Texas A&M University System Standard - Encryption of Confidential and Sensitive Information

Standard Statement

The purpose of this standard is to provide guidance for System Office (SO) on the use of encryption to protect the System Office's information resources that contain, process, or transmit Confidential and/or Sensitive information.

Definitions

Confidential - 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). Refer to System Regulation 29.01.03 and the related data classification standard for more information.

Examples of "Confidential" data may include but are not limited to the following:

- Personally Identifiable Information, such as: a name in combination with Social Security number (SSN) and/or financial account numbers
- Student Education Records
- Intellectual Property, such as: certain intellectual property as set forth in section 51.914 of the Texas Education Code
- Medical Records

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

Encryption (encrypts, **encipher**, **or encode**) - 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.

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.

.

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.

Sensitive data – an optional SO or owner defined category. Sensitive data may be subject to disclosure or release under the Texas Public Information Act, however the SO 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:

- operational information
- personnel records
- information security procedures
- research
- internal communications

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.

Responsibilities and Standards

---

1. GENERAL

   System Office information resource owners, or designees, formally identify and classify data annually. This is accomplished during the risk assessment process using the state-provided risk management 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.

   This standard provides standards and requirements for the use of encryption to protect the SO information resources that contain, process, or transmit Confidential and/or Sensitive information.

2. APPLICABILITY

   This standard applies to all SO employees and affiliates, including contractors. 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 standard is compatible with, but does not supersede or guarantee compliance with all 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 standard 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 standard. All exclusions must be in accordance with standard 29.01.99.S1.27 Exclusions from Required Risk Mitigation Measures.

3. RESPONSIBILITY

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 standards 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. STANDARDS

4.1 All encryption mechanisms implemented to comply with this standard 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 SO Information Security Officer or designee.

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 that have been encrypted shall be sanitized in accordance with TAC §202.78, Removal of Data from Data Processing Equipment 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 SO) 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 must 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 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, or Requirements

Supplements *System Regulation 29.01.03*

Additional Information ***Data Encryption***

Contact Office

For interpretation or clarification, contact The Texas A&M University System Chief Information Officer.

OFFICE OF RESPONSIBILITY**:** The Texas A&M University System Chief Information Officer