## Policy Statement

Passwords are a critical aspect of computer security forming the front line of protection for user accounts. A poorly chosen password can result in the compromise of CSU's entire network. As such, all CSU students, and employees (including contractors and vendors with access to CSU systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

## Purpose

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.

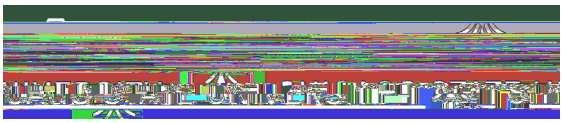
## Scope

The scope of this policy includes all users who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any CSU facility, has access to the CSU network, or stores any non-public CSU information.

## Definitions

- **University-Related Persons / Employee / Staff** are University students and applicants for admission, University employees and applicants for employment, Designated Campus Colleagues (DCCs), alumni, retirees, temporary employees of agencies who are assigned to work for the University.
- **Associate / "Extra Help", Third-party or 3rd party** is someone officially attached or connected to the College who is not a student or employee (e.g., Extra Help, vendors, interns, temporary staffing, volunteers.)
- **ITD Resources / Information Resources**

Password



## Responsibility

The Password Policy for CSU Information Resources applies to all active members of the University-Related Persons / Employees / Staff, Associates / Contractors or 3rd parties, and Students who use or access University Information Resources.

## Policy

### General

**Under no circumstances should a user divulge their password to another person.**

1. All system-level passwords (e.g., root, enable, admin, application administration accounts, etc.) must be changed on at least a semi-annual basis.
2. All production system-level passwords must be part of the IT Services administered global password management database.
3. All user-level passwords, (e.g., email, web, desktop computer, etc.), subject to the technological constraints of the platform must
    1. Be reset every 180 days
    2. Exhibit complexity by
        1. Not contain all or part of the user's account name
        2. Contain characters from three of the following four categories:
            1. Uppercase characters (A through Z)
            2. Lowercase characters (a through z)
            3. Base 10 digits (0 through 9)
            4. Non-alphabetic characters (for example, !, $, #, %)
    3. Maintain a password history of 12 passwords and not allow reuse
    4. Must be a minimum of 12 characters
    5. Be locked out for a minimum of 15 minutes if more than 3 unsuccessful attempted logons
    6. ***Those platforms that are technologically incapable of those levels of password complexity and restrictions must be configured to require the maximum level complexity allowed by the particular platform up to and including those parameters described in 3.1 through 5.5 above.***
4. CSU systems capable of such functionality will have automatic log-offs after a predetermined period of inactivity; username and password will be required for re-authentication.
5. 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.
6. Username and password combinations must not be inserted into email messages or other forms of electronic communication unless the message is encrypted.
7. Where 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 log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
8. All temporary passwords must be changed at first logon.

## References

- NIST CSF: PR.AC-1

## Version History

| Version | Modified Date | Next Review | Approved Date | Approved By | Comments |
|---|---|---|---|---|---|
| 1.0 | 11/3/2022 | 11/1/2023 | 11/6/2022 | Donna Hart | |
| | | | 11/1/2023 | Donna Hart | |
| | | | | | |