Lebanese American University

Information Security Regulations

IT Security Department Regulations

Last Updated: June 2017
Version 1.2

Overview

The IT Security Department is responsible to develop and communicate guidance to preserve the confidentiality, integrity and availability of the University's electronic assets.

Purpose

The purpose of these regulations is to describe the role of the IT Security Department to keep LAU assets (physical and data) secure and maintain its confidentiality, integrity and availability.

Scope

These regulations apply to all IT security staff.

Regulations

Decision Maker On Information Security Matters

The IT Security Department is the reference on all matters relating to information security at LAU. This department is charged with orchestrating and coordinating information security across the organization. All information security matters must consistently comply with the IT Security regulations unless a risk acceptance process has been successfully completed.

Information Security Department Mission

The Information Security Department is responsible for the prevention of serious loss or compromise of critical, valuable, and sensitive information resources at LAU by coordinating and directing specific actions that will provide a secure and stable information systems environment consistent with LAU goals and objectives.

IT Security Regulations and Procedures

IT Security Department must publish written Information Security Policy, Regulations, Guidelines and Procedures and make them available to all users online. Those documents must be reviewed, maintained and updated on an annual basis. The various versions must be preserved for a period of at least ten years.

IT Security Department Tasks

The IT Security Department must provide the direction and technical expertise to ensure that LAU's information is properly protected. This includes consideration of the confidentiality, integrity, and availability of both information and the systems that handle it. The department will act as a liaison on information security matters between all LAU departments and divisions for all information security activities throughout LAU. The Department must perform risk and vulnerability assessments, prepare action plans, participate in evaluating vendor products, the information security and data privacy requirements in in-house system development projects, assist with control implementations, investigate information security breaches, conduct awareness programs, and perform other activities which are necessary to assure a secure information handling environment.

Computer Security Incident Response Team

The IT Security Department must organize and maintain an in-house Computer Security Incident Response Team (CSIRT) that will provide accelerated problem notification, damage control, and problem correction services in the event of computer related emergencies such as virus infestations and hacker break-ins.

Production System Risk Assessments

All production computer information systems must be periodically evaluated by the IT Security Department to determine the minimum set of controls required to reduce and maintain risk at an acceptable level.

Annual Information Technology Risk Report Required

The IT Security Department must submit to the AVPIT a special annual report. This report must include a description of all LAU information technology related risks, an assessment of how these risks are currently being managed and a list of all exceptions during that year.

System Log Review

The IT Security Department must review records reflecting security relevant events on all IT resources on daily basis.