Information Technology BYOD Certification Form

Information Technology: 409 740 4714, helpdesk@tamug.edu

This form certifies a personal device used by an Undergraduate or Graduate Student worker meets the necessary compensating controls to protect University data and is certified for use for University business.

Compensating Controls

Compensating control measures will need to be in place as part of the certification 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
- External hard drives and USB drives are encrypted

Complete in Person or Email completed signed form to helpdesk@tamug.edu.

Requestor Information

Name: _____ Date: _____

UIN: _____

Phone: _____ Email: _____

Title: _____

Dept: _____

Bldg: _____ Room: _____

Supervisor: _____

Device Information:

Make: _____

Model: _____

Serial or Service Tag Number: _____

Created: 3/12/2021

Information Technology BYOD Certification Form

Information Technology: 409 740 4714, helpdesk@tamug.edu

Business Justification: Describe the business reason for using your personal device.

Data Sensitivity: Describe what type(s) of data will be hosted on the machine. Do not just list the data definitions. Examples: grades, research data. Refer to TAMU Data Classification for definitions. TAMU Data Classification

User Responsibilities

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

- The owner 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 owner should not attempt to change or disable any security settings protecting the device.
- In the event that the owner 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 the owner 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 the owner ceases employment, 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 owner must notify the Information Technology department that the device will no longer be used to connect to University resources, systems, or networks.

By signing this document I am agreeing to implement any compensating controls required to protect University data from misuse and unauthorized access and abide by the user responsibilities:

Requestor Signature: Date:

Information Technology BYOD Certification Form

Information Technology: 409 740 4714, helpdesk@tamug.edu

TEXAS A&M UNIVERSITY
GALVESTON CAMPUS

Information Technology Internal Use Only

End Point Protection Installed? Yes ☐ No ☐ Vendor: _____

Password Protected? Yes ☐ No ☐

Screen Lockout Timer? Yes ☐ No ☐

Encrypted Hard Drive? Yes ☐ No ☐

Security Updates Installed? Yes ☐ No ☐

Automatic Updates On? Yes ☐ No ☐

USB / External HDD encrypted? Yes ☐ No ☐

Computer Name: _____

MAC Address: _____

IT Technician Name: _____ Date: _____

Incident Number: _____

ISO Approval: _____ Date: _____

Created: 3/12/2021