Password Requirements

All passwords must be strong, meaning they use multiple character sets. These are much more difficult to crack or guess.

**Passwords must contain at least 8 characters.**

Passwords **should** contain characters from at least 3 of the following character sets:

- Upper case letters
- Lower case letters
- Numbers
- Special characters

**Simple Substitutions:**

- a = @
- l = !
- L = l
- o = O
- S = $

For more information, go to: [www.creighton.edu/secureit](http://www.creighton.edu/secureit)

-OR-

Write to: infosec@creighton.edu

Creating Strong Passwords

Passwords – your 1st line of defense

Systems security is EVERYONE’S job!
How to Create Strong Passwords

Method #1

- Start with an easy password.
  sammy

- Guideline # 1: Add more information to make your password longer.
  sammy is my dog

- Guideline # 2: Make sure your password does not contain dictionary words (remove spaces).
  sammyismydog

- Guideline # 3: Introduce simple substitution into the password to make guessing it more difficult.
  $@mmYI$mYdOg

Method #2

- Take a favorite phrase, lyric, sentence from a book, song, etc. and use the first letter of every word.
  “The quick brown fox jumped over the lazy dog”
  Becomes: tqbfjotld

- Use three of the four available characters as substitutions.
  Becomes: tqBfjOt!d

NEVER, NEVER share your password!!

Avoid passwords with obvious personal significance such as your name or default passwords such as “default”.

Method #3

- Develop a scheme that is difficult to guess but never changes:
  @#4word@word*
  Becomes: @#4herO@SnorE*

- When it is time to change your password, replace the words with new words.
  Becomes: @#4bENch@SONgs*

NEVER reuse old passwords.