

Password Policy

1. Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Elmhurst College's resources. All users, including College students, employees, contractors, vendors, guests, and others with access to Elmhurst College 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 individuals or groups 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 Elmhurst College facility, has access to the Elmhurst College network, or stores any non-public Elmhurst College information.

4. Policy

4.1 Password Creation

4.1.1 All user-level and system-level passwords must meet or exceed the strong password standard articulated by the following **Password Construction Guidelines**.

Password Construction Guidelines:

Strong passwords have the following characteristics:

- Contain at least 8 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example, !\$%^ *()_+|~-=\`{}[]: ";>?,/) chosen from a list provided by the Office of Information Services (OIS).

Poor, or weak, passwords have the following characteristics:

- Contain fewer than eight characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of “Welcome123” “Password123” “Changeme123”

Never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation. (NOTE: Do not use either of these examples as passwords!)

4.1.2 Users must not use the same password for Elmhurst College accounts as for other non-Elmhurst College access (for example, personal ISP account, bank account, merchant account, and so on).

4.1.3 User accounts that have system-level administrative privileges must have a unique password from all other accounts held by that user.

4.2 Password Change

4.2.1 All system-level passwords (for example, root, enable, admin, application administration accounts, and so on) must be changed on at least a quarterly basis.

4.2.2 All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least annually. The recommended change interval is every six months.

4.2.3 Password cracking or guessing may be performed on a periodic or random basis by the Office of Information Services (OIS) or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the **Password Construction Guidelines** articulated above.

4.3 Password Protection

4.3.1 Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential Elmhurst College information ([*Policy on the Definition, Classification, and Use of Sensitive Information*](#)).

4.3.2 Passwords must not be inserted into email messages or other forms of electronic communication.

4.3.3 Passwords must not be revealed over the phone to anyone.

4.3.4 Do not reveal a password on questionnaires or security forms.

4.3.5 Do not hint at the format of a password (for example, "my family name").

4.3.6 Do not share Elmhurst College passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.

4.3.7 Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.

- 4.3.8 Do not use the "Remember Password" feature of applications (for example, web browsers).
- 4.3.9 Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

5. Policy Compliance

5.1 Compliance Measurement

The Office of Information Services (OIS) will verify and promote compliance to this policy through various methods, including but not limited to, reports, internal and external audits, and feedback to individuals and campus departments.

5.2 Exceptions

Any exception to the policy must be approved by the Chief Information Officer in advance.

5.3 Non-Compliance

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

Related Standards, Policies and Processes

- [*Policy on the Definition, Classification, and Use of Sensitive Information*](#)