Campus Administrative Policy

Policy Title: Information Systems Networked Resource Passwords

Policy Number: 5005 — Functional Area: Information Technology

Effective: July 1, February 25, 2019

Date Last Amended/Reviewed: February 125, 2019

Date Scheduled for Review: July 1, 2024


Approved by:

Donald M. Elliman, Jr.
Chancellor, University of Colorado Anschutz Medical Campus

Dorothy A. Horrell
Chancellor, University of Colorado Denver

Roderick Nairn
Provost and Executive Vice Chancellor for Academic and Student Affairs

Prepared by: Sean Clark, Information Security Officer and Director of IT Security and Compliance

Reviewing Office: Executive Vice Chancellor for Administration and Finance

Senior Vice Chancellor for Administration and Finance

Responsible Officer: Russell J. Poole III, Associate Vice Chancellor and Chief Information Technology Officer

Applies to: University of Colorado Anschutz Medical Campus

University of Colorado Denver

Prepared by: Internship Taskforce

Reviewing Office: Provost and Executive Vice Chancellor for Academic and Student Affairs

Responsible Officer: Provost and Executive Vice Chancellor for Academic
A. INTRODUCTION

At CU Denver | Anschutz Medical Campus UCHSC, information technology users have the ability to change their passwords. In order to protect computers, information and other related resources, the CU Denver | Anschutz Medical Campus UCHSC requires its system users to have “strong” passwords.

CU Denver | Anschutz Medical Campus UCHSC 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 UCHSC university is a privilege and as such, any individuals who use the information technology resources of the UCHSC university are responsible for complying with the password requirements of this policy.

This policy applies to all users of the CU Denver | Anschutz Medical Campus UCHSC internal data network and IT systems who are connected through either a direct physical connection or connected via wireless connections, campus modem lines, DSL service, cable modems, over the Internet, or by other means.

B. DEFINITIONS

Users of the CU Denver | Anschutz Medical Campus UCHSC internal network refers to any individuals and/or electronic devices that are connected to the UCHSC Campus using infrastructure that interconnects computers, networking equipment, printers, personal digital assistants, and other electronic devices for the purpose of data or information exchange.

IT—is an abbreviation for information systems

IS—is an abbreviation for information technology

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 UCHSC internal network.

CU Denver | Anschutz Medical Campus OITUCHSC Department – is the centralized service unitdepartment that provides data networking, e-mail, file server, telephone, and other information technology support services for the UCHSC campuscentralized information technology support of the CU Denver | Anschutz Medical Campuses.

C. POLICY STATEMENTS

1. General
Passwords are an integral component of UCHSC’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, CU Denver | Anschutz Medical Campus UCHSC resources and data are vulnerable to attack. With only a few access to a single insecure password, an experienced hacker may be able to do irreparable or costly harm to UCHSC-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, CU Denver | Anschutz Medical Campus OIT UCHSC-reserves the right to probe and monitor computing activities on any and all devices connected to the UCHSC-university network to ensure they are operating in compliance with this policy. In addition, UCHSC-OIT may withdraw a user’s privileges or disable their credentials when violations of this policy occur.

2. Conditions for Use of CU Denver | Anschutz Medical UCHSC-IT Resources

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

b. UCHSC IS-OIT password policy ensures that all resources accessing the UCHSC.edu-university Active Directory domain use the password criteria. (See following section, Password Criteria.)

c. UCHSC IS-OIT retains the right to scan domain university passwords to ensure compliance to this policy. UCHSC IS-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 communication network.

d. Except for technical support, and as authorized by UCHSC IS-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 UCHSC IT-university resources, should be immediately reported to the Director of Information Systems Security via the Help OIT Service: Desk (phone 303-
3. **Non-compliance with Policies**

   a. **UCHSC-IS/IT** will identify non-compliant passwords through network monitoring or other means.
      i. Direct telephone or e-mail contact with system owner
      ii. Contact with **unit-level** departmental IT staff
      iii. Escalation via departmental administrative channels

   b. **UCHSC-IS/IT** will follow up with communications to owners of non-compliant passwords.

   c. Remedies will take the form of one of the following options:
      i. Password will be changed and systems reconfigured as needed; or,
      ii. The IS Department **OIT** will authorize a written exclusion from this policy; or
      iii. 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:
      i. Lowercase alpha (a, b, c, etc.)
      ii. Uppercase alpha (A, B, C etc.)
      iii. Number (0, 1, 2, 3, etc.)
      iv. 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 his/her LAN administrator department-level IT support or the **OIT Help Service** Desk (at 303-724-4357 or 4-HELP) in order for the account to be unlocked and the password changed.

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

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

**Notes**

1. Dates of official enactment and amendments:
   - Adopted by CU Denver Chancellor’s on February 25, 2003: Adopted by the Provost
   - July 1, 2019: Reviewed/Updated.

2. History:
Modified on September 6, 2018: Modified to reflect a 2018 Campus-wide effort to recast and revitalize Campus policy sites into a standardized and more coherent set of chaptered policy statement 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, etc)

3. Initial Policy Effective Date:
   February 25, 2003

4. Cross References/Appendix:
   - University Policy Framework and Hierarchy
   - CU System APS 6005: IT Security Program Policy
   - University of Colorado Health Sciences Center Fiscal Policy for Secure Computing