

CONCORDIA COLLEGE

Policy and Procedure Manual

Subject: Passwords

Section: General

Number: 1.7

Effective Date: June 1, 2008

Scope: The College

Purpose

To outline the creation and use of user ID's and passwords that grant access to various systems and applications and the information assets they protect.

Policy

Concordia College is committed to protecting the confidentiality, integrity, and accessibility of the information it owns or controls, passwords must be created and protected in a manner that minimizes the likelihood of unauthorized persons gaining access to the assets they protect. Accounts holders are held responsible for any activity done under their account. Passwords should be unique and must not be shared.

The President or designee must approve any exceptions to this policy.

Scope

This policy applies to any person granted access to a Concordia College information asset that requires a user name and password.

Enforcement

The CIO is responsible for monitoring and reporting compliance with this policy. In all cases, the College will disclose information as required by controlling law.

Procedures/Guidelines

Passwords created by any person granted access to Concordia College information assets must meet the following guidelines:

- Passwords must be at least eight (8) characters in length
- Passwords must be different than a user name
- Passwords should consist of no familiar names (e.g., pets, relatives)
- Passwords must not be words found in the dictionary
- Passwords must be formed using at least two of the following three groups of characters:
 - Alphabetic characters (A-Z, a-z)
 - Numbers (0-9)
 - Special Characters (e.g., #, \$, *)
- Passwords must be changed at intervals specified by the procedures for the application in which they are used

- If passwords must be written down to help memorize them, the paper they are written on must be protected from unauthorized access (e.g., no Post-It Notes ® under the keyboard).

Default account passwords that are included in many applications must be changed prior to deploying that application into the network. Since these default accounts are a common target for attack, these passwords should be made up of at least eight (8) characters using at least one of all three character groups mentioned above as well as meeting all other password creation guidelines. This password should also be written down, placed in a sealed envelope, and stored in a secure location. If the seal of that envelope must be opened or is found open, the password should be changed immediately.

Responsibilities

It is the responsibility of each account holder:

1. To create a password for each application
2. To not share passwords with anyone
3. To protect passwords from unauthorized use
4. To change passwords at intervals specified in application's procedures
5. To immediately notify the Chief Information Officer (CIO) if they believe their password has been compromised.

History: Approved 04/07/2008, Effective 06/01/2008