University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

ADMINISTRATIVE POLICY STATEMENT

Policy Title: Providing and Using Information Technology

APS Number: 6001 **APS Functional Area:** **INFORMATION TECHNOLOGIES**

Brief Description:	Sets forth university-wide parameters for providing and using information technology and allows campuses and system administration to create and implement policies consistent with those parameters.
Effective:	April 9, 2015
Approved by:	President Bruce D. Benson
Responsible University Officer:	Vice President for Employee and Information Services
Responsible Office:	Employee and Information Services
Policy Contact:	Employee and Information Services
Supersedes:	Providing and Using Information Technology, February 1, 2000
Last Reviewed/Updated:	April 9, 2015
Applies to:	All Campuses

Reason for Policy:

This policy sets forth requirements for providing and using information technology. Recognizing that the campuses and system administration may require additional standards for use of technology, campuses and system administration may extend this policy with supplementary policies and guidance specific to each environment.

I. INTRODUCTION

The university has a responsibility to manage, secure and protect *IT resources*. Effective and efficient use of these resources is integral to the teaching, scholarly research, and public service missions of the university. IT service providers play critical roles in this entire process, including development of best practices to meet future needs.

The purposes of this Administrative Policy Statement are to set forth University requirements for providing and using *IT resources* and to establish expectations for *campuses* and system administration. Campuses and system administration may create and implement additional policies and guidance necessary for each unique environment consistent with the ownership and management provisions of this policy.

II. POLICY STATEMENT

A. University Ownership and Management of IT Resources

1. Subject to Regent, State and Federal laws, rules and/or regulations, and other university policies, all IT resources acquired or created through the use of *university resources*, including grant funds from contracts between the university and external funding sources, are property of the university. Rights and ownership of intellectual property and educational materials are governed by the following policies:

a. Ownership and disposition of intellectual property created by University employees and students is addressed in APS 1013 - Intellectual Property Policy on Discoveries and Patents for Their Protection and Commercialization.

b. Rights, responsibilities and rewards for the University and its employees in the development and commercialization of educational materials are addressed in APS 1014 - Intellectual Property That is Educational Materials.

2. Management responsibility for IT resources lies with the Chief Information Officer (CIO) as specified by APS 6005 - IT Security Program.

3. To the extent permitted by law, the university retains all rights of access to its IT resources as necessary to conduct the work of the university.

4. Only university faculty, staff and students and other persons who have received permission under the appropriate university authority are authorized users of IT resources.

5. The university shall take reasonable and prudent measures to maintain the privacy, confidentiality and integrity of communications and stored data. Specific expectations for all employees and IT Service Providers are specified in APS 6005 - IT Security Program, System-wide Baseline Security Standards and Standards for Individuals with Privileged Access.

6. The university provides access to IT resources in support of *official university business* and may revoke access privileges for reasons deemed appropriate by the Chief Information Officer (CIO) as specified by APS 6005 - IT Security Program.

7. IT resource users may access IT resources for incidental and occasional personal use as long as any such personal use does not violate laws, is not substantial use of *university resources*, or does not create a *conflict of interest* or commitment[1]. Decisions about whether use of these resources is "substantial" or "customary and current" shall be determined by the responsible campus chancellor or designee.

8. Except as provided in this policy the University will take all reasonable and prudent efforts to protect an IT resource user's personal privacy.

B. Use of External Email to Conduct University Business

1. The university expects employees and designated university affiliates shall use their official university email account when conducting *official university business*. Notwithstanding any other provision, employees shall not use an external email provider for storage or transmission of *highly confidential information* (e.g., protected health information, social security numbers. etc.).

a. If technical limitations in an official university email account cause a barrier to an employee performing his or her university duties, the employee shall first consult with the campus IT unit to determine if it is possible to mitigate the limitation. For example, it may be necessary for the campus IT unit to, temporarily, increase an employee's storage quota. If the technical limitations cannot be resolved in a reasonable timeframe, and *highly confidential information* will not be stored or transmitted, the employee may use an external email provider.

b. If employees or designated university affiliates attempt to forward email to an external email provider (e.g. Google, an affiliated government agency, another university), the university does not guarantee delivery to external servers.

c. The use of an external email service for university-related business creates university records outside of the university's official email system. Employees and designated university affiliates who use an external email service either directly or through establishing an email forward are responsible for the following:

[1] See APS 5012 – Conflicts of Interest and Commitment and Regent Policy 3B – Conflict of Interest.

i. Maintaining and preventing from deletion all emails (and associated attachments) used to conduct university-related business, in accordance with the university's Record Retention. Because email is not easily secured and preserved, users should use other means to save information specified in the campus records retention schedule.

ii. Upon request of the Office of University Counsel, an employee using a third-party email service for university-related business shall be expected to suspend any automated destruction process, provide requested information from his/her official university email account, and provide information related to *official university business* from his/her third-party account(s). Unless otherwise required by law, the Office of University Counsel shall provide an explanation for a request before the employee is required to furnish any requested information.

iii. If an employee or designated university affiliate does not take reasonable measures to provide specifically requested university information in response to the Office of University Counsel's request, or intentionally destroys the requested information in violation of a legal hold, disciplinary sanctions, up to and including termination, may apply.

C. Colorado Open Records Act Provisions

1. Information, no matter where it is stored, that is created, maintained or kept by the university and that relates to the performance of public functions or the receipt or expenditure of public funds may be a public record subject to public inspection under the Colorado Open Records Act, C.R.S. §24-72-201et seq., which governs disclosure of public records.

2. In the event of an Open Records Request affecting data residing on any university IT resource, the Office of University Counsel may instruct the appropriate IT office to capture and save the relevant data.

3. In response to an Open Records Request, the Office of University Counsel may review collected data to determine if any of the data constitutes a public record subject to public inspection.

D. Legal Hold Provisions

1. Data residing on any IT resource used for university business may be subject to a legal hold, discovery request, subpoena, court order or other legal request.

2. In the event of a legal hold, discovery request, subpoena, court order or other legal request regarding data residing on any university IT resource, the Office of University Counsel may instruct the appropriate IT office to capture and save the data.

3. In response to a discovery request, subpoena, court order, legal hold or other legal request, the Office of University Counsel may review the captured data to determine if any of the data may need to be disclosed.

E. Other Access

1. The university reserves the right to access and disclose data on IT resources when the university deems a legitimate and appropriate business need. These instances shall be documented and approved by appropriate authorities determined by the Chief Information Officer (CIO). Users shall be notified of access to the individuals account unless prohibited by law. Each Chief Information Officer (CIO) shall compose a written statement of procedure to request such approval. The procedure shall protect the personal privacy rights of individuals, take into consideration ways to minimize the time and effort required to submit and respond to requests and the need to minimize interference with university business.

F. Policies of Campuses and System Administration.

1. Each campus and system administration have different missions and environment and may create policies and guidance regarding use of IT. Campus policies and guidance shall be consistent with all provisions of this policy. The attached Campus Acceptable Use Policy Guidance provides guidance to campuses regarding rights, responsibilities and legal considerations.

2. If a campus or system administration elects to adopt local policies and procedures, it shall submit copies to the President's Office, which shall review them for conformance to this policy statement and publication with this policy.

3. Campuses and system administration shall communicate at least annually employee responsibilities and expectations as outlined in this APS and, if applicable, in local policies. The communication shall include, but is not be limited to, awareness of processes and possible circumstances under which data on IT Resources (e.g. records of extensively browsing social media or travel websites for personal use on work computer during business hours) may be accessed and disclosed.

III. RELATED POLICIES, PROCEDURES, FORMS, GUIDELINES, AND OTHER RESOURCES

A. Administrative Policy Statements (APS) and Other Policies

1. APS 2006 - Retention of University Records
2. APS 6005 - IT Security Program
3. System-wide Baseline Security Standards
4. Standards for Individuals with Privileged Access
5. APS 6002 - Electronic Communications

B. Campus Policies

1. CU Boulder – Acceptable Use of CU Boulder's IT Resources
2. UCCS - Information Technology Responsible Computing
3. CU Denver | Anschutz Medical Campus - Acceptable Use of Information Technology Resources
4. System Administration - Use of IT resources

IV. HISTORY

A. Non-substantive clean-up – May 1, 2015. Use of the title "Chief Technology Officer (CTO)" has been terminated and references to it were removed.

B. APS 6001 Providing and Using Information Technology was revised on April 9, 2015, and replaces Providing and Using Information Technology which was approved on 2/1/2000.

C. Providing and Using Information Technology was approved on 2/1/2000 to replace Establishment of University Management Systems Policy Committee and Campus Advisory Committees (dated 9/27/78) and University Computing Policy Formulation, Monitoring and Implementation (dated 4/15/81).

D. In III.B.3, updated title and link to the CU Denver | Anschutz Medical Campus policy (11/25/15).

ATTACHMENT - Campus Acceptable Use Policy Guidance

Recognizing that the campuses and system administration may also require additional standards for the use of technology, the campuses and system administration may extend the use of IT APS with policies and guidance specific to each environment. When drafting such policies the campuses should consider the following:

a. How do employees report violations of IT policy to the campus chief information officer or chief technology officer?
b. How are sanctions for violations reviewed by campus administrative officers such as vice chancellors and deans?
c. What additional guidance is required regarding IT resource user accountability for ethical and responsible use of IT resources. Examples include:
    i. respect for the rights of others: respecting privacy, using only authorized access, respecting intellectual property, not knowingly doing harm to others or denying service to others;
    ii. respect for resources: using good security practices, not knowingly doing harm to data, systems or the property of others, not wasting resources;
    iii. academic and professional integrity including honest representation of identity and authorship; and
    iv. proper use of resources: while some personal use of IT resources is permitted, such personal use should not interfere with academic, research, or administrative needs.
d. IT resource users are responsible for knowing and complying with applicable laws, policies, and procedures. Campus leadership and employee supervisors have responsibility for providing appropriate training regarding applicable laws, policies and procedures. What process will the campus communicate and train employees annually regarding employee responsibilities?
e. Should it be necessary for the university administration to access university accounts without employee prior consent, for example to access for administrative and/or investigative purposes, approval must be provided by the appropriate administrative officer (such as the campus chancellor, vice chancellor, dean or vice president). Otherwise, unless legally required employees must be notified of such access by another person.
f. Any use of university IT resources involving copyrighted materials must comply with applicable provisions of Federal copyright law and specific license agreements.