Lebanese American University

Information Security Regulations

Computer and Network Regulations

Last Updated: April 2017
Version 1.2

Overview

LAU grants computing devices and networking infrastructure to qualified users (faculty, staff, students, guests …). Users are responsible for the protection of LAU physical and data assets. Thus the computing devices and the networking resources should be handled and used in a secure manner.

Purpose

The computer and network regulations define the information security-related requirements for the use of LAU computers, laptops, devices and network.

Scope

The computer and network regulations apply to all users using LAU devices or network.

Regulations

Personal User IDs Responsibility

Users are responsible for all activity performed with their personal user IDs. They must not share their users IDs and passwords with others and must not permit others to logon with their user IDs, and they must not perform any logon with IDs belonging to other users. If you have suspicious that your account has been compromised, reset your password immediately.

Typing Passwords When Others Are Watching

Users must never type their passwords at a keyboard or a telephone keypad if others are known to be watching their actions. To do so unduly exposes the information accessed thereby to unauthorized access.

Unattended and Idle Machines

Users must not leave their personal computer, workstation, or terminal unattended without logging out or invoking a password-protected screen saver. Any machine that is idle for 10 minutes must be automatically switched to screen saver mode with password protection.

Positioning Computer Display Screens

The display screens of all personal computers, workstations and terminals must be positioned such that they cannot be readily viewed through a window, door, by persons walking in a hallway, or by persons in any public areas.

Hacking Activities

Users must not engage in hacking activities in/from LAU that include, but are not limited to:

(a) gaining unauthorized access to any information systems,

(b) damaging, altering, or disrupting the operations of any information systems, and

(c) capturing or otherwise obtaining passwords, encryption keys, or any other access control mechanism that could permit unauthorized access.

File and Message Ownership

LAU has legal ownership of the contents of all files and messages stored or transmitted on its computer and network systems, and reserves the right to access this information without prior notice whenever there is a business need after the approval of the President.

Software Installation and Upgrade

Users must not install or upgrade software on their personal computers except if needed for business use and after obtaining approval of the concerned supervisor. All software listed in http://it.lau.edu.lb/services/software-and-applications-support.php are supported by the IT department.

Most Recent Software Release

All LAU production operating systems, database management systems, firewalls, routers, switches and related systems software, and all production business applications software, must be kept at a non-vulnerable state.

User Processes, Sessions, And Files

LAU system administrators may, without notice, alter the priority of, or terminate the execution of, any user process that he/she believes is consuming excessive system resources or is significantly degrading system response time, terminate user sessions or connections if this usage is deemed to be in violation of security policies.

AntiVirus Software Installation

Virus screening software must be installed, enabled at all times and configured to run a full scan once a week on all LAU's servers, desktops and laptops, where applicable, by the IT Support Department. AntiVirus software should be activated once servers, desktops and laptops are powered up and should be kept up -to-date. All foreign and removable media must be scanned automatically upon connection.

Involvement with Computer Viruses

Users must not intentionally write, generate, compile, copy, collect, propagate, execute or attempt to introduce any computer code designed to self-replicate, damage or otherwise hinder the performance of any LAU computer or network.

Eradicating Computer Viruses

Any user who suspects infection by a virus must immediately unplug the network cable from the computer, call the IT Help Desk, and make no attempt to eradicate the virus.

Personal Computer and Workstation Firewalls
All personal computers and workstations that connect to the Internet must have their own firewalls (approved by the IT Security Department) installed and continuously enabled

Exploiting Systems Security Vulnerabilities
Users must not exploit vulnerabilities or deficiencies in information systems to damage systems or information, to obtain resources beyond those they have been authorized to obtain, to take resources away from other users, or to gain access to other systems for which proper authorization has not been granted. Users should report vulnerabilities to the IT Helpdesk.

Testing Information System Controls
Users must not test, or attempt to compromise security controls unless this activity is specifically approved in advance, and in writing, by the IT Security Department.

Systems Security Testing Tools
LAU users must not use hardware or software tools that could be employed to evaluate or compromise information systems security, unless specifically authorized by the IT Security Department. Examples of such tools include those which defeat software copy protection, discover secret passwords, identify security vulnerabilities, or decrypt encrypted files.

Disabling Critical Security Components
Critical components of LAU information security infrastructure (firewall, IDS, access control, antivirus, web filtering ..) must not be disabled, bypassed, turned off, or disconnected.

No Accommodation to Support Peer-To-Peer File Sharing Software
No changes may be made to firewalls, virus screening systems, or any other systems software to accommodate peer-to-peer software.

Equipment Maintenance
All information systems equipment used for production processing must be maintained in accordance with the supplier's recommended service intervals and specifications, with all repairs and servicing performed only by qualified and authorized maintenance personnel

Power Conditioning Equipment
With the exception of all mobile devices, all personal computers and workstations must be outfitted with uninterruptible power supply (UPS) systems

Computer System Names
The function performed by a computer or the software that it runs must not be used in any part of the computer's name or its alias.

Internet Domain Name and Host Name Approval Process
Every Internet host computer name and every Internet web site name, which is run or owned by LAU, must be approved in advance of its use by the IT Department.

Blocking Access to Web Sites

As a standard business practice, to encourage the productive use of the Internet, LAU routinely uses software which blocks users from visiting those Internet sites which management considers to be objectionable or clearly personal in nature. These include, but are not limited to, racist sites, hate sites, gambling, gaming and pornographic sites. Management may, at any time, without notice, update the list of prohibited web sites.

Internet Access

All Internet access from systems connected to the LAU networks must be routed through a firewall.

Known Identities

All accounts having the privilege to logon to LAU systems should be linked to known users.