1. **Purpose**

The purpose of this policy is to provide Texas A&M University-Kingsville (TAMUK) guidance on the use of encryption to protect TAMUK information resources that store or transmit confidential and sensitive information. Additionally, this policy provides direction to ensure that State and Federal regulations are followed.

2. **Scope**

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

3. **Policy**

3.1. **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:

- Accellion Secure File Transfer
- Pretty Good Privacy (PGP)
- Secure Socket Layer (SSL)

3.2. **Confidential/Sensitive Information**

3.2.1. **Data in transit**

3.2.1.1. **Copying and moving documents and files**

Users will follow TAMUK acceptable use policies when transmitting data and must take particular care when transmitting or re-transmitting confidential or sensitive data (e.g., personal identification information). University faculty and staff must encrypt files and documents containing sensitive or confidential University information for protection against unauthorized disclosure while in transit. This includes copying and moving of files and data.

3.2.1.2. **Emailing documents and files**

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

3.2.2. **Data at rest**

3.2.2.1. **On-campus data**

Confidential and 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.
3.2.2.2. Off-campus data
Confidential and sensitive data at rest on computer systems not owned by or located within TAMUK controlled spaces and networks must be protected by encryption. All off-site information resource contracts must include data encryption assurances as part of the contract language.

3.2.3. Portable Devices
Portable devices represent a specific category of devices that contain data-at-rest. As a general practice, confidential 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 confidential 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.

3.2.4. 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.

4. Disciplinary Actions
Violation of this policy, [e.g., willful or negligent exposure of confidential information,] may result in disciplinary action which may include termination of employment, dismissal, suspension, or expulsion from an institution of higher education if violated by a student and debarment if violated by a contractor. Additionally, employees, contractors and agents who violate this policy may be subject to loss of TAMUK Information Resources access privileges, and to civil and criminal prosecution.