## Purpose

This document outlines requirements for Bring Your Own Device (BYOD) usage and establishes the steps that both employees and the Information Technology department should follow to support, and certify devices for University business. These requirements must be followed as documented to protect University systems and data from unauthorized access or misuse.

It is ***REQUIRED*** that employees use their University issued device for ***ALL*** University business.

## Scope

This document covers all full-time and part-time employees (including student workers and graduate students), contract workers, consultants, temporary workers, and other personnel granted access to University systems, networks, software, and/or data.

## Protecting University Data

As an employee of the University you need to be aware of the types of data that you need to protect. Misuse or exposure of this data can lead to damage to the University's reputation, loss of funding and fines.

Some types of data you need to protect are (but not limited to):

- Social Security Numbers
- Credit Card Numbers
- Student Records (Any combination of data that allows identification of student – Grades, DOB…)
- Protected Health Information (Any health related information, medical conditions, diagnoses…)
- Controlled Research Information

Always follow the rule: **If in doubt, protect it.**

## Equipment

Equipment covered by this document includes (but is not limited to) ***PERSONALLY*** owned:

- Desktops, laptops, and tablet computers
- Smartphones (defined as any cellular telephone that connects to the internet via Wi-Fi or a mobile provider network)
- Flash, memory, and/or thumb drives
- External hard disks
- Entertainment and gaming consoles (Xbox, PS3, Wii, DS3, etc.) that connect to Wi-Fi networks and are used to access University email and systems

## University Supplied Software

Subject to each software specific Licensing Agreement, ***University Supplied Software*** will **NOT** be installed on any personal device, even if the employee states they use the device for University business and that the device has been approved for University business by the COO and CIO.

University personnel should be using their University issued computing device for University Business.

Software for use on a personal computer can be purchased from software.tamu.edu or the vendor of the software. Software availability from software.tamu.edu is dependent on the employee's eligibility.

## Personal Devices – excluding smartphones

If a staff or faculty member wishes to use their personal device for University Business they must provide a ***Business Use*** justification as to ***why their UNIVERSITY ISSUED DEVICE will not meet the requirements for them to carry out their daily activities***. This request needs to be approved by the Chief Information Officer (CIO) and the Chief Operating Officer (COO). Refer to the "IT Security Exception Request" form.

Undergraduate and Graduate students working for the University MAY USE their personal device for University business provided it is certified by the Information Technology Department that it has the necessary compensating controls listed below.

If the personal device is approved, the owner ***ACCEPTS*** that using their personal device for University Business makes that personal device subject to the University's "Privacy Rule" as stated in this document in the Privacy section, and they accept responsibility for any University data stored on that device. They also accept their device will be subject to the open records request policy in accordance with the Public Information Act and be searchable if requested.

## Compensating Controls

Compensating control measures will need to be in place as part of the approval process to show how the device will be protected and how it will protect University data from misuse or compromise. At a minimum the device will need to have:

- End point Protection installed
- Be password protected with a strong password or other strong protection method
- Where supported, be encrypted
- Have up to date software and security patches installed
- Where supported, have a screen lockout timer

Contact helpdesk@tamug.edu if you need assistance with the compensating controls.

## BYOD Certification Process

Undergraduate and Graduate students employed by the University using their personal devices for University business will need to get it certified by the IT Department that it has the necessary compensating controls in place by doing the following:

- Bring the device to the IT Helpdesk during normal business hours (CLB Room 113) (Also bring any external hard drives or USB drives used for storing University data so we can assist in encrypting these devices)
- Complete the BYOD Certification Form
- IT staff will verify the compensating controls are in place and sign the form or assist in putting the controls in place when possible
- The device owner will sign the form which states they will abide by the "User Responsibilities" stated in this document
- The device owner agrees to recertify the device annually

## User Responsibilities

These responsibilities apply to any ***Approved*** Personal Devices.

- The employee is responsible for any and all University data saved to their personal device. Using a personal device DOES NOT remove the user from the responsibility to protect University data.
- The employee should not attempt to change or disable any security settings applied to the device by the Information Technology department.
- In the event that an employee believes a personally owned device that is authorized to connect to the University's resources, systems, or networks might be compromised, they must immediately notify the Information Technology department of the potential security risk.
- If an employee loses or misplaces a personally owned device that is authorized to connect to the University's resources, systems, or networks, they must immediately notify the Information Technology department of the potential security risk.
- Whenever an employee decommissions, prepares to return, or otherwise ceases using a personally owned device that is authorized to connect to the University's resources, systems, or networks, the employee must notify the Information Technology department that the device will no longer be used to connect to University resources, systems, or networks.

## University Email

Checking of University email from a web browser on a personal device is allowed, however, downloading or saving documents from University email to your personal device should be avoided to limit any potential exposure of University data.

## Smartphones

Personally owned smartphones can be used for University Business, specifically University Email, provided the following has been applied to the device:

- PIN/ Password Lock Screen function applied
- Device Location and Remote Wipe function enabled where supported

Personal smartphones used for University business are subject to the University's "Privacy Rule" as stated in this document in the Privacy section, and the user accepts responsibility for any University data stored on that device. They also accept their device will be subject to the open records request document in accordance with the Public Information Act and be searchable if requested.

Refer to your smartphone manufacturer's website for information on activating these features.

## Privacy

By requesting and receiving approval to use a personal device for University Business you are agreeing to the privacy terms as stated in this document and University SAP 29.01.03.M1.17 Information Resources – Privacy.

The University has the right to examine information on information resources which are under the control or custody of the University. The general right to privacy is extended to the electronic environment to the extent possible. However, there should be no expectation of privacy beyond that which is expressly provided by applicable privacy laws. Privacy is limited by the Texas Public Information Act, administrative review, computer system administration, and audits.