SOUTHERN STATE
COMMUNITY COLLEGE

Creating a Strong Password

Passwords are like passports or a blank check; if lost or stolen they give hackers a world of opportunity by providing access to your personal, financial and work data. The campus Password Policy helps you be proactive in selecting a strong password and managing them, to protect your identity and College resources. Once you've read and understood the password policy, you should change your password and other campus passwords that do not meet the standards.

Strong Password Characteristics

- Are at least eight characters long
- Contain at least:
  - One digit (0-9)
  - One lower case letter (a-z)
  - One upper case letter (A-Z)
  - One special character (@#$%^&+=)
- Do not contain a part of your name, login ID, username, email address, or initials.
- Are kept private. Passwords should be memorized or, if written down, kept in a locked file cabinet or other secure location. (They should never be shared.)

Weak Password Characteristics

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign) or a word in any language, slang, dialect, jargon, etc.
- The password is the same as your user name or login name
- The password is a commonly used word such as names of family, pets, friends, computer terms, birthdays, other personal information, or patterns like aaabbb, dddddd, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

A List of Don’ts

- Don't reveal a password over the phone or in person to anyone. Not your boss. Not your family. Not your co- workers. If someone demands a password, refer them to this document.
- Don't reveal a password in an email message
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Avoid writing passwords down, but if you must, store them in a secure place (e.g., a locked file cabinet)
- Passwords should never be stored unencrypted on-line
- Do not use the "Remember Password" feature of applications (e.g., Internet Explorer, FireFox, etc.)
- Don't use the default password, if one is provided. Change it immediately to a new, stronger password.
- Don't reuse old passwords. (Passwords should not be reused within a 12-month period.)