THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: IT0311-HSC-E.01 Encryption for Mobile Computing and Storage Devices	
Version 4	**Effective Date: 03/17/2016**

Responsible Office: Office of Cybersecurity	Last Review: 03/01/2025 Next Review: 03/01/2027
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

To outline encryption requirements for all personally owned and the University of Tennessee Health Science Center (UTHSC) owned and managed mobile computing and storage devices.

Scope

All mobile computing and storage devices, appliances, laptops, tablets, smartphones, peripherals, etc. regardless of device ownership accessing, storing, and transmitting UTHSC data or information with a level 2 categorization rating per IT0005-HSC-A-Data & System Classification.

Definitions

Level 2 Data - The effect on confidentiality and integrity of the Data is significant and includes compliance requirements. This Data is governed by federal, or state compliance requirements, and unwarranted exposure can lead to compliance issues and/or fines. This includes all Data that contains personally identifiable information (PII), protected health information, student education records, and cardholder Data. This categorization level also includes lower-risk items that, when combined, represent increased risk. per IT0005-HSC-A-Data & System Categorization. Minimum security requirements are explained on the webpage https://uthsc.edu/its/cybersecurity/requirements.php.

Personal Device – any device that is not purchased or owned by UTHSC.

UTHSC Information Technology (IT) Resource - a broad term for all things related to information technology from a holistic point of view and covers all University owned or managed information technology services, including cloud-based services, that users have access to.

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 determines if data access is allowed.

Information Technology Services (ITS) is responsible for the deployment of the technical controls to manage personal 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 IT0005-HSC-A-Data & System Categorization. The security of the data is based on IT0311-HSC-D-Data Security.

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

System Owner is responsible for the development, procurement, integration, modification, operation, and 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.

Practice

1. UTHSC data or information with a level 2 categorization must be protected by encryption during transmission over any wireless network and any non-UTHSC network.
2. All mobile devices deployed after October 1, 2017 through ITS CTS (Customer Technology Services) are encrypted.
3. Regardless of device ownership, as of January 1, 2016, UTHSC data or information with a level 2 categorization stored on mobile computing and/or portable storage devices must be encrypted.
4. 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 IT0506-HSC-A.01-Password Management and Complexity. The following exception applies:
      i. Small portable computing devices where keyboard entry is cumbersome (e.g. smart phones) 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’s Office of Cybersecurity or designee.
   d. Whenever possible, devices will include the ability to remotely wipe stored data in the event the device is lost or stolen.

5. All portable storage devices must be fully encrypted. The following exceptions apply:
   a. When NO UTHSC data or information with a level 2 categorization will be stored and encryption would interfere with the device’s intended use (e.g. a promotional USB device). Devices used in this way must be clearly marked as not for use with UTHSC data or information with a level 2 categorization.
   b. Devices and/or media used for marketing and public relations, that have no UTHSC data or information with a level 2 categorization stored on the device, and the intended recipient is not a member of the UTHSC Community.
6. Personally owned devices must adhere to IT0102-HSC-C-Personally Owned Device Security.
7. Exceptions to this Practice should be requested using the process outlined in IT0003-HSC-A.02-Security Exceptions and Exemptions to ITS Standards and Practices.
   a. If an exception is allowed and personal devices, encryption of these devices must be adhered to according to IT0311-HSC-E--Encryption.

Policy History

Version #	Effective Date
1	03/17/2016
2	12/03/2020
3	03/01/2023
4	03/01/2025 – new naming convention

References

1. IT0311-Information Technology Data Access, Management, and Recovery
2. IT0003-HSC-A-Information Security Program
3. IT0003-HSC-A.02-Security Exceptions and Exemptions for ITS Standards Practices & Controls
4. IT0005-HSC-A-Data & System categorization
5. IT0102-HSC-C-Personally Owned Device Security
6. IT0311-HSC-D-Data Security
7. IT0311-HSC-E-Encryption
8. IT0506-HSC-A.01-Password Management and Complexity