

University of Colorado Health Sciences Center
Administrative Policy for
Information Systems Networked Resource Passwords

Chapter:	5	Latest Revision:	February 25, 2003
Policy:	13	Page:	1 of 4

I. Purpose, Reference, and Responsibility

A. Purpose

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

B. Reference

University of Colorado Health Sciences Center Fiscal Policy for Secure Computing

C. Responsibility

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 is a privilege and as such, any individuals who use the information technology resources of the UCHSC are responsible for complying with the password requirements of this policy.

II. Applicability and Definitions

A. This policy applies to all users of the UCHSC internal data network 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

1. Users of the UCHSC internal network refers to any individuals and/or electronic devices that are connected to the UCHSC Campus computing infrastructure that interconnects computers, networking equipment, printers, personal digital assistants, and electronic devices for the purpose of data or information exchange.
2. IS is an abbreviation for information systems.
3. IT is an abbreviation for information technology.

University of Colorado Health Sciences Center
Administrative Policy for
Information Systems Networked Resource Passwords

Chapter:	5	Latest Revision:	February 25, 2003
Policy:	13	Page:	2 of 4

4. 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.
5. UCHSC IS Department is the centralized service unit that provides data networking, e-mail, file server, telephone, and other information technology support services for the UCHSC campus (see web site at <http://www.uchsc.edu/is>).

III. Statement of Policy

A. General

Passwords are an integral component of UCHSC's "defense-in-depth" effort. 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, UCHSC resources and data are vulnerable to attack. With only a few insecure passwords, an experienced hacker may be able to do irreparable or costly harm to UCHSC 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 IT resources. To ensure the protection of IT resources, UCHSC reserves the right to probe and monitor computing activities on any and all devices connected to the UCHSC network to ensure they are operating in compliance with this policy. In addition, UCHSC may withdraw a user's privileges when violations of this policy occur.

B. Conditions for Use of UCHSC IT Resources

1. The use of campus standards for strong passwords is mandatory and exceptions are only allowed if the UCHSC IS Department

University of Colorado Health Sciences Center
Administrative Policy for
Information Systems Networked Resource Passwords

Chapter:	5	Latest Revision:	February 25, 2003
Policy:	13	Page:	3 of 4

authorizes exclusions due to unique and extraordinary circumstances.

2. UCHSC IS password policy ensures that all resources accessing the UCHSC.edu domain use the password criteria. (See following section, Password Criteria.)
3. UCHSC IS retains the right to scan domain passwords to ensure compliance to this policy. UCHSC IS also retains the right to scan passwords in use on department-owned servers, desktop systems, workstations, applications, and equipment attached to the campus communication network.
4. Except for technical support, and as authorized by UCHSC IS, passwords must not be shared with others or written down and left in an obvious location.
5. Service accounts, or accounts dedicated to a piece of equipment, may be exempt from the frequency of change criteria.
6. All suspected policy violations, system intrusions, fraudulent request for password changes, and other conditions, which might jeopardize UCHSC IT resources, should be immediately reported to the Director of Information Systems Security via the Help Desk (phone 303-724-4357).

C. Non-compliance with Policies

1. UCHSC IS will identify non-compliant passwords through network monitoring or other means.
2. UCHSC IS will follow up with communications to owners of non-compliant passwords.
 - a. Direct telephone or e-mail contact with system owner
 - b. Contact with departmental IT staff
 - c. Escalation via departmental administrative channels

University of Colorado Health Sciences Center
Administrative Policy for
Information Systems Networked Resource Passwords

Chapter:	5	Latest Revision:	February 25, 2003
Policy:	13	Page:	4 of 4

3. Remedies will take the form of one of the following options:
 - a. Password will be changed and systems configured as needed; or
 - b. The IS Department will authorize a written exclusion from this policy; or
 - c. The account(s) will be removed from the campus network.

D. Password Criteria

For help selecting an appropriate password, see UCHSC Password Criteria at: <http://www.uchsc.edu/is/policies/passwordfaq.htm>

1. Minimum password length - 8 characters
2. Passwords must contain three of the following:
 - a. Lowercase alpha (a, b, c, etc)
 - b. Uppercase alpha (A, B, C, etc)
 - c. Number (0, 1, 2, 3, etc)
 - d. Special character (!, @, #, \$, etc)
4. 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 or the Help Desk at 303-724-4357 in order for the account to be unlocked and the password changed.
5. Accounts will be locked after five failed login attempts (call the Help Desk at 303-724-4357 for help)
6. Passwords may not be re-used if used during the last twelve (12) password cycles