29.01.03.H0.08 Encryption

Approved: April 2014
Revised: January 5, 2024
Next Scheduled Review: January 2029

Procedure Summary

Portable computing devices are becoming increasingly powerful and affordable. Their small size and functionality are making these devices more desirable and are replacing traditional desktop devices in a wide number of applications. However, the portability offered by these devices may increase security exposure if lost or stolen.

The purpose of this procedure is to provide Texas A&M University-Texarkana (TAMUT) employees with guidance on the use of encryption to protect University Information Resources that contain, process, or transmit confidential and sensitive information. Additionally, this procedure provides direction to ensure that State and Federal regulations are followed. This procedure applies to all TAMUT employees and affiliates, including contractors. It addresses encryption rules and controls for confidential and other TAMUT-sensitive data.

Definitions

Critical Internal Use: Information that is not generally created for or made available for public consumption but that may or may not be subject to public disclosure through the Texas Public Information Act 3 or similar laws.

Information Resources (IR): Any computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing websites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, tablets, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), smartphones, telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it includes the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Public Information: Public information includes all information made available to the public through posting to public websites, distribution through email, or social media, print publications or other media, and information for which public disclosure is intended or required.

Virtual Private Network (VPN): A network which utilizes public telecommunications infrastructure to conduct private data communications via an encrypted connection.

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).

Procedures and Responsibilities

1. RESPONSIBILITY

1.1 It is the responsibility of anyone (e.g., owner, custodian, user) having confidential or sensitive information 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.

1.2 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.

2. PROCEDURES

2.1 Sensitive or confidential information must not be stored on portable computers or devices. If there is no other alternative, portable computers and devices must be encrypted using at least 128-bit encryption or password protection following the guidelines of University Procedure 29.01.03.H0.11, *Identification and Authorization*. ContactIT Security by email at itsecurity@TAMUT.edu for assistance with encryption.

2.2 Information for Critical Internal Use must not be transmitted via wireless systemto or from portable computing devices unless the device is connected through TAMUT's VPN network.

2.3 Remote access to TAMUT may only be established using TAMUT's VPN solution.

2.4 Only encryption solutions approved by the Information Security Officer or designee may be utilized.

2.5 All encryption mechanisms implemented to comply with this standard must support a minimum of, but not limited to, AES 256-bit encryption for both data-at-rest and data-in-transit which **includes** Critcal Internal Use but **does not include** Public Information data.

2.6 Recovery of encryption keys must be part of business continuity planning except for data used by a single individual.

2.7 When retired, computer hard drives or other storage media that have been encrypted will be sanitized in accordance with TAC §202.-to prevent unauthorized exposure.

2.8 Transmission of confidential or sensitive documents and data over the Internet must be done using secure file transfer programs such as HTTPS or Secured-FTP.

2.9 Data-sensitive contracts are required to be reviewed by the ISO or designated security team member, as part of the procurement process.

3. DISCIPLINARY ACTIONS

3.1 Violation of this procedure may result in disciplinary action which may include termination for employees, termination of business relationships for contractors or consultants, dismissal for interns and volunteers, or suspension or expulsion for students. Additionally, individuals are subject to loss of TAMUT Information Resources access privileges and civil and criminal prosecution.

Related Statutes, Policies, or Requirements

Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C, Rule

University Procedure 29.01.03.H0.11, *Identification and Authorization*.
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Family Educational Rights and Privacy Act (FERPA)
IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies and Entities
National Institute of Standards and Technology Special Publication 800 series (e.g., NIST SP 800-57)
Payment Card Industry Data Security Standard
Texas Business and Commerce Code, Chapter 521
Texas Government Code Ch. 552, Public Information

Contact Office

Office of Information Technology
903-334-6603