29.01.99.K1.305 Encryption Standard Administrative Procedure

Approved: December 14, 2012
Revised: April 2, 2019
Next Scheduled Review: April 2, 2024

Introduction

The implementation of encryption at Texas A&M University-Kingsville (TAMUK) is designed to reduce risks to confidential or sensitive information by providing the appropriate levels of protection as required by state and federal law.

Purpose

The purpose of this procedure is to provide guidance on the use of encryption to protect TAMUK Information Resources that store or transmit confidential or sensitive information. Additionally, this procedure provides direction to ensure that System, State and Federal regulations are followed.

Audience

This procedure applies to all TAMUK employees and affiliates, including contractors. It is the responsibility of the individual having confidential or sensitive information in their possession or under their direct control to ensure that appropriate risk mitigation measures are in place to protect data from unauthorized exposure.

Encryption Procedure

1. Encryption Standards
   Any encryption performed on University systems must use University approved encryption software. All encryption mechanisms implemented to comply with this procedure must support a minimum of, but not limited to, AES 128-bit encryption. Encryption must permit properly designated University officials, when required and authorized, to decrypt the information.
   a. Proven, standard algorithms should be used as the basis for encryption technologies. Approved encryption tools include:
      i. Accellion Secure File Transfer
      ii. Microsoft BitLocker
      iii. Secure Socket Layer (SSL)
      iv. Virtual Private Network (VPN)

b. Exceptions for encryption tools must be approved by the Information Security Officer. The use of proprietary encryption algorithms is not allowed for any purpose unless reviewed and approved by the Information Security Officer.

2. Encryption Key Management

When encryption is used, appropriate key management procedures are crucial. Anyone employing encryption is responsible for ensuring authorized users can access and decrypt all encrypted data using controls that meet operational needs and comply with data retention requirements

3. Confidential/Sensitive Information

a. Data in transit

i. Copying and moving documents and files

University faculty and staff must encrypt files and documents containing confidential or sensitive University information for protection against unauthorized disclosure while in transit.

ii. Emailing documents and files

Email represents a risk to the confidentiality and integrity of information transmitted. Therefore, any confidential or sensitive information transmitted via email must be encrypted.

iii. Virtual faxing of documents

Virtual faxing of documents must be accomplished with an encrypted platform.

b. Data at rest

i. On-campus data

Confidential or sensitive data at rest on computer systems owned by and located within TAMUK controlled spaces and networks must be protected by encryption.

1. Employees' computers will have encryption activated.
2. Departments may request encryption for additional computers such as student workers who handle confidential or sensitive information.

ii. Off-campus data

University confidential or sensitive information at rest not located within TAMUK controlled spaces and networks must be protected by encryption. Contracts for off-site information systems must include data encryption assurances as part of the contract language.

c. Portable Devices

Portable devices represent a category of devices that may contain data-at-rest. Whenever possible, portable computing devices must be password protected. As a general practice, confidential or sensitive data should not to be copied to or stored on a portable device or a non-TAMUK owned computing device. However, in situations that require confidential or sensitive data be stored on such devices, encryption is required to reduce the risk of unauthorized disclosure in the event that the device becomes lost or stolen.

3. Federal export laws

Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

Disciplinary Actions

Violation of this procedure may result in disciplinary action up to and including termination for employees and temporaries; a termination of contract relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of students. Additionally, individuals are subject to loss of TAMUK Information Resources access privileges, civil, and criminal prosecution.

References

1. Computer Fraud and Abuse Act of 1986
2. Computer Security Act of 1987
3. DIR Practices for Protecting Information Resources Assets
4. DIR Standards Review and Recommendations Publications
5. The State of Texas Information Act
6. The State of Texas Penal Code, Chapters 33 and 33A
7. Texas Administrative Code, Chapter 202
8. Texas A&M University-Kingsville Acceptable Use Procedure 29.01.99.K1.010
9. Texas Government Code, Section 441
10. TAMU System Policy 29.01.03 Information Security

Contact Office

For More Information, Contact: iTech
MSC 185, 700 University Blvd., Kingsville, TX 78363-8202
Contact Phone: 361-593-2404