TEXAS A&M INTERNATIONAL UNIVERSITY

Standard Administrative Procedure (SAP)

29.01.99.L1.24 Encryption

First Approved: March 28, 2013
Revised: June 22, 2017
Next Scheduled Review: June 22, 2022

Procedure Statement and Reason for Procedure

Portable computing devices are becoming increasingly powerful and affordable. Their small size and functionality are making these devices more desirable, and the devices 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.

This SAP addresses encryption requirements and controls for Texas A&M International University (TAMIU) confidential or sensitive data on any device, regardless of ownership of that device. The purpose of this SAP is to provide TAMIU employees guidance on the use of encryption to protect TAMIU Information Resources that contain, process, or transmit confidential or sensitive information. Additionally, this SAP provides direction to ensure that State and Federal regulations are followed. This SAP applies to all TAMIU employees and affiliates, including contractors. This SAP supplements *TAMIU Rule 29.01.99.L1, Use of Information Resources and Facilities* and *TAMIU Rule 24.99.01.L1, Security of Electronic Information Resources*.

Procedures and Responsibilities

1. Responsibility

   It is the responsibility of the individual (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, restricted physical access) 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.

2. Procedures

2.1 Sensitive or confidential information must not be stored on portable computers or devices without appropriate risk mitigation measures. Whenever possible, portable computing devices must be encrypted using at least 128-bit encryption and password protection following the guidelines of *TAMIU SAP 29.01.99.L1.13, Password Management*. Contact TAMIU IT Security by email at itsecurity@tamiu.edu for assistance with encryption.

2.2 Sensitive or confidential information must not be transmitted via any network without appropriate risk mitigation measures (e.g., VPN, SSL, etc.) For information classification, see *TAMIU SAP 29.01.99.L1.31, Information Classification*. Transfer of confidential or sensitive data using secure file transfer programs (HTTPS, FTPS, SFTP) is permitted.

2.3 Only encryption solutions approved by the Information Security Officer (ISO) or designee may be utilized on TAMIU-owned Information Resources.

2.4 Recovery of encryption keys must be part of a department's business continuity planning.

2.5 When retired, computer hard drives or other storage media will be sanitized and/or physically destroyed.

Related Statutes, Policies, Regulations, or Rules

Texas Administrative Code 202, Subchapter C – Information Security Standards for Institutions of Higher Education
TAMIU Rule 24.99.01.L1, Security of Electronic Information Resources
TAMIU Rule 29.01.99.L1, Use of Information Resources and Facilities

Appendix

References:
Copyright Act of 1976
Foreign Corrupt Practices Act of 1977
Computer Fraud and Abuse Act of 1986
Computer Security Act of 1987
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The State of Texas Information Act
Texas Government Code, Section 441
Texas Administrative Code, Chapter 202
IRM Act, 2054.075(b)
The State of Texas Penal Code, Chapters 33 and 33A
DIR Practices for Protecting Information Resources Assets
DIR Standards Review and Recommendations Publications

Contact Office

Office of Information Technology, 956-326-2310