Standard Administrative Procedure Statement
The purpose of this Standard Administrative Procedure (SAP) is to provide guidance for the Texas A&M Engineering Experiment Station (TEES) on the use of encryption to protect information resources that contain, process, or transmit confidential and/or sensitive information.

Reason for Standard Administrative Procedure
This SAP provides procedures and requirements for the use of encryption to protect information resources that contain, process, or transmit confidential and/or sensitive information.

Procedures and Responsibilities

1. CONTROLS AND RESPONSIBILITIES

   1.1 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).

   1.2 The use of proprietary encryption algorithms is not allowed for any purpose unless reviewed and approved by the Chief Information Officer.

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

   1.4 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.

   1.5 Transfer, storage and access of confidential or sensitive documents and data must ensure that only authorized users can view this information.

      1.5.1 Electronic transmission of this information must occur with the data in an approved encrypted format or through an encrypted network tunnel (VPN, SSL, SFTP, HTTPS, etc.).
1.5.2 Confidential or security sensitive information cannot be stored on desktops, notebooks, laptops or portable electronic storage devices with the following exceptions:

1.5.2.1 Researchers may keep their student grades on these devices in an encrypted format.

1.5.2.2 Backup media for systems allowed to store this information may contain confidential or security sensitive information. This media must be kept physically secured.

1.5.2.3 Researchers may use division approved work desktops to develop and maintain research.

1.5.3 Confidential or sensitive information must be stored and accessible in a manner that ensures only authorized individuals have access.

Related Statutes, Policies, or Requirements
TAMU SAP 29.01.99.M1.31, Encryption of Confidential and Sensitive Information

TEES Rule 29.01.99.E1, Security of Electronic Information Resources

Contact Office
Information Technology Services
(979) 847-8585