VII 01 03 PASSWORD MANAGEMENT

Purpose

The purpose of this policy is to establish a standardized password policy for Volunteer State Community College (VSCC).

A combination of a personal user login ID for identification and a unique password for authentication will be required of all users before they are allowed access VSCC domains and systems.

Passwords will be used for authentication of access to all VSCC domains and systems except where stronger authentication methods (such as biometric authentication or two-factor authentication) are deemed necessary. The effectiveness of passwords to protect access to the institution's information directly depends on strong construction and handling practices.

I. Password Construction

All users must construct strong passwords for access to all institution networks and systems, using the following criteria where technically feasible:

a. Must be a minimum of 8 characters in length
b. Must be composed of a combination of at least three of the following:
    i. Upper case alphabetic character
    ii. Lower case alphabetic character
    iii. Numeric character
    iv. Non-alphanumeric character

II. Password Management

The following requirements apply to end-user password management.

a. Storage and Visibility
    i. Passwords must not be stored in a manner which allows unauthorized access.
    ii. Passwords must not be stored in a clear text file
    iii. Passwords must not be sent via unencrypted email
    iv. Passwords must not be shared with anyone
b. Changing Passwords
    i. Faculty and Staff must change their password at least once every 90 days. Students must change their password at least once every 120 days.
    ii. Password must be changed immediately if any of the following occurs:

1. Unauthorized password discovery or usage by another person
2. System compromise (unauthorized access to a system or account)
3. Insecure transmission of a password
4. Accidental disclosure of a password to an unauthorized person
5. Status changes for personnel with access to privileged and/or system accounts

III. Password Protection-System Accounts

a. System accounts can be defined as:
    i. Accounts used for automated processes without user interaction
    ii. Accounts used for device management
b. System Accounts are not required to expire but must meet the following password construction requirements:
    i. Must be a minimum of 30 characters in length or the maximum the system will allow if less than 30.
    ii. Must be composed of each of the following:
        1. Upper case alphabetic character
        2. Lower case alphabetic character
        3. Numeric character
        4. Non-alphanumeric character
c. Vendor provided passwords must be changed upon installation using the password construction requirements above.

IV. Compliance and Enforcement

a. This policy applies to all users of information resources including students, faculty, staff, temporary workers, vendors, and any other authorized users.
b. Allegations of violation of this policy shall be referred by the Chief Information Officer to the appropriate person(s) for disciplinary action.
    i. If a student, the policy violation will be referred to the Vice President of Student Services under TBR Policy 3:02:00:01.
    ii. If an employee, the policy violation will be referred to the immediate supervisor and the division's Vice President.
c. If there is a policy violation, which the Chief Information Officer believes rises to the level of a serious violation of this or any other VSCC policy, the Chief Information Officer is authorized to temporarily revoke access privileges after consultation with the Vice President of Business and Finance or the President. In those cases, the revocation of access must be reviewed by the appropriate disciplinary authority for review and final determination of access privileges within a three business day timeframe. In such cases the authorization of the Chief Information Officer carries

with it the authorization to make subjective judgments, such as whether material or statements violate VSCC Policy.

d. Justifications for exceptions to this policy must be documented by the institution.

TBR Source: G-051: Guideline approved at Presidents Meeting, August 19, 2014, effective September 26, 2014.

VSCC Source: President's Cabinet, September 12, 2016.