College Operating Procedures (COP)	FLORIDA SOUTHWESTERN STATE COLLEGE

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

Specific Authority:
Board Policy
Florida Statute 1001.65
Florida Administrative Code

Procedure Actions: Adopted: 7/15/08; 6/01/10;11/19/12; 11/14/13

Purpose Statement: The purpose of creating policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

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. The following characteristics are required when creating an FSW password

Contain at least three of the five following character classes:

- Lower case characters
- Upper case characters
- Numbers
- Punctuation
- “Special” characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc)
- Contain at least 8 alphanumeric characters

B. Weak passwords have the following characteristics:

The password contains less than 8 characters.
The password is a word found in a dictionary (English or foreign).
The password is a common usage word such as:

- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- The words "Florida SouthWestern State College", "sanjose", "sanfran" or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

C. 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, the phrase might be: “This May Be One Way to Remember” and the password could be: “TmB1w2R!” or “Tmb1W>r#” or some other variation.

(NOTE: Do not use either of these examples as passwords!)

II. Password Protection Standards

- Always use different passwords for Florida SouthWestern State College accounts from other non-Florida SouthWestern State College access (e.g., personal ISP account, option trading, benefits, etc.).
- Always use different passwords for various Florida SouthWestern State College access needs whenever possible. For example, select one password for systems that use directory services (i.e. LDAP, Active Directory, etc.) for authentication and another for locally authenticated access.
- Do not share passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Florida SouthWestern State College information.
- Passwords should never be written down or stored on-line without encryption.
- Do not reveal a password in email, chat, or other electronic communication.
- Do not speak about a password in front of others.
- Do not hint at the format of a password (e.g., "my family name").
- Do not reveal a password on questionnaires or security forms.

- If someone demands a password, refer them to this document and direct them to the Information Technology.
- Always decline the use of the "Remember Password" feature of applications (e.g., Email account, Messenger services, Web Browser, etc).

If an account or password compromise is suspected, report the incident to the Information Technology Department or email abuse@fsw.edu.

C. Application Development Standards

Application developers must ensure their programs contain the following security precautions.

Applications:

- Shall support authentication of individual users, not groups.
- Shall not store passwords in clear text or in any easily reversible form.
- Shall provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

III. Password Expiration / Change

- 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 45 days.
- 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).
- All user-level and system-level passwords must conform to the guidelines described below.