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
Revised July, 1, 2015
Revised March 28, 2018
Next Scheduled Review: March 2023

UAP Purpose

This purpose of this University Administrative Procedure (UAP) is to provide specific guidance on the responsibilities of information resource owners to adequately protect data residing on portable devices. In addition, the performance of these procedures is necessary to ensure compliance with the Texas Administrative Code 202.75 Information Resources Security Safeguards.

Definitions

Confidential Information - information that is confidential pursuant to state or federal law. Such information may also be subject to state or federal breach notification requirements. (TAMUS Data Classification Standard).

Information Security Breach Notification Matrix – advises readers of their responsibilities in notifying the correct personnel in the event of a breach of information. (TAMUS Notification Matrix).

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.

Information Resources Manager (IRM) – person responsible to the State of Texas for management of the University's information resources. The designation of an IRM is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the University's information activities, and ensure greater visibility of such activities within the University. The IRM has been given the authority and the accountability by the State of Texas to implement security policies, procedures, practice standards, and guidelines to protect the information resources of the University. If an IRM is not designated, the title defaults to the University's executive director who then will be responsible for adhering to the duties and requirements of an IRM.

Information Resource Owner - an entity responsible for a business function and for determining controls and access to information resources supporting that business function.

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.

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 Prairie View A&M University (PVAMU) information resources. This includes, but is not limited to: laptops, personal digital assistants (PDAs), and IPads.

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).

Official Procedures and Responsibilities

---

1. GENERAL

1.1 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 There may be additional measures that department heads or deans will implement to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the department heads and their identified information security administrators. In accordance with Texas Administrative Code 202.75 Information Resources Security Safeguards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this UAP based on documented information security risk management decisions and business functions. Such risk management decisions must be documented and approved by the designated Information Security Officer (ISO).

2. APPLICABILITY

2.1 This UAP applies to all portable computing and storage devices that utilize information resources, especially those that process, store, or transmit confidential information. The intended audience for this UAP includes, but is not limited to, all information resources management personnel, owners, system administrators, and users of University information resources.

3. PROCEDURES

3.1 Portable computing shall be protected from unauthorized access by passwords and encryption.

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 or

University approved storage alternative for which the 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 List will require the submission of a completed Business Plan supporting the purchase to be approved by the IRM, the Chief Information Officer, and the ISO.

3.6 All portable storage devices are required to be ordered with encryption if the device supports it, and it is available for the device.

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

3.8 Keep portable computing devices patched/updated, and install anti-virus software and a personal firewall where possible.

3.9 All portable storage devices are required to be registered in the University's Fixed Asset System.

3.10 The Office of 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.

Related Statutes, Policies, Regulations and Rules

Texas Administrative Code 202.75 Information Security Standards

System Policy 29.01 Information Resources

System Regulation 29.01.03 Electronic Information Services Access and Security

---

Contact Office

Office of Information Resources Management 936-261-9350
