CRYPTOGRAPHIC CONTROLS

1. Purpose

Employees of the UNT System (System) must adhere to all information technology regulations, policies, and standards related to cryptographic controls. Systems, devices, and files requiring cryptographic control must adhere to the protocols listed herein.

2. Scope

This standard applies to all employees of the System and establishes cryptographic control requirements for all System information resources that store and/or process System data.

3. Definitions

3.1. Confidential Information. Information that requires protection from unauthorized disclosure or public release based on state or federal law (e.g., the Texas Public Information Act, and other constitutional, statutory, and judicial requirements), legal agreement, or information that requires a high degree of confidentiality, integrity, or availability.

3.2. Cryptography. The discipline that embodies the principles, means, and methods for the transformation of data to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification.

3.3. Encryption. Cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption," which is a transformation that restores encrypted data to its original state.

3.4. Modern Cryptographic Protocols. Current algorithms and ciphers that enable the encryption and decryption of information, such as the Advanced Encryption Standard (AES) cipher suites.

3.5. System Administrator. A Custodian responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established policy and procedures.

3.6. UNT System Information Security Program. The UNT System Information Security Program includes the policies, Information Security Handbook, controls catalogs, standards, procedures, trainings, strategies, objectives, resources, and plans that establish the information resources security function for the UNT System and its institutions.

3.7. User. An individual or automated application authorized to access information or information resources in accordance with the Information Owner-defined controls and access rules.

4. Responsibilities

4.1. Web-based Encryption

4.1.1. System Administrators should use TLS 1.3 for web-based encryption using the most up to date cipher suites.

4.1.1.1. If the system is incapable of TLS 1.3 the System Administrator should use TLS 1.2.

4.1.2. System Administrators must not use deprecated cryptographic standards without a documented security exception. See NIST Special Publication 800-175B Revision 1 for additional information on deprecated cryptographic standards.

4.1.3. Legacy systems and systems that cannot support modern compatibility encryption protocols (e.g., TLS 1.0, TLS 1.1) must have a documented security exception and compensating controls in place.

4.2. Full Disk Encryption

4.2.1. System Administrators should employ full disk cryptographic mechanisms using modern cryptographic protocols on systems with confidential information at endpoints.

4.2.2. Users with access to confidential information requiring protection in accordance with external security requirements (e.g. NIST 800-171, CMMC, NIH Best Practices) must encrypt mobile and desktop computing devices using modern cryptographic protocols.

4.2.2.1. Inherent protocols must be set to the highest level of encryption.

4.2.3. Encryption key management best practices must always be followed, including, but not limited to:

4.2.3.1. Use only FIPS-approved or NIST-recommended key generation methods.

4.2.3.2. Ensure all keys are stored in a cryptographic vault, such as a hardware security module (HSM) or isolated cryptographic service.

4.2.3.3. Should the transfer of private encryption keys be necessary, the transfer must occur through a secure vault and never manually through any electronic communication channel.

4.2.3.4. Records of key sharing must be accurate and up to date.

4.2.3.5. Keys should never be stored in plain-text format.

4.2.3.6. Lost or stolen key-enabled devices must be reported immediately.

4.2.3.7. Key management activities must be regularly logged and audited.

4.2.3.8. Rotation of encryption keys should occur upon major changes to the information system.

4.2.3.9. Rotation of encryption keys is recommended at a minimum of two-year intervals.

4.2.3.10. Rotate or delete keys after a potential compromise.

4.3. File Encryption

4.3.1. Users must encrypt files as required by the UNT System Information Security Program.

4.3.2. Users with access to confidential information stored on a portable storage device must encrypt the files using inherent cryptographic protocols provided by the vendor.

4.3.2.1. Inherent protocols must be set to the highest level of encryption.

4.3.3. Users with access to confidential information requiring protection in accordance with external security requirements must encrypt files according to the requirements set forth by the external party.

4.4. Communications Encryption

4.4.1. Users must encrypt confidential information transmitted over a public network using approved and centrally administered communication systems.

4.5. References

4.5.1. FIPS 140-3 – Security Requirements for Cryptographic Modules
4.5.2. NIST Cryptographic Standards and Guidelines
4.5.3. NIST Special Publication 800-175B Revision 1 – Guideline for Using Cryptographic Standards in the Federal Government
4.5.4. OWASP Key Management Cheat Sheet

DOCUMENT VERSION LOG			
Version	**Approved By**	**Date**	**Description**
1	Rich Anderson	1/26/2024	New Cryptographic Control Standard