University of Colorado System Administration Information Technology Policy

Use of IT resources

Policy Sections

Overview

Computers, networks, software applications and other information technology (IT) products are powerful tools that facilitate the University of Colorado's (CU's) core mission in teaching, learning, research, and service. Access to these tools is a privilege available to university faculty, staff, students, and authorized guests. With this privilege comes a responsibility to follow principles of acceptable use.

Policy

The purpose of the CU System Administration Information Technology Policy is to ensure IT products and tools are used for purposes consistent with and supportive of the university's core mission.

Details

Applicability

This policy applies to use of:

- System Administration user accounts – accounts issued to System Administration employees, other CU employees, vendors, contractors, affiliates, retirees, and other authorized guests;
- System Administration technology hardware – desktop and laptop computers, tablets and smartphones, printers, networks and other infrastructure devices, and all other information technology products; and
- System Administration software, whether owned or licensed - e-mail domains operated by CU, CU websites, HR system, finance system, student information system, file servers, VPN service, and other web portals owned or maintained by CU.

Security Practices for Acceptable Use

The acceptable use of IT resources requires individuals to follow basic security practices. Users of System Administration IT resources must:

- Implement reasonable and appropriate safeguards to prevent unauthorized access to any CU IT resources;
- Protect sensitive or critical information that they create or maintain;
- Dispose of sensitive information in a secure manner (e.g., shredding, physical destruction, disk wiping);
- Report any IT security incidents or security policy violations to the Director of Information Security, Internal Audit or the ethics hotline;
- Cooperate with authorized investigations by legal counsel, internal audit and IT security;
- Cooperate with authorized requests to discontinue activities that threaten the confidentiality, integrity, or availability of IT resources;
- Return all institutional data and IT resources to CU upon termination of employment; and,
- Securely delete all institutional data from personally-owned devices/media upon termination of employment.

Authorized System Administration Monitoring Purposes

CU policies and procedures permit authorized staff to take certain actions to manage and protect IT resources. . Authorized System Administration staff (including but not limited to IT Security) may, without notice:

- Monitor, inspect, or copy network communications, IT resources, and the data they contain. Use of the System Administration network and/or IT resources constitutes consent to such monitoring;

- Assess IT resources connected to the System Administration network for security vulnerabilities;
- Take emergency protective actions such as restricting user access rights or access to IT resources or the network; or,
- Block potentially malicious network communications.

Unacceptable Use

The university considers, at a minimum, the following uses to be unacceptable. IT resources should not be used to:

- Violate any laws or applicable university policies;
- Violate professional ethics;
- Prevent an employee from fulfilling job responsibilities;
- Adversely impact or conflict with any activities that support CU's mission or operations;
- Realize personal financial gain;
- Promote political candidates or campaigns;
- Exceed an employee's job responsibility or authority;
- View of content that would contribute to a hostile work environment (pornography, promotion of hateful actions, etc.);
- Destroy data or IT resources without authorization;
- Incur unauthorized cost to the university;
- Violate copyrights or license agreements for any type of intellectual property;
- Share passwords or other access credentials;
- Hack, bypass, or violate security controls;
- Conduct unauthorized testing of IT resources for security vulnerabilities;
- Access, modify, or share sensitive data without appropriate authorization; or,
- Attempt to impersonate another individual in order to access IT resources.

Consequences of Unacceptable Use

If a CU System Administration employee unacceptably uses IT, the following sanctions may apply:

- Removal of inappropriate material from the relevant IT resources;
- Suspension or termination of access;
- Disciplinary action (up to and including termination of employment) in accordance with applicable university policy; and
- Civil or criminal prosecution.

Related University of Colorado Policies

As noted in this policy, employees should review other policies related to their work. It is recommended that all employees who use computers as part of their daily work review the following policies:

- APS 6001 - Providing and Using Information Technology
- APS 6002 – Electronic Communications
- APS 2006 – Retention of University Records

Employees who have a primary job duty related to IT should also review these policies:

- APS 6005 – IT Security Program
- APS 6010 – Data Governance

Employees who work with student records should also review these policies:

- APS 2007 – Access to Student Records
- APS 7003 – Collection of Personal Data from Students and Customers

Contact Information

Brad Judy – Director of Information Security, University Information Systems, University of Colorado

Dan Jones – Chief Information Security Officer, University of Colorado

Revision History

Version 1.0 – 10-16-2012 (not published)

Version 1.1 – incorporated feedback from Vice Presidents