PROCEDURE

Subject:	**Password**	**Number:** 2.60.07
Source:	Vice President, Planning and Institutional Effectiveness	**Reference (Rule #)** 6HX14-2.60
President's Approval/Date:	**4/10/18**	

PURPOSE: This Procedure details the password requirements for State College of Florida (SCF) user accounts.

SCOPE: This procedure applies to:

- Users, systems, and locations;
- Employees, contractors, service providers; and
- Applies to all facilities.

POLICY STATEMENT: State College of Florida (SCF) resources will use strong passwords, passwords will be kept private, and passwords will be terminated in a timely manner when no longer business justified.

Password Creation

- All passwords, including initial passwords shall:
- Be comprised of a minimum of eight (8) characters.
- Must do three of four of the following:
- Contain both upper and lower case characters.
- Contain at least one (1) alphabetic.
- Contain at least one (1) numeric characters.
- Contain at least one (1) special character (!@#$%^&*_+=?/~`;:,<>|\).
- Contain no more than two consecutive letters of the associated username.
- Be changed every 90 days at a minimum.
- Not be the same as any of the last four passwords used.
- Passwords must not be easy to guess and they:
- Must not use or be your username.
- Must not use or be your name.
- Passwords must not be reused for a period of one year.
- Passwords must not be shared with anyone.
- Passwords must be treated as confidential information.

- First time passwords must be unique and changed upon first login.
- Password changes shall require verification of the individual prior to reset.
- Systems that cannot accomplish the above password strength requirements must receive a formal “exception” from the Information Security Team (email TBD).
- Passwords entered incorrectly (6) times consecutively must be automatically locked out.

Password Disable

- In the event that a College employee or contractor separates from their employment, all passwords associated with or known by that individual shall be disabled immediately.
- Accounts shall be locked out after six failed login attempts. Accounts shall remain locked out for a minimum of 30 minutes or until manually unlocked.
- User sessions shall time out after 15 minutes.

Password Maintenance

- Stored passwords must be encrypted or hashed.
- If the password may have been compromised the password must be changed immediately.
- You are required to change your password if the Information Technology (IT) department requests your password to perform administrative duties.
- Administrators must not circumvent the Password Procedure for the sake of ease of use.
- SCF Domained computing devices must not be left unattended without enabling a password protected screensaver or logging off of the device.
- 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 reveal a password on questionnaires or security forms
- If someone demands a password, refer them to this document and direct them to the IT Help Desk at (941) 752-5357.
- Always decline the use of the "Remember Password" feature of applications

IT Help Desk password change procedures will include the following:

- Authenticate the user to the helpdesk before changing password.
- Change password meeting the strength requirements above.
- New password must be random.
- User must change password at first login.

NONCOMPLIANCE: Any employee/contractor found to have violated this procedure may be subject to disciplinary action, up to and including termination of employment. Service providers found to have violated this procedure may be subject to financial penalties, legal action, and including termination of contract.