unattended portable computing or storage devices, containing confidential information, shall be kept physically secure using means appropriately commensurate with the associated risk.
- 3.9 Where appropriate, keep portable computing devices patched/updated, and install anti-virus software and a personal firewall.
- 3.10 All portable storage devices are required to be registered in the University Fixed Asset System.
- 3.11 University Information Technology Services does not support cellular phones and devices on the University's network to the extent of repairing them or diagnosing problems. Authorized phones will get network support and they are subject to open records requests.

Contact Office; Information Security Officer: 936/261-2126