Revision Responsibility: Associate Vice President of Information Technology
Responsible Executive Officer: Vice President of Finance and Administration

Source/Reference: TBR Policy: 01.08.03.00 Access Control

## PURPOSE

The purpose of this policy is to establish a standard for the creation, use and protection of passwords by Columbia State faculty, staff, and students.

## INTRODUCTION

Passwords are one of the most important elements of computer security and are the front line of protection for user accounts including network login, email accounts, and web accounts. Poorly constructed passwords or passwords that may be easily detected could result in the compromise of Columbia State's network and its data. Given the threat to personally identifiable information, this policy is provided as one means to safeguard that information.

The following policy and procedures apply to all Columbia State Community College faculty, staff, students, visitors, and contractors. The policy also applies to all academic, administrative, networking and computer resources owned or installed at all Columbia State Community College (Columbia State) locations.

In addition to this policy, all users are subject to existing state and federal laws along with institutional and Tennessee Board of Regents (TBR) regulations concerning the use of computers, email, and the Internet. To the extent a discrepancy exists between this policy and related TBR or state policy or law, TBR and state policy or law shall take precedence if those policies are more restrictive.

## POLICY

I. Definitions

A. *Password* - a string of characters used for authentication of users on a computer system

B. *Privileged Account* –accounts with administrative or root access to a system. They are used for the administration of a system, application or database. Example: Oracle database administration, Banner, etc.

C. *System Account* - Accounts used for automated processes without user interaction or device management.

II. General

All users of Columbia State information systems will have a unique user identifier and password.

III. Passwords

A. Users will activate the use of Okta for multi-factor authentication.

B. Initial passwords will be set to pre-expire upon first login and must be changed by the user.

C. Employee passwords (network logon, portal, etc.) will be set to expire every 90 days.

D. Student passwords will be set to expire every 180 days.

E. Privileged Accounts –Privileged account passwords will be set to expire every 30 days.

F. System Accounts – System Account passwords are not required to expire, but must meet the password construction requirements defined in this policy.

G. Guest Accounts - Guest Accounts may be granted on a 24-hour basis for patrons and guests of the college.

H. Passwords for third party accounts i.e. MyLabsPlus or Ocelot, should follow the same construction requirements defined in this policy, and should not be the same as your Columbia State account(s).

IV. Other

A. Default vendor provided passwords must be changed upon installation using the construction standards in this policy.

B. User accounts that have system-level privileges granted through group membership or programs such as “sudo” must have a unique password from all other accounts held by that user.

C. Where Simple Network Management Protocol (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 login interactively. A key must be used where available and technically feasible (e.g. SNMPv2 or v3).

D. Password resets must be done through Okta.

E. All user-level and system-level passwords must conform to the guidelines for strong passwords as described below in Section V-A.

F. Password parameters will be set to prevent users from reusing the past twelve (12) passwords.

G. The minimum age duration for passwords will be one day.

H. Password grace periods will be ten (10) days during which the user will be warned the password is due to expire.

I. Accounts will be locked after five (5) unsuccessful attempts and remain locked for 30 minutes. Users can use OKTA to unlock their account or contact the Help Desk to reset before the lockout period ends.

J. Faculty and staff desktops will be locked after 30 minutes of inactivity requiring a logon using their password.

K. Lab computers will be logged out after 60 minutes of inactivity requiring users to logon using their password.

L. Passwords must be changed immediately if any of the following events occur:
   1. Unauthorized password discovery or use by another person
   2. System compromise or any unauthorized access to a system or account.
   3. Insecure transmission of a password
   4. Accidental disclosure of a password to an authorized person.
   5. Status changes for personnel with access to privileged and/or system accounts.
   6. Notification of an account compromise or breach.

V. General Password and Account Authenticators

A. Passwords will have the following characteristics:

1. Contain of at least eight (8) characters or more consisting of three (3) of the following four (4) character categories.
   - ASCII upper case characters (A-Z)
   - ASCII lower case characters (a-z)
   - Base 10 digits (0-9)

- Non alphanumeric characters (i.e. ~!#%*?_-)
- Construction of complex passwords will be enforced.

2. The following is recommended:

- Consists of more than 8 characters, numbers or letters in combination
- Not easily guessed
- Not based upon birthdates or personal information such as street address or telephone number
- Excludes use of part of the username.

B. Use of Passphrases

A passphrase is a longer version (23-character minimum) of a password and is therefore inherently more secure. A passphrase is typically composed of multiple words and therefore provides more security against brute force attacks. An example is "This May Be One Way to Drive Away" and the passphrase could be "ThisMaybe0neWaytoDriveAway" or reduced to "TmB1w2DW!" Another example: "1amtheMa$teroftheCoffeeMug".
Use of passphrases is encouraged as a viable alternative to passwords because they are generally easier to remember, but much more difficult to compromise.

VI. Password Protection Standards

A. Do not use the same password for Columbia State accounts as used for access to non-Columbia State accounts – that is personal Internet Service providers such as Gmail, Yahoo, PayPal, trading accounts, banking accounts, etc.

B. Do not share your Columbia State account information with anyone, including administrative assistants, colleagues or supervisors. All passwords are to be treated as sensitive and confidential Columbia State information.

C. Here are some account password security best practices:

- Do not reveal a password over the phone, through email, on a questionnaire or form.
- Do not use the "Remember Password" feature in any applications.
- Do not store in an unsecure manner i.e. on paper, and leave it "hidden" somewhere in your office.

D. If you suspect your password has been compromised report the incident to the Information Technology helpdesk immediately and if possible, change your password on all devices.

E. Accounts that are reported as compromised will be locked. Access to network resources will be suspended until the user is verified by the IT Helpdesk.

VII. Account Expiration and Privilege Revocation

A. Columbia State reserves the right to revoke network account privileges at any time. Revoking privileges may be required for individuals who are no longer associated with Columbia State, account abuse or account compromise.

B. An employee who is terminated or a student who is expelled will have all account privileges terminated immediately upon notification by Human Resources or the VP of Student Affairs respectively.

C. Student accounts will expire at the end of six months following graduation or end of activity.

D. Students admitted to the college but not registering for classes in the first term following the acceptance date will have account privileges terminated on November 1 for Fall semesters, April 1 for Spring semesters, and August 1 for Summer semesters.

E. Contractors, auditors, other affiliates - An account may be granted on a temporary basis upon written request and require sponsorship by a full-time employee. Temporary accounts will expire after 90 days, and require a written request from the sponsor to be reactivated. Exceptions are granted for training accounts which are created for special events or workforce development.

F. Individuals leaving Columbia State may leave to take other employment, retirement, or simply move on to other activities that do not include responsibilities at Columbia State. Normal expiration of an account will be determined as defined below:

1. Faculty or Staff who leave before retirement - All account privileges will be revoked upon the completion of last day worked and notification of such from Human Resources.

2. Retired faculty and staff – Upon retirement from Columbia State account expiration will be based on last day worked. This includes portal login and access to Columbia State email.

VIII. Enforcement and Compliance

A. The policy applies to all users of information resources including students, faculty, staff, temporary workers, vendors, and any other authorized users who are permitted access.

B. Persons in violation of this policy are subject to a range of sanctions, including the loss of computer network access privileges, disciplinary action, dismissal from the College, and legal action.
C. Some violations may constitute criminal offenses, per Tennessee and other local, and federal laws. The College will carry out its responsibility to report such violations to the appropriate authorities.

IX. Exceptions

Justification for exceptions to this policy must be approved in writing by the president.

*April 6, 2023 (new policy); reviewed/accepted by Cabinet, approved signed by the President May 16, 2023*