PRAIRIE VIEW A&M UNIVERSITY
UNIVERSITY ADMINISTRATIVE PROCEDURE

29.01.03.P0.22 Information Resources - Encryption of Confidential and Sensitive Information
Approved May 4, 2011
Revised July 1, 2015
Revised June 11, 2018
Next Scheduled Review: June 2023

UAP Purpose

The purpose of this University Administrative Procedure (UAP) is to provide guidance for Prairie View A&M University (PVAMU) on the use of encryption to protect the university's information resources that contain, process, or transmit confidential and/or sensitive information. In addition, the performance of these procedures is necessary to ensure compliance with the Texas Administrative Code Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education.

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. See the Texas A&M University System Data Classification Standard for additional 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.

Custodian of an Information Resource - a person responsible for implementing owner-defined controls and access to an information resource. Custodians may include PVAMU employees, vendors, and any third party acting as an agent of, or otherwise on behalf of PVAMU and/or the owner.

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

User of an Information Resource - an individual or automated application authorized to access an information resource in accordance with the owner-defined controls and access rules.

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.

Official Procedures and Responsibilities

1. GENERAL

1.1 PVAMU information resource owners, or designees, formally identify and classify data annually. This is accomplished during the risk assessment process using the ISAAC system. The purpose of this identification and classification process is to determine the appropriate security controls to apply in order to protect the data. For data that has been classified as confidential or sensitive, encryption is often the most appropriate control measure to put in place.

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 Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education, 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 PVAMU information resources. 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. It addresses encryption requirements and controls for confidential and/or sensitive data that is at rest (including portable devices and removable media) regardless of ownership of the particular storage device, and data in motion (transmission security). This UAP is compatible with, but does not supersede or guarantee compliance with all state and federal encryption standards.

3. RESPONSIBILITY

3.1 It is the responsibility of anyone (e.g., owner, custodian, user) having confidential or sensitive data in their possession or under their direct control (e.g., manages the storage device) to ensure that appropriate risk mitigation measures (e.g., encryption) are in place to protect data from unauthorized exposure. When encryption is used, appropriate key management procedures are crucial. Anyone employing encryption is responsible for ensuring that authorized users can access and decrypt all encrypted data using controls that meet operational needs and comply with data retention requirements.

4. PROCEDURES

4.1 All encryption mechanisms implemented to comply with this procedure must support a minimum of, but not limited to, AES 256-bit encryption (reference ***Data Encryption*** for recommended and supported encryption tools).

4.2 The use of proprietary encryption algorithms is not allowed for any purpose unless reviewed and approved by the ISO.

4.3 Recovery of encryption keys must be part of business continuity planning except for data used by a single individual (e.g., grade book archives).

4.4 When retired, computer hard drives or other storage media shall be sanitized in accordance with Texas Administrative Code Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education to prevent unauthorized exposure.

4.5 Any confidential or sensitive data transmitted to or from a site not on the campus network (e.g., to and from vendors, customers, or entities doing business with the University) must be encrypted or be transmitted through an encrypted tunnel that is encrypted with virtual private networks (VPN) or secure socket layers (SSL).

4.6 Confidential or sensitive data transmitted as an email message should be encrypted.

4.7 Transmitting unencrypted confidential or sensitive data through the use of web email programs is prohibited.

4.8 If peer-to-peer (P2P) or instant messaging (IM) is used to transmit confidential or sensitive data, traffic flows between peers must be encrypted and access only allowed to managed IM servers that provide gateways to public services.

4.9 Encryption is required when confidential or sensitive data is accessed remotely from a shared network, including connections from a Bluetooth device to a personal digital assistant (PDA) or cell phone.

4.10 Transfer of confidential or sensitive documents and data over the internet using secure file transfer programs (e.g., HTTPS, "secured FTP") is permitted.

Related Statutes, Policies, Regulations and Rules

Tex. Admin. Code Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education

Security Control Standards Catalog

System Policy 29.01 Information Resources

System Regulation 29.01.03 Information Security

Contact Office

Office of Information Resources Management	936-261-9350
