Campus Administrative Policy

Policy Title: **Acceptable Use of Information Technology Resources**

Policy Number: 5001 Functional Area: Information Technology

Effective:	July 1, 2019
Date Last Amended/Reviewed:	May 22, 2019
Date Scheduled for Review:	July 1, 2026
Supersedes:	Ethical Use of Computing Policy (June 27, 2006)
Approved by:	Donald M. Elliman, Jr. Chancellor, University of Colorado Anschutz Medical Campus Dorothy A. Horrell

cases when unauthorized use of accounts or resources is detected or suspected, the account owner should change the password and report the incident to the appropriate account administrator, Unit Information Security Manager, and/or Dean, Director, or Department Chair. Users must understand that disclosing their account credentials to cybercriminals may result in personal losses that that they are ultimately responsible for.

D. POLICY STATEMENT

As a condition of use of University network and computing resources, every University IT resource user agrees:

1. Account Use
    a. Users shall utilize their accounts only for the purposes specified by the account grantor.
    b. Users shall not use any other individual's credentials or attempt to access an account when authorization has not been granted for them.
    c. Users shall not attempt to alter or avoid account access controls for computing systems.
    d. Accounts and passwords may not, under any circumstances, be used by persons other than those to whom they have been assigned by the account administrator.
    e. Users shall not share/disclose their account passwords with/to others.

2. Privacy
    a. Users shall not intentionally seek information on, obtain copies of, or modify files, hard drives, passwords or credentials, or any type of data belonging to other users unless specifically authorized to do so by the data owner or by the University.
    b. Users should always avoid violating others' privacy by;
        i. Tampering with security provisions.
        ii. Attempting entry to non-public hosts.
        iii. Sharing login credentials with others.

3. Computer and Network Security
    a. Users shall not attempt to alter, delete, or avoid computer audit controls and accounting log files.
    b. Users shall not attempt to bypass computer and network controls.
    c. Users shall not use CU Denver | Anschutz IT resources to infiltrate other systems, or damage or alter the software components of the systems.
    d. Users should avoid overuse of resources as defined by CU Denver | Anschutz OIT. Resources include;
        i. Network bandwidth,
        ii. Network file storage,
        iii. Printers,
        iv. Wireless networks (WiFi), and
        v. All other CU Denver | Anschutz IT resources.

e. Users must conform to campus standards for antimalware/endpoint protection. Exceptions are only allowed if CU Denver | Anschutz OIT authorizes exclusions in writing due to unique and extraordinary circumstances.
f. Users shall not implement their own network infrastructure without explicit written permission by OIT. This includes, but is not limited to, network devices such as hubs, switches, routers, network firewalls, DHCP servers, DNS servers, email servers or relays and wireless access points. Users must not implement alternate methods of access to CU Denver | Anschutz IT resources such as wireless access points (WiFi) and virtual private networks (VPNs).

4. Legal and Ethical Use

Users shall not:

a. Abuse, harass, intimidate, threaten, stalk, or discriminate against

example, University workstations/computers, servers, graphics devices, printers and networks, both voice and data, are resources that must be shared in an equitable manner.

d. Users m

further investigation or action.

The University may suspend, block or restrict access to an account when it appears necessary to do so:

a. to protect the integrity, security, or functionality of University or other IT resources;
b. to comply with legal or contractual requirements;
c. to investigate alleged or potential violations of law or policy including, without limitation, state, federal, or local law, or University or Board of Regents rules, regulations, policies, or collective bargaining agreements;
d. to investigate any asserted, threatened or potential complaint or grievance filed or credibly alleged pursuant to law or University or Board of Regents rules, regulations, policies, or collective bargaining agreements, or subject of law enforcement review or investigation;
e. or to protect the University from liability or disruption.

Notes

1. Dates of official enactment and amendments:
   June 17, 2006: Adopted by