THE LeMoyne-Owen COLLEGE

LEADERSHIP. OPPORTUNITY. CHANGE.

LeMoyne-Owen College

AC5 - Passwords

March 16, 2020

AC5 - Passwords

Organization members use strong passwords.

LeMoyne-Owen College
Password Policy

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. This means that all LeMoyne-Owen College employees (including contractors and vendors with access to LeMoyne-Owen College systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose

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

3.0 Scope

The scope of this policy includes all personnel 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 any LeMoyne-Owen College facility, has access to the LeMoyne-Owen College network, or stores any non-public LeMoyne-Owen College information.

4.0 Definitions

Application Administration Account: Any account that is for the administration of an application (e.g., Oracle database administrator, System administrator).

5.0 Policy

5.1 General

- Whenever possible, avoid passwords altogether by using Single Sign on (SSO). Whenever possible, use 2-Factor Authentication (2FA) or 2-Step Authentication.
- All system-level passwords (e.g., root, enable, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the LeMoyne-Owen College IT administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) should be changed at least every six months.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must not be shared between users without specific business reasons and must be managed by a centralized enterprise password management system.
- End user passwords shall be conveyed to staff and customers in a secure manner.
- End users shall be required to change their initial password to something that adheres to the policy and is known only to that user.
- All user-level and system-level passwords must conform to the guidelines described below.

5.2 Guidelines

5.2.1. General Password Construction Guidelines

Passwords are used for various purposes at LeMoyne-Owen College. Some of the more common uses include: user level accounts, web accounts, email accounts, screensaver protection, voicemail password, and local network devices. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once),
all users should be aware of how to select strong passwords.

Users should use a randomly generated password from a password generator/manager (i.e. 1Password, LastPass). Strong passwords have the following characteristics:

- Consider using passwords containing both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- User passwords should be 14 semi-random characters (example: bpTE!z2stNc9$!).
- Passwords should NEVER be "Password" or any derivation.
- The password should **not** be:
  - A single word/phrase found in a dictionary (in any language).
  - A common usage word like computer terms and names, commands, sites, commands, sites, companies, hardware, software.
  - Names of family, pets, friends, co-workers.
  - Birthdays and other personal information such as address and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Same as passwords/phrases used on personal accounts (e.g. email, online banking, social media).
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
- Administrative passwords should be 20 (semi-random) characters long.

5.2.2. Passphrases

Passphrases can be used as an alternative to passwords. They are an easy way to remember complex passwords. They can be based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TsmyB1wy2Rmmr!" or some other variation. NOTE: Do not use any of these examples as a secret!

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

5.2.3. Use of Passwords and Passphrases for Remote Access Users

Access to the LeMoyne-Owen College Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

5.3 Password Protection Standards

- Do not use the same password for LeMoyne-Owen College accounts as for other non-LeMoyne-Owen College access (e.g., personal online accounts, etc.).
- Where possible, don't use the same password for various LeMoyne-Owen College access needs. For example, select one password for an Engineering system and a separate password for an IT system.
- Select separate passwords to be used for different system (Mac, Windows, Linux, etc.) accounts.
- Do not share LeMoyne-Owen College passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential LeMoyne-Owen College information.
  - Don't reveal a password over the phone to ANYONE.
  - Don't send a password in an email message.
  - Don't talk about a password in front of others.
  - Don't hint at the format of a password (e.g., "my family name").
  - Don't reveal passwords on questionnaires or security forms Don't share passwords with family members.
  - Don't reveal a password to co-workers while on vacation.
- Do not use the "Remember Password" feature of applications (browsers, email clients, etc.).

- Do not write passwords down and store them anywhere in the office. Do not store passwords in a file on ANY computer system (including phones or tablets) without encryption. Do not insert passwords into unencrypted email messages or other forms of electronic communication.
- If an account or password is suspected to have been compromised, report the incident to LeMoyne-Owen College IT and change all passwords.
- Password cracking or guessing may be performed on a periodic or random basis by LeMoyne-Owen College IT or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Users shall NOT share passwords with other users/employees. If such a demand is made, users shall point to this policy or direct it to their supervisor or IT.

5.4 Application Development Standards

Application developers must ensure their software contains the following security precautions.
Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

6.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Controls

AC5.0 - Application Passwords

Applications are configured to meet minimum password requirements. The password is anonymized and not in cleartext.

AC5.1 - Multi-Factor Authentication

Applications require multi-factor authentication (MFA) to authenticate users.

AC5.2 - Corporate Password Management

A password management system is implemented for all organization users.

AC5.3 - User Passwords

User passwords are at least 14 characters long and use upper case, lower case characters, digits and punctuations. This includes all user passwords for all applications.

AC5.4 - Administrative Passwords

Applicable to Administrative passwords.
Administrative passwords carry more risk than regular user passwords due to the privileges associated with the account. Hence, enhance controls around their usage.

AC5.5 - Password Protect Personal Devices

Personal devices are password protected.