| | |
|---|---|
| **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)
- 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 "CIU", "BLS", 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)

Strong passwords have the following characteristics:

- Contains both upper- and lower-case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e).
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored in an unencrypted format. 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!

**Password Protection Standards**
Do not use the same password for CIU accounts as for other non-CIU access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, do not use the same password for various CIU access needs.

For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share CIU passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential CIU information.

Here is a list of "don’ts":

- Do not reveal a password over the phone to ANYONE.*
- Do not reveal a password in an email message to ANYONE.*
- Do not reveal a password to the boss or IT Services.*
- Do not talk about a password in front of others.
- Do not write a password down on paper that is left visible on your desk or computer.
- Do not hint at the format of a password (e.g., "my family name").
- Do not reveal a password on questionnaires or security forms.
- Do not share a password with family members.
- Do not reveal a password to co-workers while on vacation.
- Do not share your MFA code with anyone.
- Do not approve MFA prompts unless you are certain that you have initiated the prompt.

Note that the guidelines above denoted by an asterisk are allowed to Information Technology staff if the need is warranted or authorized by an IT supervisor.

Here is a list of “do’s”:

- If someone demands a password, refer them to this document or have them call the Information Technology Services Department.
- If an account or password is suspected to have been compromised, report the incident to IT Services and change all passwords.
- Password cracking or guessing may be performed on a periodic or random basis by IT Services or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

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

Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should 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.
- should support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

**Use of Passwords and Passphrases for Remote Access Users**
Access to the CIU Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

**Passphrases**
Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are different from passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All the rules above that apply to passwords apply to passphrases.

**Enforcement**
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.