Chapter 5	Information Management & Services	Effective:	June 2000
Section 5.8	Information Security	Revised:	October 2016
Policy 5.8.12	**Mobile Device And Personally Owned Computing Policy**	Responsibility:	Chief Information Security Officer

MOBILE DEVICE AND PERSONALLY OWNED COMPUTING POLICY

Policy

UT Health San Antonio shall adopt and document standards and procedures to manage mobile computing devices and personally owned computing devices ("Bring Your Own Device" or "BYOD") that may connect to the UT Health San Antonio 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 UT Health San Antonio are exempt from this policy and must comply with all other UT Health San Antonio policies and standards.

2. Only mobile and BYOD computing devices approved by Information Management and Services (IMS) may be used to connect to the UT Health San Antonio network infrastructure or used to create, store or transmit Confidential or Mission Critical Data.

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

    - 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 UT Health San Antonio 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 UT Health San Antonio 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 five (5) minutes of inactivity

d. encrypt UT Health San Antonio Data stored on the device in compliance with UT Health San Antonio policies, standards and procedures;

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 UT Health San Antonio policies, standards and procedures;

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

h. not disable operating system security features ("jailbreak") or bypass UT Health San Antonio 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 UT Health San Antonio Confidential or Mission Critical Data to personal Cloud services;

l. be cautious about merging of personal and UT Health San Antonio email accounts on the device;

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

- UT Health San Antonio Data must only be sent through an email account or other file transfer method approved and provisioned by the University.

m. use the UT Health San Antonio 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 UT Health San Antonio Data upon termination of access rights to the Data.

4. To minimize risk of mobile and BYOD devices accessing or storing UT Health San Antonio 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 UT Health San Antonio policies and standards.

d. immediately revoke access or synchronization for terminated Users and force deletion of UT Health San Antonio Data; and

e. maintain documentation of authorized mobile devices.