Lebanese American University

Information Security Regulations

Data Centers Regulations

Last Updated: May 2017
Version 1.2

Overview

The Data Center is a critical place where all LAU servers and systems reside. The following regulations must be implemented to maintain and operate the Data Centers in a secure environment.

Purpose

The data center regulations describe how the data centers should be managed and maintained.

Scope

The data center regulations apply to all data centers operated and maintained by IT at LAU.

Regulations

Data Center Construction

New and remodeled LAU data centers must be constructed so that they are protected against fire, water damage, vandalism, and other threats known to occur, or that are likely to occur at the involved locations. All data centers must be equipped with alarm systems that automatically alert those who can take immediate action.

Data Center Environmental Controls

The Campus Operations and Maintenance Department must provide and adequately maintain fire detection and suppression, power conditioning, air conditioning, humidity control, and other computing environment protection systems in every LAU data center. Those controls should be monitored and provide notifications in case limits are exceeded.

Redundant Utility Suppliers

All LAU data centers must have redundancy on the following:

- Mechanical cooling system
- Electrical power system
- UPS system
- Data communications connections

Physical Access Control To Data Centers

Access to Data Centers must be physically restricted to personnel with legitimate business need.

Data Center Infrastructure

LAU must segment its data processing centers into minimum two distinct and physically isolated data centers, each able to handle all critical production information systems services.

CCTV monitoring
LAU Data Centers should be monitored by CCTV.

Access Control System Records
The IT Department must maintain a logging system of all personnel who access Data Centers and securely retain this information for at least one year.

Escorts Required For All Visitors To Data Centers
Authorized visitors to Data Centers must be escorted by the concerned employee in the IT or Facilities Management Departments whenever they are in the Data Centers.

Data Center Staff Access
A complete list of all employees who are currently authorized to access the data centers must be maintained, reviewed, and updated by the Network, Telecom & Multimedia department on a quarterly basis.

Smoking, Eating, And Drinking
Employees and visitors must not smoke, eat, or drink in the data centers.

Securing Propped-Open Data Center Doors
Whenever doors to the data center are propped-open, the entrance must be continuously monitored by an employee or a guard from the Physical Security Department.

Data Centers Door Closing
Data Centers doors must automatically close immediately after they have been opened. An audible alarm must set off when they have been kept open beyond 2 minutes.

IT Resources Location
All core IT resources including, but not limited to, servers, firewalls, LAN systems, WAN systems, Network devices and voice mail systems must be physically located within secure data centers.