Encryption Procedure

Introduction
The implementation of encryption at Texas A&M University-Kingsville (TAMUK) is designed to reduce risks to sensitive and critical 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 critical and sensitive information. Additionally, this procedure provides direction to ensure that State and Federal regulations are followed.

Audience
This procedure applies to all TAMUK employees and affiliates, including contractors.

Encryption Procedure
1. Encryption Standards
   Any encryption performed on University systems must use University approved encryption software. Encryption must permit properly designated University officials, when required and authorized, to decrypt the information.
   Proven, standard algorithms should be used as the basis for encryption technologies.
   Examples of standard encryption tools include:
   a. Accellion Secure File Transfer
   b. Pretty Good Privacy (PGP)
   c. Secure Socket Layer (SSL)

2. Critical/Sensitive Information
   a. Data in transit
      1) Copying and moving documents and files
         Users will follow TAMUK Acceptable Use Procedure when transmitting data and must take particular care when transmitting or re-transmitting critical or sensitive data (e.g., personal identification information). University faculty and staff must encrypt files and documents containing sensitive or critical University information for protection against unauthorized disclosure while in transit. This includes copying and moving of files and data.
      2) Emailing documents and files
         Email, by default, is unencrypted and represents a risk to the confidentiality and integrity of information transmitted. Therefore, any critical or sensitive information transmitted via email must be encrypted.
   b. Data at rest
      1) On-campus data
         Critical or sensitive data at rest on computer systems owned by and located within TAMUK controlled spaces and networks must be protected by encryption or firewalls with strict access controls that segregate systems and data from the campus at large and logical and physical access controls.
2) Off-campus data
   Critical or sensitive data at rest on computer systems not owned by or located within
   TAMUK controlled spaces and networks must be protected by encryption. Off-site
   information resource contracts must include data encryption assurances as part of the
   contract language.

c. Portable Devices
   Portable devices represent a specific category of devices that contain data-at-rest. As a
   general practice, critical or sensitive data should not to be copied to or stored on a
   portable computing device or a non-TAMUK owned computing device. However, in
   situations that require critical or sensitive data to 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.

d. 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 employment relations in the case of contractors or
consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a
student. Additionally, individuals are subject to loss of TAMUK Information Resources access
privileges, civil, and criminal prosecution.

References

1. Copyright Act of 1976
2. Computer Fraud and Abuse Act of 1986
4. DIR Practices for Protecting Information Resources Assets
5. DIR Standards Review and Recommendations Publications
7. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
8. IRM Act, 2054.075(b)
9. The State of Texas Information Act
10. The State of Texas Penal Code, Chapters 33 and 33A
11. Texas Administrative Code, Chapter 202
12. Texas A&M University-Kingsville Procedure 29.01.03.K1.010
13. Texas A&M University-Kingsville Procedure 29.01.04.K1.010
14. Texas Government Code, Section 441