Password Guidelines

Purpose

To define password guidelines for creating strong passwords and securing your password to protect the university data you have access to.

A computer account consists of a username and password. At the U of S, the most common form of a username is the Network Services Identifier (NSID). The NSID consists of three letters followed by three numbers (e.g. abc123). Members of the university community are provided with a randomly generated password that can be changed in PAWS. Your computer account provides access to a variety of university services, including but not limited to, PAWS, e-mail, student and financial systems, computer labs, file storage space, wireless network, servers, and databases.

Scope

- The password guidelines are applicable to all members of the university community.

Protecting a Password

- Keep your password a secret.
- Commit your passwords to memory. If a password is written down, it should be locked away in a secure place.
- If a website or browser asks to keep you signed in, unclick that option and re-enter your password each time.
- Make sure sites are secure (https) before you enter your password.
- When off-campus, use a virtual private network (VPN) to access campus resources.
- University IT Service Desk or IT support staff will never ask for users’ passwords.
- Do not respond to emails or phone calls requesting you to verify your passwords.
- Do not share your passwords for any reason – even with trusted individuals.
- Never send passwords by email.

What makes a strong password

The general guidelines below offer helpful ideas for selecting a password that is both strong and easy for you to remember.
• The longer the password is, the better. Passwords should never be shorter than eight characters.
• Choose a password that you’re comfortable with and is easy to remember.
• Use a mixture of upper and lower case characters, numbers and symbols.
• Do not use words in the dictionary for any language. Stay away from words spelled backwards, misspelled words, and abbreviations that are easy to figure out.
• Never use your name, NSID, birthday, address, driver’s license or passport number.
• Avoid using information that your colleagues and/or acquaintances might know.
• Do not use a password you’ve used previously.
• Avoid character or number repetition (4444 or dddd).
• Avoid simple sequences (abcdefg or 123456) or use letters that appear in a row on your keyboard (qwerty).

If an account or password is suspected to have been compromised, report the incident to the ICT Service Desk.