Lebanese American University

Information Security Regulations

IT Staff Regulations

Last Updated: March 2017
Version 1.2

Overview

The IT staff are responsible for managing the University IT resources and should utilize these resources in an ethical and lawful manner.

Purpose

The purpose of the IT Staff Regulations is to manage LAU assets (Physical or Data) in a secure manner while maintaining its confidentiality, integrity and availability.

Scope

These regulations apply to all LAU IT Staff.

Regulations

Security Changes After System Compromise

Whenever a system has been compromised, or suspected of being compromised by an unauthorized party, System Administrators must immediately reload a trusted version of the operating system and all security -related software, and all recent changes to user and system privileges must be reviewed for unauthorized modifications.

Integrity Assessment Tools

All Internet-connected systems used for production purposes must employ integrity assessment tools that compare hashes or digital signatures from critical files to hashes or digital signatures maintained on an off -line system on a daily basis.

Security Products And Services

All critical information security functions must be supported with best-of-breed, commercially-available products and services.

Non-Disclosure Agreements

All employees must personally sign an LAU non-disclosure agreement before work begins. If an employee has been working without a non-disclosure agreement, a signature must be provided as a condition of continued employment.

Revealing Information to Prospective Employees

Information systems technical details, such as network addresses, network diagrams, and security software employed, must not be revealed to job applicants until they have signed a confidentiality agreement and also have been hired or retained.

IT Department Ownership Responsibility
With the exception of operational computer, network, telecom and multimedia information, the IT Department must not be the Owner of any production business information.

Disclosure of Information System Controls
Employees must not disclose to any persons outside LAU either the information system controls that are in use or the way in which these controls are implemented without the permission of the AVPIT.

Security Weaknesses and Vulnerability Discussion
Users who discover a weakness or vulnerability in the information security measures used by LAU must escalate it to his/her director and the director should inform the IT Security Department.

Reuse of authentication credentials on public web sites.
LAU employees must never use their University internal network credentials (userid and password) on a public internet site which requires authentication.

Encryption Process Approval
Users are not permitted to employ encryption, digital signatures, or digital certificates for any LAU business activity or business information without the written authorization of their department head. Before they utilize these complex technologies, users must also be properly trained and their systems must be configured by authorized personnel.

Internet Web and Application Sites
A current digital certificate is required for every Internet server handling LAU applications where applicable.

Logon Information
When logging into an LAU computer or data communications system, if any part of the logon sequence is incorrect, the user must be given only feedback that the entire logon process was incorrect. Specific diagnostic feedback is prohibited.

Logon Banner Information
All logon banners on network-connected LAU computer systems must direct the user to log on, and must not provide any identifying information about the organization, operating system, system configuration, or other internal matters until the user's identity has been successfully authenticated.

Last Logon Time and Date
At logon time, every user must be given information reflecting the last logon time and date where applicable.

Secret User IDs or Passwords
Developers must not build or deploy secret user IDs or passwords that have special privileges, and that are not clearly described in the generally available system documentation.

Change Control Procedure
All significant changes to critical IT systems must be communicated through the IT Change Management Application.

Systems Administrators Install/Update Server Software
Only authorized Systems and Application Administrators are permitted to install and/or update software on LAU servers.

Systems Administrator User IDs
System administrators managing computer systems with more than one user must have at least two user IDs, one that provides privileged access and is logged, and the other that provides the privileges of a normal user for day -to-day work.

Circumventing Access Controls
Programmers and other technically-oriented staff must refrain from installing any code that circumvents the authorized access control mechanisms found in operating systems or access control packages.

Production and Development Separation
Critical business application software in development must be kept strictly separate from production application software.

Back-Off Procedures
Adequate back-off procedures, which permit information processing activities to quickly and expediently revert to conditions in effect prior to the most recent change in software, must be developed for all changes to production systems software and production application software where applicable.

Privilege Restriction — Need to Know
The computer and communications system privileges of all users, systems, and programs must be restricted based on the job need/task.

Internet Server Command Response
Internet servers must be modified so the verbose response to certain commands does not reveal information about the server software installed where applicable.

Only Widely-Deployed Information Systems Technology
LAU staff must not deploy information systems technology unless this same technology is widely -used, as well as generally accepted as stable, reliable, and fit for its intended purpose. Exceptions will be made only if purchase commitments are preceded by a risk assessment and the approval of the AVPIT.

Vendors Providing Mission Critical Hardware, Software, and Services

All LAU mission critical hardware, software and services must be purchased, rented, leased, or otherwise obtained from a trusted and well-established vendor who is able to provide both maintenance services as well as warranties.

Wireless Network Interfaces Disabled
Wireless network interfaces must be disabled on all LAU servers that handle production information.

Non-Disclosure and Confidentiality Agreements — Third Party
Prior to sending any secret, confidential, or private information to a third party for copying, printing, formatting, or other handling, the third party must sign LAU's non-disclosure and confidentiality agreements prepared by LAU's Legal Counsel. In addition to all LAU contractual agreements with third parties, all LAU RFPs and maintenance agreements must be accompanied by non-disclosure agreements. If LAU terminates its contract with any third-party organization that is handling LAU private information, this same third-party organization must immediately thereafter destroy or return all of the LAU private data in its possession.

Information Transfer to Third Parties
LAU software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-LAU party for any purposes other than those expressly authorized by VPHURS.

Third-Party User IDs
Individuals who are not employees, contractors, or consultants must not be granted a user ID or be given privileges to use LAU information systems unless the written approval of the concerned department head has first been obtained.

Third-Party Remote Access Limitations
Inbound Internet, or any other inbound access to LAU networks or systems must not be granted to third-party vendors unless the relevant department head determines that these vendors have a legitimate business need for such access. These privileges must not be provided unless they are enabled for specific individuals and only for the time period required to accomplish approved tasks.

Project Manager Notification Regarding Third Party Access
When third party access to LAU computers or networks is no longer needed for business purposes, the involved project manager within LAU must immediately notify the relevant Systems Administrators.

Disclosure of Third-Party Information
LAU employees must not disclose sensitive information that has been entrusted to them by third parties to other third parties unless the originator of the information has provided advance approval of the disclosure and the receiving party has signed an approved non-disclosure agreement.

Usage of a privilege account
If a privilege account should be used by non-privilege users for a specific job and for a specific time, a request should be sent to the director concerned to secure his/her approval, the credentials will be

given to the requester and at the end of the duration requested the password will be changed or the privilege account is disabled.

Network Central Point of Failure
The IT Department must design LAU communications networks so that no single point of failure could cause network services to be unavailable.

Network Ports Not in Use
All network ports not in use must be promptly disconnected at the wiring closet or at another centralized location.

Logical Isolation of Wireless Access Points
All wireless access points must be logically distinguished from the main LAU internal network.

Systems Network Access
Systems without the required software patches or systems that are virus-infested must be disconnected from the LAU network or routed to a quarantine network.

Security Configuration
Configurations and set-up parameters on all hosts attached to the LAU network must comply with LAU information security policy, regulations and standards.

Disable Vendor-Supplied Privileged User IDs
Before any production system is installed at LAU, technical staff must disable or rename all privileged user IDs such as those named “administrator,” “auditor,” or “installer.”

Clock Synchronization
All computers, servers and systems connected to the LAU internal network must always have the current time accurately reflected in their internal clocks synchronized with LAU's NTP server.

Request for Information
With the exception of data needed for day to day operations, data should never be delivered to end-users without securing the approval of the VP concerned, VPHRUS and the Legal Counsel.

Initial and Default Passwords
Initial and default passwords must be expired, forcing the user to choose another password before the next logon process is completed.