University of Colorado Anschutz Medical Campus

Administrative Policy

Policy Title: Acceptable Use of Information Technology Resources

Effective: March 1, 2014

Approved by: IT Governance Committees and IT Cabinet

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

Responsible Office: Office of Information Technology

Policy Contact: Sean Clark, Information Security Officer and Director of IT Security and Compliance

Supersedes: Ethical Use of Computing Policy; June 27, 2006

Last Reviewed/Updated: April 1, 2014

Applies to: University of Colorado Denver | Anschutz Medical Campus

---

I. Policy Snapshot

Brief Description: Sets forth the University's policy with regard to use of and access to University of Colorado Denver | Anschutz Medical Campus IT Resources including university account use, privacy, computer and network security, legal and ethical use, networking and computing conduct, and software and intellectual property use. Further includes the steps the university may take should this policy be violated.

II. Scope

This policy applies to all users of University of Colorado Denver | Anschutz Medical Campus IT resources (including faculty, staff, students, and sponsored accounts) whether affiliated with the University or not, and to all uses of those resources, whether on campus or from remote locations.

III. Introduction

The Office of Information Technology at the University of Colorado Denver | Anschutz Medical Campus (CU Denver | Anschutz) is charged with the acquisition, development, and maintenance of computers, computer systems and networks. These Information Technology (IT) resources are intended for

University-related purposes, including direct and indirect support of the University's instruction, research, clinical and service missions; University administrative functions; student and campus life activities; and the free exchange of ideas within the University community and among the University community and the wider local, national, and world communities.

The use of network, computing, and other technology resources at the University is a privilege. It is the shared responsibility of all users, including faculty, staff and students to use these resources in an efficient, ethical, and legal manner.

This policy may be modified as deemed appropriate by the University. Users are encouraged to periodically review this policy as posted on CU Denver | Anschutz Office of Information Technology web site.

IV. General Rules

Users of University IT resources shall comply with federal and state laws, University rules, regulations and policies, and the terms of applicable contracts including software licenses while using University IT resources. Users who engage in electronic communications with persons in other states or countries or on other systems or networks may also be subject to the laws of those jurisdictions and the rules and policies of those other systems and networks. Users with questions as to how the various laws, rules and regulations may apply to a particular use of University computing resources should contact the University Counsel for more information.

Users are responsible for ascertaining what authorizations are necessary and for obtaining them before using University IT resources. Users are responsible for any activity originating from their accounts which they can reasonably be expected to control. In 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.

V. Statement of Policy

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

1. Account Use

- Users shall utilize their accounts only for the purposes specified by the account grantor.
- Users shall not use any other individual's credentials or attempt access to account not granted for them.
- Users shall not attempt to alter or avoid account access controls for computing systems.
- 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.

- Users shall not share/disclose their account passwords with/to others.

2. Privacy

- 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 University Counsel.
- Users should always avoid violating others' privacy by;
    - tampering with security provisions,
    - attempting entry to non-public hosts, or
    - sharing login credentials with others.

3. Computer and Network Security

- Users shall not attempt to alter, delete or avoid computer audit controls and accounting log files.
- Users shall not attempt to bypass computer and network access controls.
- Users shall not use CU Denver | Anschutz IT resources to infiltrate other systems, or damage or alter the software components of the systems.
- Users should avoid overuse of resources us defined by CU Denver | Anschutz OIT. For example;
    - network bandwidth,
    - network file storage,
    - printers,
    - wireless networks (WiFi), and
    - all other CU Denver | Anschutz IT resources.
- Users must conform to campus standards for anti-virus protection. Exceptions are only allowed if the CU Denver | Anschutz OIT authorizes exclusions in writing due to unique and extraordinary circumstances.
- 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;
    - abuse, harass, intimidate, threaten, stalk, or discriminate against others through the use of computing resources or
    - send obscene, abusive, harassing, or threatening messages to any other individual.
- IT resources are not to be used for personal commercial purposes, non-University business, or for personal financial or other gain. Occasional personal use of University IT resources for other purposes is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user's job or other University responsibilities, and is otherwise in compliance with this and other University policies, including without limitation the University's policies on outside activities and use of University trademarks and names. Further limits may be imposed upon personal use in

accordance with normal supervisory procedures concerning the use of University equipment.

- Users shall not misrepresent oneself or others through electronic communication including email.
- Users shall follow all University of Colorado, CU Denver | Anschutz, and CU Denver | Anschutz OIT policies, ethical standards and all local, state, and federal laws related to computing.
- Engaging in physical or cyber vandalism or mischief that incapacitates, compromises, or destroys CU Denver | Anschutz IT resources.

5. Network and Computing Conduct

- Users should avoid violating others' privacy, tampering with security provisions, or attempting entry to non-public hosts and/or data without written approval from the University Security Principal.
- Disruptive use of University IT resources is not permitted.
- Users should avoid excessive use of resources, controlled or otherwise. For example, University workstations/computers, servers, graphics devices, printers and networks, both voice and data, are resources that must be shared in an equitable manner.
- Users may not use any IT resource to gain unauthorized access to remote computers or to impair or damage the operations of University computers or networks, terminals or peripherals. This includes blocking communication lines, intercepting or sniffing communications, and running, installing or sharing virus programs.

6. Software and Intellectual Property Use

- Use of copyrighted software must be in compliance with vendor license requirements. Obtaining proper licensing for software that is not provided by the University is the responsibility of the user, as is the proper maintenance of such licenses and any associated software licensing fees.
- Users shall not violate vendor software copyright and authorized use policies. This includes using, duplicating, or distributing licensed software and documentation without the express written permission of the original copyright owner.
- Users shall not install and use:
    - File and/or music sharing programs,
    - Video and/or audio streaming programs that are playing non-campus mission related content.
    - Other programs that violate the ethical, efficient, and productive use of the campus internet resources.

VI. Responsibility & Action

Violation of this policy or other University information technology policies can result in revocation of computing privileges as well as corrective and/or disciplinary action.

Office of Information Technology (OIT)

OIT is responsible for interpretation and guidance regarding this policy. OIT also reserves the right to take additional action against violations of these policies. OIT may also refer suspected violations of law to appropriate law enforcement agencies for further investigation or action.

Other Responsible Parties

Other offices, departments, schools, etc. may be responsible for campus compliance and enforcement of this policy to take further action against violations. Other responsible parties include but are not limited to The Office of Regulatory Compliance, Human Resources, University Counsel, Student Affairs, and the Office of the Chancellor.

Users who violate this policy may be subject to other penalties and disciplinary action, including expulsion or dismissal, under applicable University or Board of Regents rules, regulations, policies, or collective bargaining agreements. Other responsible parties may also refer suspected violations of law to appropriate law enforcement agencies for 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.

VII. Reference Documents

CU System APS 6001: Information Technology; Providing and Using

CU System APS 6002: Use of Electronic Email

CU System APS 6005: IT Security Program Policy

Ethical Use of Computing Policy; June 27, 2006