University of Colorado Boulder	**University of Colorado Boulder Campus-wide Policy**

Effective: January 1, 2012
Responsible Office: The Office of the AVC for IT and CIO
Policy Title: Acceptable Use of CU-Boulder's IT Resources
Approved *IT Executive Advisory Committee*

Purpose: Further defines privileges and responsibilities for information technology (IT) resources at the University of Colorado Boulder; augmenting the APS "IT Resource User Responsibilities."

A. Introduction

Most privileges and responsibilities for information technology (IT) resources are covered by the University of Colorado Administrative Policy Statement, "IT Security Program – IT Resource User Responsibilities" and "University Information Security Standards for Trusted Campus Authentication;" however, additional responsibilities are outlined below for appropriate uses of IT resources at the University of Colorado Boulder campus.

B. Privileges and Responsibilities

CU-Boulder employees and students are granted access to *IT resources* and *university information* based on academic, research, or administrative needs. Access may be suspended or revoked due to violations of policy or abuse of IT resources.

Every employee and student receives an @colorado.edu email account and an *IdentiKey*, which gives an individual certain access and authorization into electronic resources based on their affiliation (role and status) within the university. Passwords associated with your email account and *IdentiKey* must be kept secure; and may not be shared with anyone. If you ever suspect that someone knows your password or has accessed your account, change your password immediately then contact the IT Security Office.

Employees have the responsibility to protect *university information* in accordance with requirements and other guidance from the IT Security Office. The employee's responsibility to protect *university information* also applies to personally-owned computing devices. *Private information* shall not be stored on personally-owned computing devices unless specifically justified for business purposes and adequately secured (as per guidance from the IT Security Office). IT service providers and other employees with *privileged accounts* will have additional responsibilities and should consult with the IT Security Office.

The University may access and disclose employee or student *individual content* when the University deems a legitimate and appropriate business need. Access and disclosure of content can occur without the consent of the user as long as the protocol outlined in Section D of this policy is followed. Privacy and/or confidentiality should never be assumed in electronic communications.

C. User Accountability for Ethical and Responsible Use

Use resources efficiently and effectively
While some personal use of IT resources is permitted, such personal use must never interfere with academic, research, or administrative needs.

Deliberate attempts to harm, degrade, or negligently disrupt the performance of any CU-Boulder *IT resources* or use CU-Boulder's resources to harm other *IT resources* is not acceptable (e.g. don't create or spread viruses, damage equipment, software, or data, disrupt services, or engage in IP spoofing). Contact the IT Security Office prior to running vulnerability or penetration testing tools.

Don't harass
Don't annoy, intimidate, threaten, or offend another person(s) by: conveying obscene language, pictures, and/or other materials; making threats of bodily or psychological harm; contacting another person repeatedly with the intent to annoy or bother; and/or contact a person who has expressed a desire for electronic communication to cease.

Don't use CU-Boulder's IT resources for commercial and/or political purposes
It is against state law for state resources or funds to be used for supporting political campaigns, candidates, legislation, or ballot issues.

Additionally, given the University's status as a state agency employees cannot use CU-Boulder's *IT resources* for personal financial gain and/or commercial purposes, whether for-profit or non-profit, with the exception of the 1/6 rule that allows for regular and periodic consulting activities (see: https://facultyaffairs.colorado.edu/a-z-information-guide-docs/one-sixth-rule.pdf/view). This use of network resources for regular and periodic consulting must not create a direct cost or violate the University's policies on conflict of interest/commitment.

Student organizations that are officially recognized by CU Student Government (CUSG) may advance their organization's mission as long as they abide by university policy as well as by state and federal law. Student personal use of CU-Boulder's network resources for commercial purposes is prohibited.

Comply with intellectual property law
Don't violate copyright law by illegally copying, distributing, downloading and/or uploading information using computing or network resources. Even innocent, unintentional infringement violates copyright law. Information regarding CU Boulder's statement on copyright can be found at: http://ucblibraries.colorado.edu/copyright/

D. User Expectations

As stated in Section B, the University may access and disclose employee or student *individual content* when the University deems a legitimate and appropriate business need and those instances are documented and approved by the appropriate authorities. In those instances, if it is necessary to access *individual content* on *IT resources* without the consent of an individual currently affiliated with the University, approval must be 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, the Divisional Vice Chancellor; for undergraduate student users, the Dean of Students; and for graduate students, the Dean of the Graduate School. *Individual content* may be accessed without the consent of the user to comply with legal requirements (including, but not limited to, subpoena, court order, e-discovery request, and/or open records request) as

determined by University Counsel. Departmental supervisors may request access to *individual content* when an employee retires, is terminated, unexpectedly passes away, or otherwise leaves the employment of the University.

If emergency access to *individual content* without the consent of the users is required to preserve public health and safety, or preserve the integrity of IT resources and campus facilities, notice shall be provided to the *campus IT security principal*, notifying them of the need to access files. *The campus IT security principal* can also assist in obtaining files. All instances of access will be logged by the *IT security principal.*

Individual content may be accessed through automated information security systems (such as antivirus software, intrusion detection systems, and/or data loss prevention systems) for the purposes of detecting and responding to threats to campus information resources. Excluding client antivirus or antimalware software, the campus IT security principal must authorize all automated information security systems that systematically access *individual content*. Automated information security systems will log only *individual content* needed to respond to and identify incidents.

Other than backups for disaster recovery purposes CU-Boulder does not systematically archive contents of email communications. CU-Boulder, at the direction of University Counsel, arranges ongoing archival of email accounts as required to meet legal requirements.

E. Administration and Enforcement

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

CU-Boulder may temporarily 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 AVC for IT and Chief Information Officer shall, as determined by the circumstances of a potential policy violation, work with the appropriate University offices such as University Counsel, the Office of Student Conduct (in cases involving students), the CU Police Department, deans and directors, and others to enforce this policy.

F. Definitions

Campus IT security principal: The person who performs day-to-day management of, and is the point of contact for, the IT Security Program at the campus level.

CU-Boulder's computing and network resources: IT Resources that are attached to or access CU-Boulder's network and all University information that is transmitted via CU-Boulder's computers, networks, or information systems.

Individual content: University information stored on university-owned IT resources for which system permissions have been configured to limit access to an individual user or where physical access is restricted to an individual user. Examples include email messages in a user's email account, office files stored in a user's home directory on a file server, files stored on a university-provided desktop, laptop, or other mobile device.

IdentiKey: An IdentiKey consists of a CU login name and an IdentiKey password. IdentiKeys play a large role in computing at CU-Boulder. An IdentiKey gives you access to: MyCUInfo (the student and faculty portal), My.CU (the employee portal), email, computers in OIT computing labs, UCB Wireless network, CULearn, Desire2Learn, and Skillsoft (the computer-based training).

IT Resource: Computers, networking equipment, storage media, software, and other electronic devices that store, process, or transmit University information. In the context of IT security policy, this includes all IT resources that are owned, leased, licensed, or authorized for use by the University.

Privileged accounts: privileged accounts are those that have been granted system privileges beyond that of a typical user. Examples may include the ability to install software; install or modify system processes; create or modify system configurations; create or modify system access controls.

Private information: Personal information about an individual for which the individual can reasonably expect will not be made available to the public. This type of University Information includes personally identifiable information (a category of personal information regulated by federal law), as well as other non-public personal information that would adversely impact an individual if inappropriately used or disclosed. Examples include FERPA-protected information, Social Security numbers, credit card numbers and medical records.

University Information: Official information of the institution, including but not limited to: university work products, results, materials, records, or other information developed or produced with university goods, funds or services. University information encompasses all information created by the university, including information classified as private or restricted. Examples include university web site content, schedules of courses, requests for proposals, policies and guidelines, personnel records, student data, and research data.

G. Selected References to University Policies.

The University of Colorado

Administrative Policy Statement, "IT Security Program Section 1, IT Resource User Responsibilities" https://www.cu.edu/policies/aps-it.html

Administrative Policy Statement, for IT Users, "Providing and Using Information Technology" https://www.cu.edu/policies/aps-it.html

Administrative Policy Statement, "Political Participation by Members of the University Community" http://www.cusys.edu/policies/Personnel/politicalpart.html

Administrative Policy Statement, "Use of Electronic Mail" https://www.cu.edu/policies/aps-it.html

The University of Colorado Boulder.

Account Activation, Authentication and Termination: http://www.colorado.edu/avcit/sites/default/files/attached-files/account.pdf

CU-Boulder's Web Publishing policy: http://www.colorado.edu/policies/webpolicy.html