Lebanese American University

Information Security Regulations

Password Regulations

Last Updated: May 2017
Version 1.2

Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of LAU's resources. All users, including contractors, guests and vendors with access to LAU systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of the password regulations is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The password regulations apply to all users who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at LAU, has access to LAU's network, or stores any non-public LAU information.

Regulations

Password Structure

All passwords must conform to the Password Construction Guidelines and applied on all LAU resources where there is no hardware or software constraints.

Password Sharing

Passwords must not be shared with anyone. All passwords are to be treated as sensitive and confidential information.

Typing Passwords When Others Are Watching

Users must never type their passwords if others are known to be watching their actions. To do so unduly exposes the information accessed thereby to unauthorized access.

Writing Down Passwords

Users must not write their passwords down unless they have effectively concealed such passwords in seemingly unrelated characters or they have used a coding system to conceal the password.

Public Password Disclosure

Passwords must not be written down and left in a place where unauthorized persons might discover them.

Account Lockout

All LAU computer systems must be configured to permit only five attempts to enter a correct password, after which the user account is locked or temporarily locked, depending on the application, and can be unlocked by the Help Desk staff after authenticating the user’s identity.

Password Changes Performed By Involved User

Password changes and resets may be performed only by the involved user. Under no circumstances may a user delegate or otherwise request that another person handle this task on the user's behalf.

Passwords in Communications Software

Users must not store passwords in any communication programs, internet browsers, or related data communications software at any time (eg. vpn, ftp,…).

Password Encryption

Passwords must always be encrypted when held in storage for any significant period of time or when transmitted over networks.

Storage of Passwords in Readable Form

Passwords must not be stored in readable form in batch files, automatic logon scripts, software macros, terminal function keys, in computers without enforced access control mechanisms, or in other locations where unauthorized persons might discover or use them.

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.

Password Logging

Unencrypted passwords, whether correctly typed or not, must never be recorded in system logs.

Remember Password feature

Do not use the "Remember Password" feature of applications (for example, web browsers).

Required Password Changes

All faculty and staff users, system accounts and application accounts must be automatically required to change their passwords at least once every 120 days. A password can only be used after it has been changed four times.

Null Passwords Always Prohibited

At no time, may any System Administrator or Security Administrator enable any user ID that permits password length to be zero (a null or blank password).

Password Display and Printing

Users must enter passwords if and only if the display field is masked, suppressed or obscured so that unauthorized parties will not be able to observe or subsequently recover them.

Passwords Set To Expired After Intrusion

After either a suspected or demonstrated intrusion to an LAU computer system, the status of all passwords on that system must immediately be changed to expired, so that these passwords will be changed at the time that the involved users next log-in. Each user must immediately change his/her password if the password is suspected of being disclosed, or known to have been disclosed to an unauthorized party.