

PRAIRIE VIEW A&M UNIVERSITY
UNIVERSITY ADMINISTRATIVE PROCEDURE

29.01.03.P0.22 Encryption of Confidential and Sensitive Information

Approved (May 04, 2011)

Next Scheduled Review (May 2012)

1. PURPOSE

- 1.1 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.

2. GENERAL INFORMATION AND APPLICABILITY

- 2.1 **General** - Prairie View A&M University information resource owners, or designees, formally identify and classify data annually. This is accomplished during the risk assessment process using the ISAAC system. Informal identification/classification occurs as the need arises. 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. This UAP provides procedures and requirements for the use of encryption to protect the University's information resources that contain, process, or transmit confidential and/or sensitive information.
- 2.2 **Applicability** - This UAP applies to all Prairie View A&M University employees and affiliates, including contractors. It addresses encryption requirements and controls for confidential and/or sensitive data that is at rest, including portable devices including portable computing devices as listed at <http://pvamu.edu/include/UAP/29.01.03.P1.16.pdf> and on email as listed at <http://pvamu.edu/include/UAP/29.01.03.P1.03.pdf>, regardless of ownership of the particular storage device, and data in motion (transmission security). This UAP is compatible with, but does not supersede State and Federal encryption standards. The information resource owner or designee (e.g., custodian, user) is responsible for ensuring that the risk mitigation measures described in this UAP are implemented. Based on risk management considerations and business functions, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures provided in this UAP. All exclusions must be documented and reported to the Information Security Officer.

3. DEFINITIONS

- 3.1 **Confidential Information** - Information that must be protected from unauthorized disclosure or public release based on state or federal law, (e.g. the Texas Public Information Act and other constitutional, statutory, judicial, and legal agreements). Examples of "Confidential" data may include, but are not limited to the following:
- 3.1.1 Personally identifiable information, such as a name in combination with Social Security number (SSN) and/or financial account numbers,
- 3.1.2 Student education records,

- 3.1.3 Intellectual property, such as certain intellectual property as set forth in Section 51.914 of the Texas Education Code, and,
- 3.1.4 Medical records.
- 3.2 **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:
 - 3.2.1 Social Security Number;
 - 3.2.2 Driver’s license number or government-issued identification number (including UIN or Student ID);
 - 3.2.3 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.
- 3.3 **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.
- 3.4 **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.
- 3.5 **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.
- 3.6 **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.
- 3.7 **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.
- 3.8 **Sensitive data** – an optional PVAMU or owner defined category. Sensitive data may be subject to disclosure or release under the Texas Public Information Act, however the University or owner has decided that the data should have the same or equivalent level of protection as confidential data. Examples of Sensitive data may include but are not limited to:
 - 3.8.1 Operational information,
 - 3.8.2 Personnel records,
 - 3.8.3 Information security procedures,
 - 3.8.4 Research, and,
 - 3.8.5 Internal communications.

4. RESPONSIBILITY

- 4.1 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.

5. PROCEDURES

- 5.1 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).
- 5.2 The use of proprietary encryption algorithms is not allowed for any purpose unless reviewed and approved by the Information Security Officer.
- 5.3 Recovery of encryption keys must be part of business continuity planning except for data used by a single individual (e.g., grade book archives).
- 5.4 When retired, computer hard drives or other storage media that have been encrypted shall be sanitized in accordance with TAC §202.78, Removal of Data from Data Processing Equipment to prevent unauthorized exposure.
- 5.5 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).
- 5.6 Confidential or sensitive data transmitted as an email message should be encrypted.
- 5.7 Transmitting unencrypted confidential or sensitive data through the use of web email programs is prohibited.
- 5.8 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.
- 5.9 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.
- 5.10 Transfer of confidential or sensitive documents and data over the Internet using secure file transfer programs (e.g., HTTPS, "secured FTP") is permitted.