

Effective:	January 28, 2003
Responsible Office:	CIO
Policy Title:	Use of CU-Boulder's Computing and Network Resources
Approved	<i>Chancellor Dick Bynny</i>
Purpose:	Outlines the Rights and Responsibilities of IT users on the CU-Boulder campus

A. Introduction.

The purpose of this policy is to clarify the requirements, prohibitions, and procedures applicable to the use of CU-Boulder's computing and network resources.

CU-Boulder's computing and network resources include:

- All computers, computer systems, peripherals, network devices, and networks that are owned by CU-Boulder or that are attached to or access CU-Boulder's network; and
- All institutional data, user data, programs, system software, and/or configuration files that are contained in, stored on, or are transmitted via CU-Boulder's computers, networks, or information systems.

B. Access and Appropriate Use of CU-Boulder's Computing and Network Resources.

1. Passwords.

The University of Colorado Administrative Policy Statements on "Providing and Using Information Technology" and "Use of Electronic Mail" both state:

Only University faculty, staff, and students and other persons who have received permission under the appropriate University authority are authorized users of the University's electronic mail systems and resources.

CU-Boulder grants permission to individuals to have access to portions of its computing and network resources by issuing a password. The password is the mechanism by which a system permits a specific, authorized individual to have access to that system and/or data. Each user who obtains a password is required to keep it secure.

2. Group Use of a Single Password.

In very limited circumstances, a group of users may need to use a single user account to access resources. Under no circumstances should a password to an account established for the sole use of an individual be given out or shared. ITS mandates additional controls for group accounts. Please refer to CU-Boulder's Access and Authorization policy for password and group account requirements and procedures (<http://www.colorado.edu/ITS/security/ITSAccessAuthPolicy.doc>).

3. Faculty, Staff, and Student Web Pages.

CU-Boulder allows students, faculty, and staff to create and maintain personal web pages on CU-Boulder's servers. The policy applicable to such personal web pages is set forth in CU-Boulder's Web Publishing Policy (<http://www.colorado.edu/policies/webpolicy.html>).

C. What is Prohibited of Users?

1. This policy prohibits a password holder from:

- a. Disclosing a password to another person, either intentionally or through carelessness;
- b. Taking any action to discover, intercept, or decode others' passwords; and/or
- c. Running or otherwise configuring software or hardware to intentionally allow access by unauthorized users.

2. This policy prohibits anyone, whether or not they have been issued a password from:

- a. Taking any action to discover, intercept, or decode others' passwords; and/or
- b. Running or otherwise configuring software or hardware to obtain unauthorized access to CU-Boulder's computing and network resources.

3. Users must not disrupt or damage the academic, research, service, administrative, or related pursuits of another through the use of any CU-Boulder computing and network resource.

4. Users must respect the integrity of all CU-Boulder computing and network resources. Users are prohibited from using these resources to:

- a. Develop or execute programs that could infiltrate any computing and network resource;
- b. Tamper with security provisions;
- c. Damage or alter any computing and network resource;
- d. Gain or seek to gain unauthorized access to any computing and network resource; and/or
- e. Engage in any spoofing activity (constructing electronic communication so that its origin cannot be determined, or so it appears to be from someone else).

5. Users are prohibited from unauthorized monitoring or eavesdropping on any CU-Boulder computing and network resources.

6. Personal use of CU-Boulder's computing and network resources for commercial purposes not directly related to the University's business or for obtaining personal gain, or use that creates a direct cost or constitutes a conflict of interest or conflict of commitment for the University is prohibited.

7. Other use of CU-Boulder computing and network resources that violates University, State, or Federal law is prohibited. These prohibitions include but are not limited to:

- a. Use to harass, intimidate, or otherwise violate the rights or privileges of another person, organization, or legal entity;
- b. Use to support a political campaign in violation of the Fair Campaign Practices Act (section 1-45-117, Colorado Revised Statutes);
- c. Use to violate Colorado and/or Federal Copyright and Intellectual Property laws;
- d. Use to defame or invade the privacy of another person, organization, or legal entity;
- e. Use to access and/or download obscene material as defined by Colorado and/or Federal laws.

D. May Computing and Network Resources be Used to Transmit Confidential Information?

As used in this policy, Confidential Information includes information that is confidential pursuant to Colorado and/or Federal law. Types of Confidential Information include but are not limited to information that is protected from disclosure pursuant to the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Colorado Open Records Act, the attorney-client privilege, etc.

Because information transmitted by using University computing and network resources runs the risk of being unintentionally disclosed to the wrong addressee or to others with access to the resources, the user should consider whether or not using the computing and network resources is prudent. Notwithstanding this risk, staff, faculty, and others who are authorized to use University computing and network resources to transmit information on behalf of the University are permitted to transmit Confidential Information, when such transmission is appropriate. Before transmitting Confidential Information, faculty and staff should consult with their dean, director, or department head. Supervisors who have legal questions about transmitting Confidential Information by using University computing and network resources may consult with the Boulder campus' Office of the University Counsel.

E. Administration and Enforcement.

1. Termination of Authorized Use.

When an authorized user changes status (e.g., terminates employment, graduates, retires, and/or changes positions or responsibilities within CU-Boulder), the unit responsible for supervising that change in status must communicate the change to appropriate administrators and ITS to ensure that access and authorization privileges reflect that status change.

2. Monitoring and Archiving.

Section D.1.a. of the Administrative Policy Statement on "Use of Electronic Mail" states:

a. To the extent permitted by law, the University reserves the right to access and disclose the contents of faculty, staff, students', and other users' electronic mail without the consent of the user. The University will do so when it believes it has a legitimate business need...

Similarly, CU-Boulder reserves the right to access and disclose any contents on CU-Boulder computing and network resources without the consent of the user. CU-Boulder will not monitor individual use of these resources as a routine matter, but it may do so as the University deems necessary and appropriate.

The University will not access individual content on computing and network resources without the consent of the user unless approval has been obtained from the appropriate authority, or his or her designee. In the case of faculty and staff working in a school or college, this is the Dean; for all other staff users, the Divisional Vice Chancellor; for undergraduate student users, the Dean of Students; and for graduate students, the Dean of the Graduate School. An exception to this procedure will be allowed only when emergency entry is necessary to preserve public health and safety or the integrity of facilities; in this case, the appropriate Vice Chancellor or Dean will be notified promptly of this emergency access. All instances of access without consent will be logged and communicated to the Associate Vice Chancellor for Academic and Campus Technology.

CU-Boulder does not systematically archive contents of shared system disks, email communications, network traffic data, or network monitoring data. The University regards email as a vehicle for delivery of information and not as a mechanism for the retention or archiving of information.

3. Enforcement.

Any person who uses CU-Boulder's computing and network resources in violation of Federal, State, or University law or policy is subject to loss of privileges, disciplinary action, personal liability, and/or criminal prosecution.

The University may block access to or remove a network connection that is endangering computing and/or network resources, or that is being used for inappropriate or illegal use.

The Office of Academic and Campus Technology and ITS will, when appropriate, work with other University offices such as the Office of Judicial Affairs (in cases involving students), the CU Police Department, deans and directors, and others to enforce this policy.

F. Selected References to University Policies:

1. The University of Colorado at Boulder.
 - o Access and Authorization policy: <http://www.colorado.edu/ITS/security/ITSAccessAuthPolicy.doc>
 - o CU-Boulder's Web Publishing policy: <http://www.colorado.edu/policies/webpolicy.html>
2. University of Colorado System.
 - o University of Colorado System, Administrative Policy Statement, for IT Users, "Providing and Using Information Technology" policy: <http://www.cusys.edu/policies/General/IT.html>

- University of Colorado System, Administrative Policy Statement, "Political Participation by Members of the University Community" policy:
<http://www.cusys.edu/policies/Personnel/politicalpart.html>
- Use of Electronic Mail policy: <http://www.cusys.edu/policies/General/email.html>

Related Links

- [Guidelines for Computer Users](#)
- Guidelines for System Administrators

