Lebanese American University

Information Security Regulations

Virtual Server Regulations

Last Updated: April 2017
Version 1.2

Overview

LAU deploys virtual server technologies to save on operational costs of managing large data centers. These regulations are designed to help minimize some of the common risks of virtual server environments. While virtualization provides many operational benefits, it also creates additional risks due to the unique feature of combining multiple operating systems and applications into one physical server. These risks may include:

- Proliferation of unknown Virtual Machines (VM).
- Physical access to machine host exposing multiple VMs to copying or theft.
- Mixed classification of data and systems within VMs.
- Vulnerability of one VM leads to another (guest hopping attack).
- Vulnerability of the virtual infrastructure to attacks.

Purpose

LAU uses virtualization technology to help reduce the cost of IT operations and increase the overall efficiency of the organization. The virtual server regulations describe internal controls used to reduce the information security risks common in virtual server environments.

Scope

The virtual server regulations apply to employees, contractors, consultants, and other users within the LAU IT Department managing the virtual server environments.

Regulations

Training Required

All LAU users involved in the implementation and management of the virtual server environments must take training on the security risks of virtual server environments.

Physical Access Controls

All LAU servers running virtual environments must have strong physical access controls and be in secure areas with access restriction.

External Ports Disabled

All LAU servers running virtual machines must have external data ports (USB, CD-RW, …) disabled to prevent unauthorized copying, exceptions will be treated on case by case after securing the approval of the director concerned.

Periodic Scanning

All virtual machines operating within LAU must be periodically scanned for vulnerabilities.

Standardized Virtual Machine Software

In order to reduce vulnerabilities and the effort required to patch systems, LAU must adopt a limited best of breed virtual machine software.

Virtual Server Software Updates

LAU must be running the latest stable version of the virtual machine software for each production virtual environment. Administrators must assess each available patch update to the virtual machine software within 30 days of its release by vendors. Patches deemed critical must be installed within 45 days.

Backup Over Secure Channels Only

System backups for all servers running virtual machines must run over a secure protocol. Virtual machines are stored in files than can easily be copied if intercepted by a hacker.