The Texas Administrative Code ("TAC") §202.71(b) requires institutions of higher education to define data classification categories and to establish appropriate controls for each category. Those controls typically include user authentication, encryption, periodic scanning, and the sanitization of decommissioned or repurposed storage media. This Procedure defines the classification of University data, and the controls to be implemented to protect University data.

Reason for Procedure

This Procedure applies to all Texas A&M University – San Antonio (“The University”) employees and affiliates, including contractors 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.

It addresses encryption requirements and controls for confidential and/or university-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 Procedure is compatible with, but does not supersede or guarantee compliance with all State and federal encryption standards.

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.

Official Responsibilities

1. All encryption mechanisms implemented to comply with this procedure must support a minimum of, but not limited to, AES 256-bit encryption. The use of proprietary encryption algorithms is not permitted for any purpose unless reviewed and approved by the Information Resources Manager (IRM) and/or University Information Security Officer (ISO).
2. Recovery of encryption keys will be part of business continuity planning where applicable and appropriate, except for data used by a single individual.

3. When University storage media is de-commissioned or repurposed, computer hard drives or other storage media that have been encrypted shall ensure that the media is either 1) physically destroyed by shredding or other accepted practice 2) be sanitized in accordance with TAC §202.78, removal of data from data processing and storage equipment to prevent unauthorized exposure.

4. Sensitive or confidential university data must not be stored on portable computing devices. However, in the event that there is no alternative, such data must be encrypted using university-approved encryption techniques unless reviewed and approved by the Information Resources Manager (IRM) and/or University Information Security Officer (ISO). Contact the Information Technology Services Helpdesk for assistance with encryption.

5. Sensitive or confidential university information must not be transmitted via wireless, including Bluetooth, to or from a portable computing device unless encryption techniques are utilized.

6. Remote access to the University systems must utilize approved encryption techniques when transmitting or receiving sensitive or confidential information.

7. Any confidential or sensitive university 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 and transmitted through an encrypted tunnel or secure socket layers (SSL) connection.

8. Confidential or sensitive data transmitted via an email message must be encrypted.

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

10. Transfer of confidential or sensitive documents and data over the Internet using approved secure file transfer protocols (e.g., HTTPS, “secured FTP”). This transfer is permitted to users that are authorized to view the confidential or sensitive data only.

11. Before confidential or sensitive university data is transferred to an authorized third party (e.g. vendors or business partners), the third party must affirm that they will protect the transferred data in accordance with the conditions imposed by the data’s Owner. At a minimum, the conditions specified in this procedure will be adopted and used as the baseline for transfer activity.
Definitions

**Confidential Information** - Information that is excluded from disclosure requirements under the provisions of applicable state or federal law, (e.g. the Texas Public Information Act and other constitutional, statutory, judicial, and legal agreements).

**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 Security Officer (ISO)** - Responsible to the executive management for administering the information security functions within the agency. The ISO is the university’s internal and external point of contact for all information security matters.

**User** - An individual or automated application or process that is authorized to the resource by the owner, in accordance with the owner’s procedures and rules.

**Portable Computing Device** - Any device that is easily portable and is capable of receiving, transmitting, processing, and/or storing data, and that can connect by cable, telephone wire, wireless transmission or via any Internet connection to the University infrastructure and/or data systems. These include, but are not limited to, notebook computers, handheld computers, PDA's, pagers, cellphones, and portable storage devices (such as flash drives, memory cards, USB-connected storage devices, etc.).

**Encryption** - The conversion of plaintext 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.

**Sanitize** means to overwrite data on a storage device with a program that complies with Department of Defense standard 5220.22-M.

Contact Office

Information Technology Services – (210) 784-4357 (HELP)