Policy Number	702.002
Policy Title	Password Policy
Responsible Officers	Vice President, Information Technology
Responsible Offices	Information Technology Services
Summary	Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Columbia International University's entire network. All CIU employees and students, as well as contractors, vendors, and volunteers with access to CIU systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change. The scope of this policy includes all user accounts on any system that resides at any CIU facility, has access to the CIU network, or stores any non-public CIU information.
Definitions	*Application Administration Account* -Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).
Approving Body	Information Security Review Committee
Approval Date	July 13, 2011
Last Revision	April 12, 2022
Renewed	Aca C (03.08.2024); Admin C (02.21.2024)
Re-evaluation Date	Fall 2026
Departmental Impact	All CIU, Ben Lippen, and Pineview Employees and Students

Failure to follow the following policy may result in disciplinary action, including termination of employment.

Policy

- Most system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed at least on an annual basis.
- All user-level passwords must be changed every 90 days.
- Termination of employees with privileged access may force an early password change for some system level 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.
- Passwords must not be inserted into email messages or other forms of electronic communication. For alternative methods, please contact Information Technology.
- All user-level and system-level passwords must conform to the guidelines described below.

General Password Construction Guidelines

Passwords are used for various purposes at CIU. Some of the more common uses include user level accounts, web accounts, email accounts, screen saver protection, voicemail access, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)

    - 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)

Strong passwords have the following characteristics:

- Contains both upper- and lower-case characters (e.g., a-z, A-Z)