Lebanese American University

Information Security Regulations

Awareness Regulations

Last Updated: May 2017
Version 1.2

Overview

Users should have a basic security awareness knowledge concerning the protection of LAU physical and data assets. The IT Security department is in charge of delivering the basic knowledge and information needed for the users to handle LAU assets (physical and data) in a secure manner.

Purpose

The awareness regulations define the information security-related requirements for awareness and training given to all users at LAU with access to LAU information systems.

Scope

The awareness regulations apply to all users who have access to any physical and data assets at LAU.

Regulations

Information Security Responsibility

Security information on a day-today basis is a collective effort between IT and users, accordingly all users should be aware and follow all items in the IT Security Policy and Regulations.

Use of Information

University information must be used only for the business. Information is a critical and vital asset, and all accesses to, uses of, and processing of, University information must be consistent with LAU policies, regulations and standards.

Information Security Policy and Regulations

On or before their first day at LAU, all new faculty, staff and students must be made aware that they must comply with the information security policy and regulations.

Specification of Minimum Information Security Awareness

The IT Security Department must provide awareness raising requirements for all users who have access to LAU information systems.

Information Handling, Access, And Usage

Information is a critical and vital asset, and all accesses to, uses of, and processing of, University information must be consistent with LAU policies, regulations and standards.

Training Responsibility

The IT Security Department must provide courses or other materials to refresh the users knowledge with respect to information security.

Information Security Regulations Changes

All LAU users must receive prompt notice of changes in the LAU information security regulations, including how these changes may affect them, and how to obtain additional information.

Accepting Security Assistance from Outsiders

Users must not accept any form of assistance to improve or change the security of their computers without first having the provider of this assistance approved by the LAU IT Security Department. This means that users must not accept offers of consulting services, must not download security software via the Internet, and must not employ security posture evaluation web pages, unless the specific provider of the assistance has been previously approved.

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, by persons walking in a hallway, or by persons in any public areas.

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.

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.

User Access Capabilities

Users must not read, modify, delete, or copy a file belonging to another user without first obtaining permission from the owner of the file.

Information Security Pranks

Users must not play practical jokes, engage in pranks, or otherwise humorously make it look like a security incident is taking place, will take place, or has taken place when this is not true.

Incident and Violation Reporting

All suspected information security incidents and violations must be reported as quickly as possible through the IT Help Desk.

Eradicating Computer Viruses

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

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.

Hacking Activities

Users must not use any information system to 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

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

(d) social engineering

(e) phishing

(f) ransomware

Internal Network Addresses

The internal system addresses, configurations, and related system design information for LAU networked computer systems must be restricted such that systems and users outside the LAU internal network cannot access this information.

Off-Site Systems Damage and Loss

Users must promptly report to their supervisor any 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.