

Password Policy

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in substantial downtime and the compromise of sensitive data and information stored on both the local and any connected machines. As such, all College of Chemistry users (including contractors and vendors with access to College of Chemistry 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 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 in any College of Chemistry building, has access to the College's network, or stores any non-public College of Chemistry information.

4.0 Policy

4.1 General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four 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 inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes in the College of Chemistry. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, and file server logins. Because of their critical function in maintaining a secure network, everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a 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.
 - Birthdays and other personal information such as addresses and phone numbers.
 - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
 - Any of the above spelled backwards, or preceded/followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain 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, !@#\$%^&*()_+|~-=\`{ }[]: ";' < > ? , /
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.

- Are not based on personal information, names of family, etc.
- 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 phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~".
(NOTE: Do not use either of these examples as passwords!)

B. Password Protection Standards

Do not use the same password for College of Chemistry accounts as for other non- College of Chemistry access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various College access needs. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share College of Chemistry passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential information.

Here is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss or co-workers
- 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 a password on questionnaires or security forms
- Don't share a password with family members

If someone demands a password, refer them to this document or have them call someone in the Information Systems Department.

Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Netscape Messenger).

If an account or password is suspected to have been compromised, report the incident to Information Services and change all passwords.

5.0 Enforcement

Any user found to have violated this policy may be subject to disciplinary action.