University of Colorado **Denver | Anschutz Medical Campus**

Campus Administrative Policy

Policy Title: Information Systems Networked Resource Passwords

Policy Number: 5005 Functional Area: Information Technology

Effective:	July 1, 2019
Date Last Amended/Reviewed:	May 22, 2019
Date Scheduled for Review:	July 1, 2026
Supersedes:	Information Systems Networked Resource Passwords, February 25, 2003
Approved by:	Donald M. Elliman, Jr. Chancellor, University of Colorado Anschutz Medical Campus Dorothy A. Horrell Chancellor, University of Colorado Denver
Prepared by:	Information Security Officer and Director of IT Security and Compliance
Reviewing Office:	Executive Vice Chancellor for Administration and Finance | CFO, University of Colorado Anschutz Medical Campus Senior Vice Chancellor for Administration and Finance | CFO, University of Colorado Denver
Responsible Officer:	Associate Vice Chancellor and Chief Information Technology Officer
Applies to:	CU Anschutz CU Denver

A. INTRODUCTION

At the University of Colorado Denver Campus and University of Colorado Anschutz Medical Campus, ("the university") information technology users have the ability to change their passwords. In order to protect computers, information and other related resources, the university requires its system users to have "strong" passwords.

University information technology providers are responsible for managing and protecting the information technology resources under their jurisdiction, including the enforcement of strong password standards. The use of computing and networking resources of the university is a privilege and as such, any individuals who use the information technology resources of the university are responsible for complying with the password requirements of this policy.

This policy applies to all users of the university internal data network and IT systems.

B. DEFINITIONS

Users of the university internal network refers to any individuals and/or electronic devices that are connected to the university using infrastructure that interconnects computers, networking equipment and other electronic devices for the purpose of data or information exchange.

Strong Password – is a password that is not readily decipherable and usually consists of symbols/characters, letters, and/or numbers that will allow a user to gain access to the university internal network.

University OIT – is the department that provides centralized information technology support of the CU Denver Campus and CU Anschutz Medical Campus.

C. POLICY STATEMENT

1. General

Passwords are an integral component of the university's "defense-in-depth" strategy. In some cases, passwords are the only protection against inadvertent or malicious access to a resource or data. Because passwords play such a vital role in protecting the security of our resources, it is essential that all accounts with access to any networked resource have passwords that meet minimum length, complexity, and frequency of change criteria.

Without passwords that meet these criteria, university resources and data are vulnerable to attack. With access to a single insecure password, an experienced attacker may be able to do irreparable or costly harm to university data or resources. In addition, passwords need to be protected against unauthorized disclosure, modification, or removal.

All activities inconsistent with these objectives or that could be construed to constitute a conflict of interest or commitment are considered to be inappropriate and may jeopardize the user's privilege of using university IT resources. To ensure the protection of IT resources, university OIT reserves the right to probe and monitor computing activities on any and all devices connected to the university network to ensure they are operating in compliance with this policy. In addition, OIT may withdraw a user's privileges or disable their credentials when violations of this policy occur.

2. Conditions for Use of university IT Resources

a. The use of campus standards for strong passwords is mandatory and exceptions are only allowed if the OIT authorizes exclusions due to unique and extraordinary circumstances.

b. OIT password policy ensures that all resources accessing the university Active Directory domain use the password criteria. (See following section, Password Criteria.)
c. OIT retains the right to scan university passwords to ensure compliance to this policy. OIT also retains the right to scan passwords in use on department-owned servers, desktop systems, workstations, applications, and other equipment attached to the campus network.
d. Except for technical support, and as authorized by OIT, passwords must not be shared with others or written down and left in an obvious or insecure location.
e. Service accounts, or accounts dedicated to a piece of equipment, may be exempt from the frequency of change criteria.
f. All suspected policy violations, system intrusions, fraudulent request for password changes, and other conditions, which might jeopardize university resources, should be immediately reported to the OIT Service: 303-724-4357 or 4-HELP.

3. **Non-compliance with Policies**

a. OIT will identify non-compliant passwords through network monitoring or other means.
    1) Direct telephone or e-mail contact with system owner
    2) Contact with unit-level IT staff
    3) Escalation via departmental administrative channels

b. OIT will follow up with communications to owners of non- compliant passwords.

c. Remedies will take the form of one of the following options:
    1) Password will be changed and systems reconfigured as needed; or,
    2) OIT will authorize a written exclusion from this policy; or
    3) The account(s) will be removed from the campus network.

4. **Password Criteria**

a. Minimum password length is eight characters
b. Password must contain three of the following:
    1) Lowercase alpha (a, b, c, etc.)
    2) Uppercase alpha (A, B, C etc.)
    3) Number (0, 1, 2, 3, etc.)
    4) Special Character (!, @, #, $, etc.)
c. Passwords should be changed every 90 days. There is a grace period of an additional 90 days. If the password reaches an age of 180 days, the account will be frozen, and the user will need to contact their department-level IT support or the OIT Service Desk (303-724-4357 or 4-HELP) in order for the

account to be unlocked and the password changed.

d. Accounts will be locked after 20 failed login attempts (call the OIT Service Desk at 303-724-4357 or 4-HELP for assistance)

e. Passwords may not be re-used if used during the last twelve password cycles.

Notes

1. Dates of official enactment and amendments:
   February 25, 2003: Adopted by the Provost
   September 6, 2018: Modified
   July 1, 2019: Revised

2. History:
   September 6, 2018: Modified to reflect a Campus-wide effort to recast and revitalize Campus policy sites into a standardized and more coherent set of chaptered policy statements organized around the several operational divisions of the university. Article links, formatting, and University branding updated by the Provost's office.
   July 1, 2019: Reviewed as part of the spring 2019 semi-annual review process. This policy was out of date with regards to the technical requirements for passwords, as well as the names used in the policy (OIT, CU Denver, CU Anschutz, etc.)

3. Initial Policy Effective Date: February 25, 2003

4. Cross References/Appendix:
   - CU System APS 6005: IT Security Program Policy