CRYPTOGRAPHIC SECURITY

07.300.04

Authority:	Chief Information Officer (CIO)
History:	Approved by CIO July 10, 2021
Sources of Authority:	UNC System Office Policy Manual, Chapter 1400 “Information Technology”; International Organization for Standardization ISO/IEC 27002
Related Links:	07.100.00 Responsible Use of Information Technology Resources 07.200.00 Responsible Management of Information Technology Resources
Responsible Office:	Information Technology Services

I. Purpose

The purpose of this policy is to define and explain requirements for cryptographic security. These measures ensure that sensitive and critical UNCW data being stored or transmitted remains accessible only to those who require access.

II. Policy

A. All sensitive UNCW data or UNCW data with a cryptographic requirement arising from state or federal statute or regulation, UNCW policy or standard, or other external source, must be encrypted by the use of valid encryption processes for data at rest and in motion.

B. General Cryptographic and Encryption Standards

1. Sensitive data is defined by the Data Classification Standard. Any staff or faculty member, or non-affiliate with access to sensitive data should review the Data Classification Standard to understand the expectations of managing, storing, and transmitting university owned data.

2. UNCW data that meets the qualification for sensitive must be encrypted during storage, transmission, and process, according to the specifications outlined in the Cryptographic Security Standard.

a) If encryption is not a viable option an appropriate and comparable compensating control must be implemented.

b) Any and all compensating controls that remove the requirement for encryption are considered exceptions to security policy and require review and approval for noncompliance.

3. If a portable media or mobile device is required to store or access sensitive data, the media or device must leverage the appropriate encryption as well as other security controls relevant to the data.

4. Responsible parties (i.e., data custodians) will maintain appropriate and up-to-date encryption protocols for all university applications, including the acquisition and upkeep of Trasport Layer Security (TLS) certificates.

5. When sensitive data is stored/processed by/transmitted to a third-party site, due diligence must be performed to ensure that it can adhere to the university's encryption standards.

6. Key management and encryption requirements:

   a) Any encryption keys must be housed in isolation from non-privileged access. Access to this part of the network must have security controls equal to or greater than that of the key itself.

   b) Only users who possess a business need to know should be provided with authorization to access encryption keys.

   c) Those entrusted with custodianship of encryption keys formally acknowledge and accept their responsibilities annually.

   d) Any and all access to encryption keys must be properly documented/logged and available for review.