https://intranet.msvu.ca/docs/Document%20Center/Password%20Policy.pdf

Password Policy

Passwords are an important aspect of computer and network security. Your password is the primary barrier for assuring the privacy of your computing activity and preventing others from using your account for disruptive, offensive, or illegal activities. Passwords address our primary concern: maintaining the integrity of your account while protecting MSVU's computing environment from abuse.

Having a network username and password at MSVU gives you access to a number of services including email, remote access, access to a high speed internet connection, and your personal network space. These types of services make us vulnerable to attacks from outside the university that could potentially disrupt our computer and network operations.

Password Restrictions

The following password restrictions are on all MSVU employee network accounts

- The minimum password length is 7
- All faculty and staff change their password every 90 days
- All faculty and staff must select strong passwords (see Guidelines below for strong passwords)
- After 4 incorrect login attempts the account is locked.
    - *The accounts will be locked for 3 days or will require a call to the Helpdesk.*
- Require unique passwords prevents the user from using any of his/her last 8 passwords.
- Grace Logins is set to 6 this is the number of times a user can login with an expired password before their account is locked.
- All passwords should be treated as sensitive confidential MSVU information and should not be shared.

Good Practices

Guidelines for selecting a Strong Password

- Passwords with 8 or more characters are the strongest
- Have both numbers and characters
- Are not based on personal information, names of family, etc.
- Shouldn't be any word that can be found in a dictionary
- Shouldn't include your login name
- Are easily remembered by you but hard to guess by others

Things you should not do with your Password

- Reveal your password over the phone
- Reveal your password in an email
- Talk about a password in front of others
- Don't share your password with family members
- Don't give your password to co-workers when going on vacation
- Don't use the "remember password" feature of applications
- Don't write down passwords and store them in your workspace (post-it notes on your monitor, under your keyboard or taped to your wall)