THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: CS-002-Personally Owned Device Security	
Version 4	**Effective Date: 03/20/2016**

Responsible Office: Office of Cybersecurity	Last Review: 01/25/2023 Next Review: 01/25/2025
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

To provide computer security standards for the appropriate use and procedures for using personally owned devices connected to the UTHSC network and the storage of intellectual property, sensitive data, or University licensed software. This standard is also designed to meet compliance requirements for data regulated by federal or state law. This includes, but is 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

This practice applies to every person accessing the UTHSC enterprise.

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.
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. Categorization of data is per GP-002-Data & System Classification. The security of the data is based on 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.

Standard

1. Those using personal devices on the UTHSC network must:
   a. Not store data with a level 3 classification rating on those devices.
   b. Not access data with a level 3 classification rating on those devices unless they have agreed to the security controls deemed appropriate by the Office of Cybersecurity and approved by the Data Owner.
   c. Not store the authoritative version of UTHSC data or information.
   d. Destroy, remove, or return all data, electronic or otherwise belonging to UTHSC once their relationship with UTHSC ends or once they are no longer the owner or primary user of the device. (e.g., the sale or transfer of the device to another person).
   e. Remove or return all software application licenses belonging to UTHSC when the device is no longer used for UTHSC business.
   f. Notify the Office of Cybersecurity of any theft or loss of the personal device containing data or software application licenses belonging to UTHSC.
   g. Not connect the personal device the UTHSC network without prior authorization.
   h. Successfully authenticate to the UTHSC network using approved credentials including, but not limited to UT-NetID, eduroam, UT-LDAP, or UTAD.
   i. Keep the device current on security patches and updates and allow UTHSC mobile device management tools to be installed and maintained.
2. Network Access:
   a. Network services provided to personal devices are limited to Internet access and University computing resources that are available to the public. Personal devices requiring additional network access to conduct UTHSC business must meet security requirements for UTHSC managed computers, dictated in CS-001-Device Life Cycle Security.

3. Failure to comply with this policy will be reported as an information security violation and may result in loss of network and system privileges for the computer and/or disciplinary action per GP-001.04-Information Security Violations for the individual violating the policy.
4. Exceptions to this Standard should be requested using the process outlined in 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 SC-005-Encryption and SC-005.02-Encryption for Mobile Computing and Storage Devices.

References

1. GP-001-UTHSC Information Security Program
2. CS-001-Computer Security
3. GP-002-Data & System Classification
4. GP-005-Data Security
5. SC-005-Encryption
6. SC-005.02-Encryption for Mobile Computing and Storage Devices
7. GP-001.02-Security Exceptions and Exemptions to ITS Standards and Practices
8. GP-001.04-Information Security Violations