Policy

Password Creation & Update Policy

Document Title	Password Creation and Update Policy
Document Owner	IT Department
Approved By	Information Steering Committee
Date Approved	02 October 2023
Date of Review	02 October 2024
Document Version	1.1

Table of Contents

1. Overview

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

2. 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.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 LCHS facility, has access to the LCHS network, or stores any non-public LCHS information.

4. Policy

4.1 General

- All system-level passwords (e.g. root, enable, Windows Administrator, application administration accounts, etc.) must be changed at least on quarterly basis.
- All production system level passwords must be part of the InfoSec administered global password management database.
- All user level passwords (e.g. email, web, desktop computer, etc.) must be changed at least every six months.
- User accounts that have system- level privileges granted through group membership or programs such as “sudo” must have unique password from all other accounts held by that user.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of “public”, “private” and “system” and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g. SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines

A. General Password Construction Guidelines

All users at London Campus of Higher Studies should be aware of how to select strong passwords.

Strong passwords have the following characteristics:

- Contain at least three of the five following character classes:
  - Lower case characters
  - Upper case characters
  - Numbers
  - Punctuation
  - “Special” characters (e.g.!@#$%^&*()_+-{}[]:”<>?,./ etc)
- Contain at least fifteen alphanumeric characters.

Weak passwords have the following characteristics:

- The password contains less than fifteen characters
- The password is a word found in dictionary (English or Foreign)
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - The words “LCHS”, “LondonCampusOfHigherStudies”, “Glaisher Street”, “London”, or any derivation.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvyts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the pfrase might be: “This May Be One Way To Remember” and the password could be: “Tmb1W>r~” or “Tmb1w2R” or some other variation.

(Note: Do not use either of these examples as passwords!)

B. Password Protection Standards

- Always use a different password for LCHS accounts from other non-LCHS access (e.g., personal ISP account, option trading, benefits, etc).

- Always use different passwords for various LCHS access needs whenever possible. For example, select one password for systems that use directory services (i.e. LDAP, Active Directory, etc.) for authentication and another for locally authenticated access.
- Do not share LCHS passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential LCHS information.
- Passwords should never be written down or stored on-line without encryption.
- Do not reveal a password in email, chat or other electronic communication.
- Do not speak about password in front of others.
- Do not hint at the format of password (e.g. “my family name”)
- Do not reveal a password on questionnaires or security forms.
- If someone demand a password, refer them to this document and direct them to the Information Security Department.
- Always decline the use of the “Remember Password” features of applications that are not trusted by your system or LCHS.

If an account or password compromise is suspected, report the incident to the Information Security Department.

C. Application Development Standards

Application developers must ensure their programs contain the following security precautions.

Applications:

- Shall support authentication of individual users, not groups.
- Shall not store passwords in clear text or in any easily reversible form.
- Shall 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.
- Shall support TACAS+, RADIUS and/or X.509 with LDAP security retrieval wherever possible.

5 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Password cracking or guessing may be performed on a periodic or random basis by the Information Security Department or its

delegates. If a password is guessed or cracked during these exercises, the user/owner will be required to changed it.

Hamzah Tariq Khan *Hamza Khan*	Muhammad Saqib Sohail *Saqib Sohail*
Director Admin / Operation	**Director Academic Affairs**
02 October 2024	02 October 2024