Lebanese American University

Information Security Regulations

Wireless Regulations

Last Updated: April 2017
Version 1.2

Overview

With the mass use of notebooks, smart phones and tablets, wireless network is almost a given at any organization. Insecure wireless configuration can provide an easy open door for malicious threat actors.

Purpose

LAU grants wireless access to the community to meet LAU's missions, goals and initiatives. Thus the University must manage the wireless infrastructure in a way to maintain the confidentiality, integrity and availability of all information assets. These regulations specify the conditions that wireless infrastructure devices must comply to.

Scope

All employees, contractors and consultants at LAU who maintain, configure and implement the wireless infrastructure devices should adhere to these regulations. These regulations apply to all wireless infrastructure devices that are connected to LAU network.

Regulations

Physical Security For Wireless Access Points

To prevent tampering, reconfiguration, theft, and other unauthorized activity, all wireless network access points must be physically secured and accessible only by authorized personnel.

Wireless Network Gateways

The LAU wireless network must always be in dedicated secure VLANs. A secure connection should be established when a user needs to connect to LAU's network to access systems and services via wireless.

Wireless Network Installation, Configuration And Administration

All wireless access points must be installed, configured and administered by an authorized member of the LAU Network and Telecom Department or authorized contractors.

Unauthorized Wireless Access Point Broadcasting LAU's SSIDs

LAU IT Network Department should always scan for unauthorized wireless access point broadcasting LAU's SSIDs and stop them using proper tools and solutions.