UT Health San Antonio

INSTITUTIONAL HANDBOOK OF OPERATING POLICIES

5.8.12 Mobile Device and Personally Owned Computing Policy

Chapter 5 - Information Technology	Original Effective Date: June 2000
Section: 5.8 Information Security	Date Last Reviewed: February 2023
Responsible Entity: Chief Information Security Officer	Date Last Revised: June 2018

I. Purpose

To establish the standard for mobile device and personally owned computers using and accessing institutionally-owned information technology resources.

II. Scope

This policy applies to all current and former faculty, staff, students, residents, healthcare providers, researchers, contractors, or any other third party entities who have direct or indirect access to Information Resources created, held or maintained by UT Health San Antonio or any controlled affiliate, including, but not limited to its clinics, hospitals, and research operations.

III. Policy

A. General

UT Health San Antonio (UTHSA) shall adopt and communicate standards and procedures to manage mobile computing devices and personally owned computing devices ("Bring Your Own Device" or "BYOD") that may connect to the UTHSA network infrastructure or create, store or transmit Confidential or Mission Critical Data.

1. Mobile computing devices are defined as smartphones, tablets and any device utilizing an operating system explicitly developed for mobile computing.

   Laptop computers owned or leased by UTHSA are exempt from this policy and must comply with all other UTHSA policies and standards, including Handbook of Operating Policies (HOP), Policy 5.8.8, Information Resource Security Configuration Management.

2. Only mobile and BYOD computing devices approved by Information Management and Services (IMS) may be used to connect to the UTHSA network

infrastructure or used to create, store or transmit Confidential or Mission Critical Data.

a. IMS may grant approval to an explicit User or blanket approval for device hardware type, configuration or function.

b. The Chief Information Security Officer may issue an exemption to explicit or all policy statements for use of applications or services that synchronize data in a secure manner.

3. When using a mobile or BYOD computing device to access the UTHSA network infrastructure or to create, store or transmit Confidential or Mission Critical Data, Users shall:

a. acknowledge Acceptable Use and Privacy Rights explicit to the use of the mobile or BYOD device;

b. ensure device configuration minimally meets UTHSA policies and standards;

c. enable password authentication to access device content or perform functions;

i. all passwords must be saved in an encrypted password store;

ii. mobile device passwords must contain a minimum of four (4) characters; and

iii. mobile device access must time-out after no more than five (5) minutes of inactivity.

d. encrypt UTHSA Data stored on the device in compliance with UTHSA policies and standards;

e. only load data essential to their role onto their device;

f. immediately report all lost or stolen devices or suspicion of unauthorized access or disclosure in compliance with UTHSA policies, standards and procedures;

g. not install unlicensed software or illegal content onto the device and only install software from University or platform-owner approved sources;

h. not disable operating system security features (“jailbreak”) or bypass UTHSA security controls;

i. install all operating system security patches and updates in a timely manner;

j. run anti-malware software if supported by the device’s operating system;

k. not synchronize or backup UTHSA Confidential or Mission Critical Data to personal Cloud services;

l. be cautious about merging of personal and UTHSA email accounts on the device;

i. Users may not use personal email addresses to send University communication;

ii. UTHSA Data must only be sent through an email account or other file transfer method approved and provisioned by the University.

m. use the UTHSA approved secure remote access methods, such as Virtual Private Network (VPN) or Secure Sockets Layer (SSL) and two-factor authentication when remotely connecting to Information Resources;

n. ensure effective physical security protection when storing or leaving the device unattended; and

o. securely delete UTHSA Data upon termination of access rights to the Data.

4. To minimize risk of mobile and BYOD devices accessing or storing UTHSA Information Resources, Information Management and Services shall:

a. define baseline security hardened standards for each approved device and/or operating system;

b. enforce device access authentication, data encryption and synchronization standards;

c. monitor and report on the security configuration state of all mobile and BYOD devices;

IMS may disable or restrict access to devices that demonstrate suspicious or abnormal behavior, deemed vulnerable to attacks or breach or assessed as not conforming to UTHSA policies and standards.

d. immediately revoke access or synchronization for terminated Users and force deletion of UTHSA Data; and

e. maintain documentation of authorized mobile devices.

IV. Definitions

When used in this document, the following words have the meaning set forth below unless a different meaning is required by context.

BYOD – "Bring Your Own Device," indicative of a personally owned device as opposd to an institutionally owned device.

V. Related References

There are no related documents associated with this Policy.

VI. Review and Approval History

A. The approving authority of this policy is the University Executive Committee.

B. The review frequency cycle is set for three years following the last review date, a time period that is not mandated by regulatory, accreditation, or other authority.

Effective Date	Action Taken	Approved By	Date Approved
06/2000	Policy Origination		
06/2018	Policy Revision		
02/2023	Policy Review/Discretionary Edits		