Lebanese American University

Information Security Regulations

Servers Regulations

Last Updated: April 2016
Version 1.1

Overview

Unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent server installation policies, ownership and configuration management are all about doing the basics well.

Purpose

The purpose of the servers regulations is to establish standards for the base configuration of internal server equipment that is owned and/or operated by LAU IT Department. Effective implementation of these regulations will minimize unauthorized access to LAU proprietary information and technology.

Scope

All employees, contractors, consultants and other users that have access to LAU servers must adhere to these regulations. These regulations apply to servers owned, operated and administered by LAU IT Department.

Regulations

System Administrators Roles

All internal servers deployed at LAU and fall under the IT Department umbrella must be managed by system administrators that are responsible for system administration. System administrators should monitor configuration compliance and implement an exception policy tailored to their environment. Each system administrator must establish a process for changing the configuration guides, which includes review and approval by IT Security Department. The following items must be met:

- Servers must be registered in the IT servers and devices inventory. At a minimum, the following information is required to positively identify the point of contact:
    - Server contact(s) and location, and a backup contact
    - Hardware and Operating System/Version
    - Main functions and applications
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures

Audit and Compliance

For security, compliance and maintenance purposes, IT Security Department must monitor and audit equipment, systems and processes.

Configuration Requirements.

- Operating System configuration should be in accordance with approved Operating System Configuration guidelines.
- Services and applications that will not be used must be disabled where applicable.
- Access to services must be logged and/or protected through access-control methods such as a web application firewall, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.
- Always use standard security principles of least required access to perform a function. Do not use root or administrator when a non-privileged account will do.
- Access to the servers must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled areas.

Monitoring Requirements

All security related events and audit trail should be enabled, logged and forwarded to a centralized management log solution. IT Security Department should monitor the logs and report security incidents to the Director of IT Security.