THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: SC-005-Encryption	
Version 6	**Effective Date: 03/17/2016**

Responsible Office: Office of Cybersecurity	Last Review: 07/24/2023 Next Review: 07/24/2025
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

To establish encryption requirements for all devices on the UTHSC network. This Standard also covers the circumstances under which encryption must be used when data is being transferred.

This standard is also designed to meet compliance requirements for data regulated by federal or state law. This includes, but not limited to, security requirements and safeguards for the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), or Gramm-Leach-Bliley Act (GLBA).

Scope

Any device, whether UTHSC IT Resources, vendor owned or personally owned by a member of the UTHSC community, i.e. computers, electronic devices, and media capable of storing electronic data that house UTHSC data or information.

Definitions

Encryption – the process by which data is transformed into a format that renders it unreadable without access to the encryption key and knowledge of the process used.
Encryption Key – a password, file, or piece of hardware that is required to encrypt and decrypt information, essentially locking and unlocking the data.
Level 3 Data Classification – the highest data classification level, also known as "High", these data types require the most stringent of security controls. Examples of Level 3 data are compliance-driven data, such as Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), or Gramm-Leach-Bliley Act (GLBA)
Personal Device – any device that is not purchased or owned by UTHSC.
UTHSC IT Resource - Any data, device, or other component of the information environment that supports information-related activities. Assets generally include hardware (e.g., endpoint devices), software (e.g., critical applications and support systems), and information.

Responsibilities

Data Owner is ultimately responsible for the data and information being collected and maintained by his or her department or division, usually a member of senior management. They assign data classification based on the data's potential impact level and determine if data access is allowed.

Information Technology Services (ITS) is responsible for the deployment of the technical controls to manage devices on the UTHSC network.

Office of Cybersecurity is responsible for establishing security controls and procedures to protect UTHSC intellectual property and data. Classification of data is per GP-002-Data & System Classification. The security of the data is based on GP-005-Data Security.

Owners of personal devices must abide by this practice and all University standards and practices while using their personal devices on the UTHSC network.

System Owner is responsible for the development, procurement, integration, modification, operation, maintenance, and/or final disposition of an information system.

UTHSC Chancellor/Executive Leadership defines the allowance for the use of personal devices on the UTHSC network.

Standard

1. Encryption algorithms and cyphers in use must meet the standards defined for use in NIST publication FIPS 140-3 or any superseding document, according to the date of implementation. For additional guidance, see NIST SP 800-131A Revision 2 or subsequent revisions.
2. No proprietary encryption algorithms are allowed, unless with documented approval from the UTHSC Office of Cybersecurity.
3. Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.
4. Devices and Media Encryption is required for all laptops, workstations, and portable drives, if available, that are used to store or access UTHSC data regardless of the data classification.
5. Data residing on servers owned and operated by UTHSC ITS and located within the UTHSC Data Center must be protected by at least one of the following:

- Encryption, or
- Strict Access Controls that authenticate individuals accessing these data, or
- Technical controls approved by the UTHSC Office of Cybersecurity

6. ITS provides, installs, configures, and supports encryption. Most devices purchased and imaged by ITS since 2016 have encryption configured. Any support needed for encryption can be handled by the ITS Service Desk or through TechConnect.
7. UTHSC data or information must be protected by encryption during transmission over any wireless network and during transmission over any non-UTHSC network.
8. All email communications that involve email addresses outside of the UTHSC email environment and that contain UTHSC data or information with a level 3 classification ranking either in the body of the email or as an attachment require that the email be encrypted.
   a. If the encryption method includes a password, that password must be transferred through an alternative method, such as calling the individual and leaving the password on their voicemail.
   b. Email messages containing encrypted data may never include the password in the same message as the encrypted data. Individuals who are unsure if they are correctly encrypting electronic data transfers should contact the ITS Office of Cybersecurity at itsecurity@uthsc.edu.
9. As of January 1, 2016, all portable storage devices and media must be fully encrypted regardless of device ownership. The following exceptions apply:
   a. When NO UTHSC data or information with a level 3 classification ranking will be stored and encryption would interfere with the device's intended use (e.g. a promotional USB device). Devices used in this manner must be clearly marked as not for use with UTHSC data or information with a level 3 classification ranking .
   b. Devices and/or media used for marketing and public relations, that have no UTHSC data or information with a level 3 classification ranking stored on the device, and the intended recipient is not a member of the UTHSC Community.
10. All persistent storage within any and all mobile computing devices used within UTHSC must meet the following encryption standards:
    a. The encryption passphrase will meet or exceed password strength

requirements per AC-002.02-Password Management and Complexity. The following exception applies:

- Small portable computing devices where keyboard entry is cumbersome (e.g., smartphones) may use reduced password strength and complexity if the device is configured to allow no more than 10 failed password entry attempts before preventing use by locking for a significant amount of time or erasing all storage.

b. The encryption mechanism includes a management component that provides key recovery and proof that the device is encrypted.

c. The encryption and key management methods used must have the approval of UTHSC Information Security or designee.

d. Whenever possible, devices will include the ability to remotely wipe stored data in the event the device is lost or stolen.

11. Personally owned devices must adhere to CS-002-Personally Owned Device Security.
12. Exceptions to this Practice should be requested using the process outlined in GP-001.02 Security Exceptions and Exemptions to ITS Standards and Practices.

References

1. National Institute of Standards and Technology (NIST) publication FIPS 140-3
2. NIST SP 800-131A Revision 2
3. AC-002.02-Password Management and Complexity
4. CS-002-Personally Owned Device Security
5. GP-001.02-Security Exceptions and Exemptions to ITS Standards and Practices
6. GP-002-Data & System Categorization
7. GP-005-Data Security