College Operating Procedures (COP)

Procedure Title: Technology Passwords
Procedure Number: 02-0401
Originating Department: Information Technology

Specific Authority:
Board Policy n/a
Florida Statute 1001.65
Florida Administrative Code n/a

Procedure Actions: Adopted: 07/15/2008; 06/01/2010;11/19/2012; 11/14/2013; 02/10/2021, 08/07/2025, 12/01/2025

Purpose Statement: This policy establishes standards for the creation, protection, and management of passwords used to access Florida SouthWestern State College information systems. It ensures that passwords meet security best practices in accordance with NIST, particularly controls related to access control, identity authentication, and protection of credentials

---

Guidelines:

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Florida SouthWestern State College's resources. All users, including contractors and vendors with access to Florida SouthWestern State College systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

All users at Florida SouthWestern State College should be aware of how to select strong passwords.

I. General Password Construction Guidelines

A. All passwords must meet the following complexity and length requirements:

- Minimum 14 characters
- At least one lower case letter
- At least one upper case letter
- At least one numeric digit
- At least one special character (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc.)

B. Best practice passwords do not include:

- . Personal Information (e.g., names, birthdates, addresses)
- Dictionary words (English or foreign).
- Predictable patterns (e.g., 123456, qwerty, abcABC)
- College name, location names and derivatives
- Avoid reuse of passwords used in the last five (5) changes

Tip: Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, “Success Usually Comes From Consistency”. Take the first letters: SUCFC then add a pattern of numbers and special characters you can recall — for example, based on positions or habits: S1u2C3f4C!@ (first letter, number, next letter, number...)

(NOTE: Do not use this example as a password!)

II. Password Use Protection

- Use unique passwords for:
  - Florida SouthWestern Accounts
  - External accounts (e.g. banking, email, personal services)
- Do not reuse passwords across systems or accounts
- Do not share passwords with anyone (including coworkers and supervisors)
- Do not store passwords in plain text or write them down unsecured.
- Do not transmit passwords via email, messaging, or chat
- Do not reveal or hint at passwords verbally or in writing.
- Disable “Remember password” or “Auto-fill” browser features
- Use password managers approved by IT (with encrypted storage)
- All passwords must be obscured during entry (e.g., displayed as bullets/asterisks).

III. Password Expiration and Reuse

- All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) should be reviewed for change on at least a quarterly basis.
- All production system-level passwords must be part of the Information Security administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 6 months (180 days).
- Password history must prevent reuse of the last five (5) passwords
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

IV. Authentication and Application Development

Application developed or procured must support:

- Individual user authentication (not shared/group accounts)
- Secure password storage using strong security measures to protect the passwords
- No storage of passwords in cleartext or reversible form
- Role-based access control without password sharing
- Secure password transmission (e.g., TLS1.2, SSH, VPN)

V. System Configuration and Enforcement

- Systems must enforce password policies through centralized authentication when possible (e.g. LDAP, SAML, AD)
- SNMP community strings must be changed from defaults and not reused as login credentials
- Where available, multi-factor authentication (MFA) should be implemented
- IT must monitor authentication systems for unusual or unauthorized login activity

VI. Incident Response

- If a password is believed to be compromised:
- Immediately report to IT Security (email: abuse@fsw.edu)
- Affected accounts will be locked and require credential reset
- IT will investigate and may require security awareness re-training