THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: SC-005.02-Encryption for Mobile Computing and Storage Devices	
Version 2	**Effective Date: 03/17/2016**

Responsible Office: Office of Cybersecurity	Last Review: 12/03/2020 Next Review: 12/03/2022
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

To outline encryption requirements for all personally owned and UTHSC owned and managed mobile computing and storage devices.

Scope

All mobile computing and storage devices, appliances, laptops, tablets, smart-phones, peripherals etc. regardless of device ownership accessing, storing, transmitting UTHSC data or information with a classification rating of 3 in any area. Classification of data is per GP-002-Data & System Classification.

Definitions

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 determines if data access is allowed.

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 Standard-InfoSec-GP-002-Data & System Classification. The security of the data is based on Standard-InfoSec-GP-005-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 classification rating of 3 in any area 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) must be encrypted.
3. Regardless of device ownership, as of January 1, 2016, UTHSC data or information with a classification rating of 3 in any area 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 Practice-InfoSec-AC-002.02-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 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.
5. All portable storage devices must be fully encrypted. The following exceptions

apply:

6. When NO UTHSC data or information with a classification rating of 3 in any area 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 classification rating of 3 in any area.
7. Devices used for marketing and public relations, that have no UTHSC data or information with a classification rating of 3 in any area stored on the device, and the intended recipient is not a member of the UTHSC Community.
8. Personally owned devices must adhere to Standard-InfoSec-CS-002-Personally Owned Device Security.
9. Exceptions to this Practice should be requested using the process outlined in Practice-Infosec-GP-001.02 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 InfoSec-SC-005-Encryption.

References

1. GP-001-UTHSC Information Security
2. CS-002-Personally Owned Device Security
3. GP-002-Data & System Classification
4. GP-005-Data Security
5. GP-001.02 Security Exceptions and Exemptions to ITS Standards and Practices
6. AC-002.02-Password Management and Complexity