Information Security: Passwords and passphrases

Resource reference: **VPS-33-D03**
Status: **Approved**
Last revision: **2023-11-01**

Introduction

This directive defines a standard for the creation and use of passphrases and passwords to protect Concordia's information systems and data.

Passphrases (sequences of words or other text) or passwords (words and strings of characters) protect your devices and information from unauthorized access.

There are three key aspects to keep your passphrases and passwords safe to protect your information:

1. Create a strong passphrase/password
2. Guard it carefully (e.g. don't share it or write it down)
3. Avoid reusing it for other systems.

Concordia's Chief Information Security Officer has issued this directive under the authority of Policy Number: VPS-33 - Information Security Policy.

Questions about this directive may be referred to: ciso@concordia.ca.

University information systems minimum requirements

All of Concordia's information systems and data must be protected by strong passphrases or passwords and must meet or exceed the following standard:

1. The passphrase/password must not contain the user's username/netname or first/last name.
2. The passphrase/password must not be reused on any other system.
3. The passphrase/password must contain the following:
   - At least one uppercase letter (A through Z)
   - At least one lowercase letter (a through z)
   - At least one number
   - At least one special character supported (for example: !, @, #, $, %, ^, &, or *)
   - Password must be minimally 8 characters long.
4. When available, multi-factor authentication must be used.

It is the responsibility of all members of the Concordia community to guard their passphrases/passwords carefully. Passphrases/passwords should be changed every 365 days and must be immediately changed if there are suspicions that they could have been compromised and the incident must be reported to the IITS Security team according to the Reporting of Information Security Incidents (VPS-33-02).

Creating Passphrases and Passwords

It is recommended that passphrases are used, as they are longer yet easier to remember than a password of random, mixed characters. A passphrase is a memorized phrase consisting of a sequence of mixed words with or without spaces. In general, your passphrase should be at least 4 words and 15 characters in length. For example, you might create a passphrase by using association techniques, such as scanning a room in your home and creating a passphrase that uses words to describe what you see (e.g. “Cl0set l@mp Bathroom Mug”).

If using a passphrase is not possible, use a password that is as complex as possible. A password made up of lowercase and uppercase letters, as well as numbers and special characters, is more complex than a password of only lowercase letters. You can also think up a phrase and then use the first letters of each word to create a complex password that is more memorable. For example, the phrase, “My jersey number when I played competitive soccer was 27!” can be used to remember the password, “Mj#wIpcsw27!”.

Protect passphrases and passwords

Passphrases, complex passwords, passcodes, and PINs must be handled, and stored carefully so that they are not compromised.

- Be aware of your surroundings when entering passwords and passphrases, passcodes
- Use a different password, passphrase, or PIN for each device and account, especially for accounts with sensitive information
- Do not give out passwords, passphrases, passcodes or PINs online or over the phone
- Do not share passwords, passphrases, passcodes, or PINs with anyone including your family or IT technical support staff.
- Log off and sign out of accounts and websites when you are done using them
- Always lock your device when leaving it unattended
- Ensure your sensitive accounts (e.g. banking, CRA) are protected by the strongest passphrase or password possible

Password Managers

It is often a challenge to ensure that the passwords you use are suitably complex and that the same passwords are not employed on multiple systems. A password manager is a solution to this problem as it automatically generates and stores strong and different passwords for various accounts.

A stand-alone encrypted password manager is recommended over a browser-based manager. Stand-alone tends to be more secure than browser-based and they allow for a complex master password and typically offer two-factor authentication . They also have more advanced features such as alerts if a website is compromised, and flagging weak passwords. You can also sync the passwords stored across your devices.

Biometric alternatives to passphrases and passwords

Biometric controls such as fingerprint readers and facial recognition are acceptable alternatives to passphrases/passwords/PINs.

Touchscreen devices

A numeric password/PIN/passcode should always be used on a device with a touchscreen. It is recommended that it is at least five characters long and always make sure your PIN is made of random numbers.

Exceptions

Exceptions to this directive must be documented and reported to the office of the Chief Information Security Officer (CISO) by email to: ciso@concordia.ca. Each exceptional instance will be assigned a consultant to perform a risk assessment and assist in the definition of appropriate mitigation measures if required.

Accessibility

Community members with accessibility questions or needs related to this directive are asked to contact the appropriate IITS resource person by emailing iits-accessibility@concordia.ca.

Implementation, audit, and review

Concordia's Chief Information Security Officer (CISO) is responsible for the implementation, review, and approval of this directive. Concordia's CISO initiates a review on an annual or as-needed basis to ensure alignment with both internal and external requirements and regulations.