Lebanese American University

Information Security Regulations

Bring Your Own Device Regulations

Last Updated: March 2017
Version 1.2

Overview

With the mass use of user's own devices at the university, users are using their own devices to access sensitive and critical LAU data. Insecure personal devices can provide an easy open door for security threats.

Purpose

The Bring Your Own Device (**BYOD**) regulations address the current controls that are required to maintain information security when employing portable devices that are not owned by LAU.

Scope

These regulations apply to all LAU staff, faculty and partners who use their personal owned devices (**POD**) to perform LAU business functions.

Regulations

Verification of Approved PODs

Users must not use PODs to process any LAU information which is not classified as publicly available until the requirements for security operation have been met and verified.

Device Wipe at Termination

All LAU information must be deleted or wiped off from an employee's or third party's POD upon termination of employment or contract.

Jailbroken and Rooted Devices

Jailbroken or rooted devices must not be used to connect to any LAU computer or communications system.

Mobile Devices Containing Sensitive Information

All Faculty and Staff PODs containing sensitive LAU information must consistently employ encryption for all such files, and wherever possible, startup and strong screen-saver-based password/boot protection.

Information Separation

All personal information stored on a POD must be kept in a location on the device that does not also contain LAU information.

Personal Information Restriction

Personal information stored on a POD must not be transferred to any LAU computer or communications system.

Ownership of Information Stored in POD

All LAU information stored in a POD is LAU property and can be inspected or used in any manner at any time by LAU after securing the approval of the President.

Storage of Remote Access Information in POD
Users must not store remote access information, e.g., fixed passwords, user IDs, in their POD, or in the device case in which their POD is stored or used for transport.

Lending POD Containing Sensitive Information
A POD used for business activities that contains LAU sensitive information must not be lent to anyone.

Image Capture - Information
Employees and partners must not use the video or still camera features on any PODs, including smartphones and tablet computers to capture images that may depict confidential LAU information, including but not limited to documents, computer displays and output.

Image Capture - Facilities
Employees and partners must not use the video or still camera features on any PODs, including smartphones and tablet computers to capture images within any LAU secure area, including but not limited to areas where proprietary procedures are performed, proprietary devices or equipment are used, or non-public information is processed, stored, or transmitted.

Personnel Responsibility
Users must keep PODs used for business activities in their possession at all times unless they have been deposited in a secure location such as a locked closet or a hotel safe. Under no circumstances should PODs be left in open view on desks, in a vehicle, or in public areas.

Hardware
Each POD must be fully maintained by the owner of the POD, i.e., LAU provides no assistance or services for PODs, which includes but is not limited to repairs, upgrades and replacements.

Software
All POD software, including but not limited to the operating system and communication applications, must be maintained with the most recent release, patches, and updates by the POD owner.

Antivirus Protection
Each POD owner must ensure that their device is equipped with LAU approved antivirus software and that this software is maintained with the most recent release, patches, and updates.

Separate Password for Portable Devices
LAU users must not use the same password for a POD that is used for accessing LAU network, devices and applications.

Immediate Reporting Lost Devices
All LAU personnel must immediately report lost or stolen PODs used for business activities to their immediate supervisor and the IT Helpdesk to proceed with the wipe off procedure.

Device Quarantine
Any POD found to be out of compliance with LAU policies and regulations must be quarantined from the network until all deviations are corrected and validated.

PODs Supported
All LAU's services will only be supported on specified Pods listed on the following link "http://it.lau.edu.lb/services/bring-your-own-device.php".

Number of PODs connected per User
The maximum number of concurrently connected PODs per user is as follows:
1 device per alumni

2 devices per student
3 devices per faculty/staff
1 device per guest

Off-Site Systems Damage or Loss

Users must promptly report to their supervisors any damage or loss of LAU device that has been entrusted to their care. In case of theft, they should also obtain a report from the police where the theft occurred.

Wireless Guest Account Request

For the creation of a wireless guest account, a request should be sent by email to the IT Helpdesk from a Full-Time faculty or staff. The approval should be secured based on the life duration of the account as follows:

- less than 3 mounts, approval of the Director/Chairperson
- greater than 3 months, approval of the Dean/AVP

Definitions

Jailbroken Device: An iOS smartphone or tablet computer which has been reconfigured to permit user access to the root level of the operating system.
Mobile Device: Any portable computing device used to access, process, transmit, or store information, e.g., laptops, smartphones, e-readers, tablet computers, which is used for LAU business purposes.
Partner: Any non-employee of LAU who is contractually bound to provide some form of service to LAU.
Personally-Owned Device (POD): Any device not owned by LAU used to access, process, transmit, or store information, e.g., smartphone, e-reader, tablet computer, notebook computer, which is used for LAU business purposes.
Rooted Device: An Android smartphone or tablet computer which has been reconfigured to permit user access to the root level of the operating system.