Lebanese American University

Information Security Regulations

Virus and Malicious Codes Regulations

Last Updated: April 2017
Version 1.2

Overview

The virus and malicious codes are software that execute without the acceptance or the knowledge of the user, creating threats for the confidentiality, integrity and availability of data across the institution. Effective implementation of these regulations will limit the exposure and effect of common malware and virus threats to the systems they cover.

Purpose

The virus and malicious codes regulations define the requirements for controls to prevent and detect the dissemination of any malicious software or virus on LAU computer and communications systems

Scope

The virus and malicious codes regulations apply to all devices where applicable, that have access to LAU network.

Regulations

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.

Multiple Virus-Screening Packages

At least two virus and malware screening software packages must be used where electronic mail and other files enter the LAU network.

Antivirus Software Updates, Scans and Logs

All antivirus programs deployed on LAU computer and communications systems must be configured to accept automatic updates of the software, periodically scan all systems for viruses and malware and log all antivirus activity.

Downloaded Information

All software and files downloaded from non-LAU sources through the Internet or any other public network must be screened with virus detection software prior to the software being executed or the files being opened.

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.

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.