This document includes:

- A “PROPOSED POLICY DRAFT” that displays a clean copy of the proposed policy if approved.

- A “PROPOSED POLICY CHANGES IN REDLINE FORMAT” that displays a redline version of the proposed changes from the current approved version.

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

ADMINISTRATIVE POLICY STATEMENT

Policy Title: IT Security Program Policy

APS Number: 6005 **APS Functional Area: Information Technology**

Brief Description:	The IT Security Program serves as the core for the University's IT security and risk activities and provides requirements to users and administrators of IT resources via the noted security and risk standards. These standards help ensure information is secured appropriately, the university information and IT resources are available, and document the best practices and control activities that help mitigate the University technology risks. This Administrative Policy Statement encompasses all IT Security-related requirements as outlined in the noted security standards.
Effective:	October 1, 2023 (Pending)
Approved by:	President Todd Saliman (Pending)
Responsible University Officer:	Chief Information Security Officer
Responsible Office:	Office of Information Security
Policy Contact:	security@cu.edu
Supersedes:	IT Security Program Policy-January 7, 2010
Last Reviewed/Updated:	October 1, 2023 (Pending)
Applies to:	Universitywide or as specifically defined by each policy section.

Reason for Policy: Defines roles, responsibilities and requirements for the users and administrators of IT resources to mitigate risk involving the confidentiality, integrity and availability of university data and IT systems.

NOTE: Several sections of the prior version of APS 6005 will remain in effect until they have completed transition to other APS documents and associated standards. Once that work is complete (expected in early 2024), these sections will be removed from this document. These sections can be found at the bottom of this document.

Those sections include:

- ***IT Resource User Responsibilities***
- ***IT Security in Personnel Job Descriptions, Responsibilities and Training***
- ***IT Security in University Operations, Business Continuity Planning, and Contracting***
- ***IT Service Provider Security***

IT SECURITY PROGRAM

Policy Overview: IT Security Program

I. INTRODUCTION

This Administrative Policy Statement (APS) is the parent policy for the university's Information Technology (IT) security standard suite, which defines and establishes the IT Security Program (Program). The Program serves as the core for the university's IT security activities and provides general guidance to the users and administrators of *IT resources* to help mitigate the risks to university information and IT resources.

More specifically, this policy assigns responsibilities for the oversight and day-to-day management of the Program. These fundamental responsibilities are essential to ensure the Program provides timely and effective guidance to the users and administrators of *IT resources* in the face of almost continuous change. The effectiveness of this guidance requires that the Program be frequently reviewed and adapted to fit the evolving needs of the University and its stakeholders.

II. POLICY STATEMENT

A. The goals of the University IT Security Program overall are as follows:

1. Identify the IT security roles and responsibilities of the Chief Information Security Officer, the Information Security Officer or designated campus IT security authority, and the Cyber Risk and Compliance Committee (CRCC).
2. Codify standards to mitigate IT security risks related to data and IT resources used across the university.
3. Ensure members of the university community are aware of the university requirements for managing security risks related to university information and IT resources.

B. The following principles shall be followed in implementing the University *IT Security Program*:

1. Each campus and System Administration shall adopt the Program and may create campus-specific policies, standards, and procedures to meet special campus needs, if they do not conflict with the requirements in the Program.
2. IT security risk management decisions shall be made by appropriate authorities with jurisdiction over those areas affected by the risks.
3. University information shall be subject to the Program regardless of the information's physical location, the nature of the device or media upon which it is stored, or the person in possession or control of the information.

IT SECURITY PROGRAM

Policy Overview: IT Security Program

C. Roles and Responsibilities for the University *IT Security Program*.

1. The Program shall be managed and monitored collaboratively by the Chief Information Security Officer (CISO), campus Information Security Officers (ISOs), CRCC, and other university representatives as appropriate. Program management responsibilities are as follows:
    a. CISO
        1. Provides day-to-day management for the systemwide elements of the Program. Reviews and reports on Program status, at least annually to the Board of Regents, President, Chancellors, IT Governance Executive Committee, and CRCC.
        2. In cooperation with the CRCC, advises the President, Chancellors, and ISOs in accordance with Program goals and requirements.
        3. Oversees the development and maintenance of procedural statements and standards for *IT security* and advises ISOs on the alignment of campus IT security procedures with administrative standards.
        4. Oversees the development and maintenance of IT security compliance testing and reporting to help monitor effectiveness and adherence to the administrative standards for IT Security.
        5. Develops and manages processes for tracking and reporting IT security risks at a systemwide level in coordination with Risk Management. Provides recommendations based on risk management activities to mitigate risk.
        6. Establishes a baseline for IT security training and awareness for all university employees, as well as IT service providers, and provides a method for tracking compliance.
        7. Provides coordination assistance via the Data Exposure Process when IT security events span multiple campus IT security programs
        8. In coordination with campus IT security leadership, provides reporting about major IT security incidents to the President, Board of Regents, CRCC and others as appropriate.
    b. Chief Information Officers (CIOs) or designated senior IT leaders
        1. Accountable for overall campus adherence to systemwide IT security policies, standards, and procedures.
    c. ISOs or designated senior IT security leaders
        1. Provide day-to-day campus IT security program management and oversight in alignment with university and campus policies, standards, and procedures.
        2. Collaborate with the CISO to conduct systemwide Program reviews and IT security risk management reporting.
        3. Advise *Organizational Units* on the evaluation and management of IT security risks and issues.
        4. Lead the preparation, approval, and maintenance of campus-specific IT security policies, standards, and procedures. Provide implementation guidance to IT service providers and department heads as appropriate.
        5. Collaborate with the CISO on the systemwide IT security awareness and training program. Additional campus IT security awareness and training requirements may be established.
        6. Develop and maintain a campus IT security incident response process and/or policy. As appropriate, coordinate with systemwide response processes.
        7. In coordination with appropriate employee and student discipline groups, address non-compliance with the Program.
    d. CRCC
        1. The CRCC provides steering and guidance for the Program. The CRCC shall be composed of members as defined in the CRCC charter. The CRCC shall provide systemwide IT security oversight and guidance as defined in the charter.
    e. IT resource users
        1. *IT resource users* shall ensure that their actions adhere to applicable university IT security policies, standards, and procedures.

2. To the extent that an individual establishes, manages, or oversees relationships with third parties that provide services handling university data, they must work with procurement and IT security teams to ensure third parties are required to adhere to applicable IT security policies, standards, and procedures.

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

The IT Security Program serves as the core for the University's IT security activities and provides general guidance to the users and administrators of IT resources to help ensure the confidentiality of personal information, the availability of university information and IT resources, and the best practices and control activities that should be in place to help mitigate the risks of using technology associated with the University. The related documents that support this APS include:

Related documents	Effective Date	Compliance Date
APS 6001 – Providing and Using Information Technology		
IT Security Controls Standard (updated to 800-171)	**10/01/2023**	**10/1/2024**
IT Security Responsibilities (new)		
Campus Acceptable Use Policies (links)		
APS 6002 - Electronic Communications		
APS 6010 - Data Governance		
Data Classification		

IV. HISTORY

Effective October 1, 2023, this APS was rewritten to establish a new format for the creation of security-related standards within the University.

The following sections of the prior version of APS 6005 remain in effect until they have completed transition to other APS documents and associated standards. Once that work is complete (expected in early 2024), these sections will be removed from this document.

IT SECURITY PROGRAM

Section 1: IT Resource User Responsibilities[1,2]

Brief Description: Establishes *IT security* requirements for all *IT resource users* in protecting *University information* and *IT resources*.

Applies to: *IT Resource Users*

SECTION 1 – IT RESOURCE USER RESPONSIBILITIES

I. INTRODUCTION

This section of the IT Security Program Policy establishes the Information Technology (IT) security safeguards that must be taken by every person using a University *IT resource* or otherwise accessing *University information*. Additional safeguards may be appropriate, depending on the situation and its inherent risk to *University information* and *IT resources*.

This policy does not impose restrictions that are contrary to the University's established culture of sharing, openness, and trust. However, the University is committed to implementing the safeguards necessary to ensure the privacy of personal information, the availability of *University information* and *IT resources*, and the integrity of University operations.

CU has three levels of data classification. These are: *Highly Confidential*, *Confidential*, and *Public*. For more information please review the University of Colorado Process for Data Classification and System Security Categorization.

II. POLICY STATEMENT

A. It is the responsibility of every *IT resource user* to know the University's *IT security* requirements and to conduct her/his activities accordingly. *IT resource users* shall comply with the following requirements:

1. **Protect the Privacy of Others.** Users shall respect the privacy of others when handling **Error! Hyperlink reference not valid.** *information* and shall take appropriate precautions to protect that information from unauthorized disclosure or use.

2. **Protect *Highly Confidential* or *Confidential Information* on Workstations and Mobile Devices.** Ordinarily, *Highly Confidential information* shall not be stored on workstations and mobile computing devices (laptops, flash drives, backup disks, etc.) unless specifically justified for business purposes and adequately secured. If *Highly Confidential information* is stored on a workstation or mobile computing device or transmitted to an external network or organization, *IT resource users* shall *encrypt* or adequately protect that information from disclosure. If *Confidential information* is stored on a workstation or mobile computing device or transmitted to an external network or organization, *IT resource users* shall adequately protect that information from disclosure. In addition to *encryption*, adequate protections may include the use of passwords, automatic logoffs, and secure Internet transmissions. IT Resource users are required to secure university information on

[1] Section 1 – IT Resource User Responsibilities was revised effective January 1, 2014.

[2] The terms private information and restricted information were changed to highly confidential information and confidential information, respectively – as of April 2014.

personally owned and/or institutionally provided mobile devices in accordance with the mobile device security standards. The protection of Highly Confidential or *Confidential information* shall be in accordance with campus *IT security* requirements and other guidance as available from the appropriate IT service center or help desk.

3. **Protect Highly Confidential Data from Unauthorized Physical Access.** *IT resource users* shall keep all *Highly Confidential* or *Confidential information* out of plain sight unless in use and shall not leave such information displayed when it is not needed.

4. **Protect Workstations and Other Computing Devices.** *IT resource users* are responsible for helping to maintain the security of workstations and other computing devices by striving to protect them from unauthorized access and malicious software infections (e.g., viruses, worms, and spyware). Users shall consult the appropriate IT service center or help desk for guidance on protecting their computing devices.

5. **Protect Passwords, Identification Cards, and Other Access Devices.** Passwords, tokens identification cards, and other access devices are used to authenticate the identity of individuals and gain access to University resources. Each person is responsible for protecting the access devices assigned to her or him and shall not share passwords or devices with others. If a password or access device is compromised, lost, or stolen, the individual shall report this to the appropriate IT service center or help desk as soon as possible so that the access device is not used by an unauthorized person.

6. **Report Security Violations, Malfunctions, and Weaknesses.** *IT resource users* shall report security related events; known or suspected violations of *IT security* policy; and inappropriate, unethical, and illegal activities involving University *IT resources*. Users shall follow the reporting process applicable to their campus. If unsure of the local incident reporting process, users shall call the appropriate IT service center or help desk.

7. **Utilize *University Information* and *IT Resources* for Authorized Purposes Only**. *IT resource users* shall access or otherwise utilize *University information* and *IT resources* only for those activities they are specifically authorized and in a manner consistent with University policies, federal and state laws, and other applicable requirements.

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

A. Administrative Policy Statements (APS) and Other Policies

The IT Security Program serves as the core for the University's *IT security* activities and provides general guidance to the computing community on ensuring the privacy of personal information and the availability of *University information* and *IT resources* and encompasses all related IT Security requirements, including the following policy sections:

- **IT Resource User Responsibilities**
- **IT Security in Personnel Job Descriptions, Responsibilities and Training**
- **IT Security in University Operations, Business Continuity Planning, and Contracting**
- **IT Service Provider Security**
-

The Laws of the Regents, section 14.A.4 states that *employees* shall be responsible for the safekeeping and proper maintenance of university property in their charge. The administrative policy "Fiscal Code of Ethics" prohibits use of University property for personal gain.

The "Use of Electronic Mail" Administrative Policy Statement sets forth the appropriate use of University email and expectations for privacy in email communications.

System-wide Mobile Device Security Standards
Standards for Data classification and System security categorization

B. Other Resources (i.e. training, secondary contact information)

Educational information and resources are available on the information security website: http://www.cu.edu/ois

Return to Main Policy Page

IT SECURITY PROGRAM

Section 2: IT Security in Personnel Job Descriptions, Responsibilities and Training

Brief Description: Establishes requirements for incorporating employee responsibilities for *IT security* into performance management processes, as well as ensuring *employees* are aware of their *IT security* responsibilities and are adequately trained to fulfill those responsibilities.

Applies to: Supervisors

SECTION 2 – IT SECURITY IN PERSONNEL JOB DESCRIPTIONS, RESPONSIBILITIES AND TRAINING

I. INTRODUCTION

Information technology (IT) security responsibilities are, to various degrees, part of all duties within the University. For *employees* and job candidates it is important that the applicable *IT security* responsibilities are known, documented, and accepted as part of the terms and conditions of employment.

II. POLICY STATEMENT

A. *IT Security* Guidance and Support

1. Campus *Information Security Officers* shall, in collaboration with the Chief Information Security Officer (CISO), provide information and guidance to supervisors on implementing the requirements of this policy.
2. Campus *Information Security Officers* shall establish and oversee *IT security* awareness and education programs for their respective campuses.

B. Supervisor Responsibilities for *IT Security*

1. Supervisors shall ensure that all *employees* within their areas of authority are aware of their *IT security* responsibilities and that these responsibilities are incorporated into *employee* performance management processes and addressed in recruitment and hiring practices.
2. Supervisors shall ensure that *employees* provide a signed, written, or other documented acknowledgment of their *IT security* responsibilities as a condition of gaining access to *University information* and *IT resources*. Where feasible, acknowledgements should be provided prior to gaining access or as soon afterward as reasonably possible. Personnel supervising authorities shall track and/or maintain the records of *employee* acknowledgements.
3. Supervisors, in consultation with the campus *Information Security Officer*, are encouraged to make recommendations on the designation of positions with significant *IT security* responsibilities as "security-sensitive positions."

C. *Employee* Training

1. Supervisors shall ensure that *employees* are adequately trained to fulfill their *IT security* responsibilities. *Employees* with elevated computing privileges (e.g., server support technicians, user account managers, or web page administrators) may require additional, specialized training for carrying out their *IT security* responsibilities effectively.
2. All University *employees* including associates and other individuals, who require the use of University *IT resources* to perform their duties, shall receive initial training and periodic refresher training relevant to their *IT security* responsibilities.
3. Supervisors shall coordinate their local *IT security* training initiatives with the campus *Information Security Officer*.

D. Changes in *Employee* Duties or Employment Status

1. Supervisors shall provide timely notification to the appropriate service center or help desk when an *employee*'s duties or employment status changes so that access to *University information* and *IT resources* is adjusted accordingly.

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

A. Administrative Policy Statements (APS) and Other Policies

The IT Security Program serves as the core for the University's *IT security* activities and provides general guidance to the computing community on ensuring the privacy of personal information and the availability of *University information* and *IT resources* and encompasses all related IT Security requirements, including the following policy sections:

- **IT Resource User Responsibilities**
- **IT Security in Personnel Job Descriptions, Responsibilities and Training**
- **IT Security in University Operations, Business Continuity Planning, and Contracting**
- **IT Service Provider Security**
-

The "Use of Electronic Mail" Administrative Policy Statement sets forth the appropriate use of University email and expectations for privacy in email communications.

B. Procedures

IT Security Training Standards and Core Topics

C. Other Resources (i.e. training, secondary contact information)

Educational information and resources are available on the information security website: http://www.cu.edu/ois

Return to Main Policy Page

IT SECURITY PROGRAM

Section 3: IT Security in University Operations, Business Continuity Planning, and Contracting

Brief Description: Requires *IT security* safeguards to be integrated into University operations, asset management, contracting, *business continuity* planning, *disaster preparedness*, and enterprise *risk management* processes.

Applies to: *Organizational Unit* Directors/Chairs

SECTION 3 – IT SECURITY IN UNIVERSITY OPERATIONS, BUSINESS CONTINUITY PLANNING, AND CONTRACTING

I. INTRODUCTION

University operations are organized into *Organizational Units* that develop and execute strategic and tactical plans to carry out the University's mission and achieve its objectives. In doing so, these units collect, store, and process information that is essential to University operations and must be protected from unauthorized use and disclosure. To ensure that *University information* is protected in a manner consistent with other strategic assets, *Organizational Units* must implement Information Technology (IT) security safeguards as a part of normal University operations.

II. POLICY STATEMENT

A. *IT Security* Guidance and Support

1. Campus *Information Security Officers* shall, in collaboration with the Chief Information Security Officer (CISO), provide information and guidance to *Organizational Units* on implementing the requirements of this policy.

B. Information Classification

1. Campus *Information Security Officers* shall provide security standards based on the criticality and sensitivity of *University information* for their respective campuses.
2. *Organizational Unit* directors / chairs or their designees shall, following guidance from the campus *Information Security Officer*, ensure that appropriate *IT security* safeguards are in place for the *University information* and *IT resources* under their care. The appropriateness of the safeguards shall be determined by the criticality and sensitivity of information involved, campus policies and guidance, and applicable external requirements (e.g., state and federal laws, and industry standards).

C. Continuity of Operations

1. *Organizational Unit* directors / chairs or their designees, with guidance from the campus *Information Security Officer*, shall ensure that *business continuity* and *disaster preparedness* plans include all appropriate *IT security* requirements and are reviewed, tested, and updated as needed to ensure the viability of such plans.

D. *IT Security* Requirements in RFPs, Contracts, and Other Service Arrangements

1. *Organizational Unit* directors / chairs or their designees shall, with guidance from the Procurement Service Center and the *Information Security Officer*, ensure that Request for Proposals (RFP), contracts, or other service arrangements include adequate safeguards so that contractors and other third parties protect *University information* at a level that is equal to or greater than that required of University *employees*.
2. *Organizational Unit* directors / chairs or their designees, with guidance from the campus Information Security Officers, shall ensure that access to *University information* and *IT resources* by contractors and third parties follows established policies and procedures.

Risk Evaluation and Handling

1. *Organizational Unit* directors / chairs or their designees shall, with guidance from the campus *Information Security Officer*, evaluate risks related to the protection of *University information* and *IT resources* in their care. *Organizational Unit* directors / chairs or their designees shall forward issues of risk to campus authorities with appropriate jurisdiction over those affected by the risks.

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

A. Administrative Policy Statements (APS) and Other Policies

The IT Security Program serves as the core for the University's *IT security* activities and provides general guidance to the computing community on ensuring the privacy of personal information and the availability of *University information* and *IT resources* and encompasses all related IT Security requirements, including the following policy sections:

- **IT Resource User Responsibilities**
- **IT Security in Personnel Job Descriptions, Responsibilities and Training**
- **IT Security in University Operations, Business Continuity Planning, and Contracting**
- **IT Service Provider Security**
-

The Laws of the Regents, section 14.A.4 states that *employees* shall be responsible for the safekeeping and proper maintenance of university property in their charge.

B. Other Resources (i.e. training, secondary contact information)

Educational information and resources are available on the Office of Information Security website.

Return to Main Policy Page

IT SECURITY PROGRAM

Section 4: IT Service Provider Security

Brief Description: Requires that *IT service providers* (e.g., server and workstation support, programmers, webmasters, user account administrators) incorporate *IT security* safeguards into the IT services and products provided to the University community.

Applies to: *IT Service Providers*

SECTION 4 – IT SERVICE PROVIDER SECURITY

I. INTRODUCTION

This section of the IT Security Program Policy sets forth the Information Technology (IT) security safeguards that must be taken by every *IT service provider*. These safeguards are necessary to protect *University information* from inappropriate access, disclosure and misuse; provide assurances that information resources are available as needed for University business; and comply with applicable policies, laws, regulations, rules, grants, and contracts. Campus *Information Security Officers* may require additional safeguards so as to address campus specific risks or compliance requirements.

II. POLICY STATEMENT

A. *IT Security* Oversight and Guidance

Campus *Information Security Officers* in collaboration with the Chief Information Security Officer (CISO) shall provide guidance and information as needed to *IT service providers* on implementing the requirements of this policy. *IT service providers* shall be aware that purchases of IT goods and services may be subject to a security review by the campus *Information Security Officer* or a designated campus authority.

Organizational Unit directors / chairs shall be aware of their responsibilities, as described by IT Security in University Operations, Continuity, and Contracting, to ensure that adequate safeguards are implemented for the *IT resources* under their control.

B. Life Cycle Management

Campus *IT service providers* shall ensure that *IT security* controls are appropriately implemented and managed throughout the life of the *IT resources* under their responsibility. This is to ensure that security is addressed in the design and purchase of new systems, implementation of new or modified systems, maintenance of existing systems, and removal from service of end-of-life systems.

C. *IT Resource* Security Management

Providing an IT service is a complex undertaking that requires continuous monitoring, maintenance, and system management to ensure that *University information* is adequately protected as it is processed, stored, and transmitted. Therefore, *IT service providers* shall implement the following controls where appropriate for the *IT resources* under their responsibility:

1. System and application security management. *IT resources* shall be maintained according to industry and vendor best practices to ensure that system and application updates, vulnerability fixes, security patches, and other modifications are applied in a timely fashion. Where applicable these practices shall include vulnerability management, system/application hardening, and security testing.

2. Malicious activity protection. *IT resources* that transmit or receive information on a University-managed network shall be adequately protected from malicious activities, such as viruses, worms, and denial of service attacks.

3. Data backup and recovery. *University information* shall be backed up and retained as appropriate for business needs, **retention** schedules, and legal requirements as provided by law or related university policy. Data backups shall be tested where appropriate to ensure the effective recovery of information.

4. Media handling and storage. Electronic storage media (e.g., CD-ROMs, memory sticks, disk drives, tapes, cartridges, etc.) shall be appropriately protected from loss and unauthorized access. All media containing Highly Confidential and *Confidential information* shall be stored in a secure location and adequately protected with a safeguard that restricts access to authorized personnel only. In addition, Highly Confidential information stored on portable electronic media shall be encrypted or otherwise adequately protected based on security standards and guidance from the campus Information Security Officers.

5. Disposal of electronic equipment and media. Computing and network equipment and storage media shall be purged of all *University information* so that information is not recoverable, or destroyed before disposal or release from University control to a third party. In the rare event the information is not purged prior to release or the device destroyed prior to disposal, the *IT service provider* shall acquire confirmation from the contracted third party that the information is properly purged. For equipment and media that is to be redeployed within the University, the *IT service provider* shall purge all information not authorized for access by the receiving person(s) prior to redeployment.

D. **Access Management**

Although *students*, faculty, and staff require access to *University information* resources for academic and business purposes, this access must be limited to what is needed for his/her work. Use of resources beyond that which is authorized results in unnecessary risks to *University information* with no corresponding academic or business value.

1. User access management. *IT service providers* shall manage user access to the *IT resources* under their responsibility, so that such access is appropriately authorized, documented, and limited to that which is needed to perform authorized tasks. Because a user's responsibilities and relationships with the University change over time, *IT service providers* shall ensure that user access privileges are regularly reviewed and adjusted to comply with currently authorized activities.

2. *IT resource* access controls. *IT service providers* shall ensure that *IT resources* under their responsibility (developed, purchased or otherwise used to handle *University information*) have adequate features and controls to support the proper management of user access as described in section II.D.1.

3. Network security controls. *IT service providers* shall ensure that electronic access to and use of the campus data networks under their responsibility is adequately controlled to protect data network equipment and other networked *IT resources*.

E. **Physical and Environmental Security**

University data centers and *IT resources* shall be sufficiently protected from physical and environmental threats to prevent the loss, damage, or compromise of assets, and interruption to business activities.

1. Data centers. Data center owners, managers, or their designees shall, following guidance from the campus *Information Security Officer*, ensure that data center facilities under their responsibility have adequate physical security safeguards. These safeguards may include: physical barriers (e.g., walls, gates, locked doors), access controls (e.g., identification cards, visitor escorts and logs, facility/equipment repair records), environmental controls and protections (e.g., uninterruptible power supplies, generators, temperature and humidity systems, fire suppression units).

2. *IT resources*. *IT service providers* shall ensure that all *IT resources* under their responsibility have adequate physical security safeguards. While the value of these *IT resources* may not rise to that found in a data center, the physical protections normally afforded to *IT resources* within a data center should be employed where reasonable and appropriate.

F. **Incident Detection and Reporting**

IT service providers shall monitor for and report security breaches or other significant security events involving the *IT resources* under their control, following guidance from the campus *Information Security Officer*.

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

A. Administrative Policy Statements (APS) and Other Policies

The IT Security Program serves as the core for the University's *IT security* activities and provides general guidance to the computing community on ensuring the privacy of personal information and the availability of *University information* and *IT resources* and encompasses all related IT Security requirements, including the following policy sections:

- **IT Resource User Responsibilities**
- **IT Security in Personnel Job Descriptions, Responsibilities and Training**
- **IT Security in University Operations, Business Continuity Planning, and Contracting**
- **IT Service Provider Security**

The Laws of the Regents, section 14.A.4 states that employees shall be responsible for the safekeeping and proper maintenance of university property in their charge.

B. Other Resources (i.e. training, secondary contact information)

Educational information and resources are available on the Office of Information Security website.

Return to Main Policy Page

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

ADMINISTRATIVE POLICY STATEMENT

Policy Title: IT Security Program Policy

APS Number: 6005 **APS Functional Area: Information Technology**

Brief Description: The IT Security Program serves as the core for the University's *IT security* and risk activities and provides ~~general guidance to the computing community on ensuring the privacy of personal information and the availability of *University information* and *IT resources*~~requirements to users and administrators of IT resources via the noted security and risk standards. These standards help ensure information is secured appropriately, the university information and IT resources are available, and document the best practices and control activities that help mitigate the University technology risks. This Administrative Policy Statement encompasses all IT Security-related requirements as outlined in the ~~following policy sections~~noted security standards.~~:~~

	~~IT Security Policy Sections~~	~~Effective Date~~	~~Last Reviewed~~	~~Applies To~~	~~Page~~
~~1~~	~~IT Resource User Responsibilities~~	~~1/1/2014~~	~~1/1/2014~~	~~IT Resource Users~~	~~6~~
~~2~~	~~IT Security in Personnel Job Descriptions, Responsibilities and Training~~	~~3/1/2011~~	~~3/1/2011~~	~~Supervisors~~	~~8~~
~~3~~	~~IT Security in University Operations, Business Continuity Planning, and Contracting~~	~~3/1/2011~~	~~3/1/2011~~	~~Organizational Unit Directors/Chairs~~	~~10~~
~~4~~	~~IT Service Provider Security~~	~~3/1/2011~~	~~3/1/2011~~	~~IT Service Providers~~	~~12~~

Effective: ~~See above.~~October 1, 2023

Approved by: President ~~Bruce D. Benson~~Todd Saliman

Responsible University Officer: ~~Vice President, Employee and Information Services~~Chief Information Security Officer

Responsible Office: Office of Information Security

Policy Contact: security@cu.edu

Supersedes: ~~IT Security Program Policy January 7, 2010; IT Resource User Responsibilities; IT Security in Personnel Job Descriptions, Responsibilities and Training; IT Security in University Operations, Business Continuity Planning, and Contracting; and IT Service Provider Security.~~IT Security Program Policy-January 7, 2010

Last Reviewed/Updated: ~~See above.~~October 1, 2023

Applies to: University-wide or as specifically defined by each policy section.

Reason for Policy: ~~Establishes the required roles, responsibilities, and functions for the effective management of the University's IT Security Program and provides general guidance to the computing community on ensuring the privacy of personal information and the availability of *University information* and *IT resources*~~Defines roles, responsibilities and

requirements for the users and administrators of IT resources to mitigate risk involving the confidentiality, integrity and availability of University data and IT systems.

NOTE: Several sections of the prior version of APS 6005 will remain in effect until they have completed transition to other APS documents and associated standards. Once that work is complete (expected in early 2024), these sections will be removed from this document. These sections can be found at the bottom of this document.

Those sections include:

- ***IT Resource User Responsibilities***
- ***IT Security in Personnel Job Descriptions, Responsibilities and Training***
- ***IT Security in University Operations, Business Continuity Planning, and Contracting***
- ***IT Service Provider Security***

IT SECURITY PROGRAM

Policy Overview: IT Security Program

I. INTRODUCTION

This Administrative Policy Statement (APS) is the parent policy for the ~~U~~university's Information Technology (IT) security standard ~~policy~~ suite, which defines and establishes the *IT Security Program* (Program). The Program serves as the core for the ~~U~~university's *IT security* activities and provides general guidance to the users and administrators of IT resources to help mitigate the risks to ~~computing community on ensuring the privacy of personal information and the availability of~~ *University information* and *IT resources*.

More specifically, this policy assigns responsibilities for the oversight and day-to-day management of the Program. These fundamental responsibilities are essential to ~~ensuring~~ ensure ~~that~~ the Program provides timely and effective guidance to the users and administrators of IT resources~~University computing community~~ in the face of almost continuous change. The effectiveness of this guidance requires that the Program be frequently reviewed and adapted~~molded~~ to fit the evolving needs of the University and its stakeholders. ~~This policy also includes the following IT security related sections:~~

~~Sections~~		~~Applies To~~	~~Page~~
~~1~~	~~IT Resource User Responsibilities~~	~~IT Resource Users~~	~~6~~
~~2~~	~~IT Security in Personnel Job Descriptions, Responsibilities and Training~~	~~Supervisors~~	~~8~~
~~3~~	~~IT Security in University Operations, Business Continuity Planning, and Contracting~~	~~Organizational Unit Directors/Chairs~~	~~10~~
~~4~~	~~IT Service Provider Security~~	~~IT Service Providers~~	~~12~~

II. POLICY STATEMENT

A. The goals of the University *IT Security Program* overall are as follows:

~~1. All members of the University community are aware of and are sufficiently trained to carry out their responsibilities for protecting *University information* and *IT resources*.~~
~~2. *University information* is regarded as a strategic organizational asset and is treated in a manner consistent with that of other strategic assets, such as financial and facility assets.~~
~~3. *IT security* is not considered a technical concern, but is addressed as a strategic business issue by integrating *IT security* safeguards into University business processes.~~
~~4. University resources are applied judiciously to *IT security* issues by focusing on those that represent the greatest risk to University operations and information.~~
~~5. *IT security* incidents are promptly detected and responded to in a manner that limits the impact to the security of *University information* and the operations of the University.~~

1. Identify the IT security roles and responsibilities of the Chief Information Security Officer, the Information Security Officer or designated campus IT security authority, and the Cyber Risk and Compliance Committee.
2. Codify standards to mitigate IT security risks related to data and IT resources used across the university.
3. Ensure members of the university community are aware of the University requirements for managing security risks related to university information and IT resources.

B. The following principles shall be followed in implementing the University *IT Security Program*:

1. Each campus and System Administration shall adopt the Program and may create campus-specific policies, standards, and procedures~~all applicable elements of the Program and may make modifications to specific Program elements~~ to meet special campus needs, if they do not conflict with the requirements in the Program.

~~as long as the modifications are as stringent as and meet the intended functionality of the applicable Program elements.~~

2. *IT security ~~R~~risk management* ~~methods shall be used to identify and manage risks to *University information* and *IT resources. Risk management*~~ decisions shall be made by appropriate authorities with jurisdiction over those areas affected by the risks.
3. *University information* shall be ~~adequately protected~~subject to the Program regardless of the information's physical location, the nature of the device or media upon which it is stored, or the person~~s~~ in possession or control of the information.

C. Roles and Responsibilities for the University *IT Security Program*.

1. The Program shall be managed and monitored collaboratively by the Chief Information Security Officer (CISO), campus *Information Security Officers (ISOs)*, CRCC~~Security Advisory Committee (SAC)~~, and other ~~U~~university representatives as appropriate. Program management responsibilities are as follows:
   a. CISO ~~(Chief Information Security Officer)~~
      1. Provide~~s~~ day-to-day management for the systemwide elements of the Program. Review~~s~~ and report~~s~~ on Program status, at least annually ~~effectiveness~~ to the Board of Regents, *President*, Chancellors, IT Governance Executive Committee and CRCC~~SAC as appropriate~~.
      2. In cooperation with the ~~SAC~~CRCC, ~~provide security advice~~ advises~~to~~ the *President*, Chancellors, and ISOs ~~campus *Information Security Officers*~~ in accordance with Program goals and requirements.
      3. Oversee the development and maintenance of ~~Administrative Policy Statements~~ procedural statements and standards for *IT security* and advise~~s campus *Information Security Officers*~~*ISOs* on the alignment of campus *IT security* ~~policies~~procedures with ~~A~~administrative ~~Policy Statements~~standards.
      4. Oversees the development and maintenance of IT security compliance testing and reporting to help monitor effectiveness and adherence to the administrative standards for IT security. ~~Provide guidance to campus *Information Security Officers* on *risk management* processes to ensure that *IT security* safeguards are applied in a judicious and effective manner. Submit reports to the SAC on *risk management* decisions as appropriate.~~
      5. Develops and manages processes for tracking and reporting IT security risks at a systemwide level in coordination with Risk Management. Provides recommendations based on risk management activities to mitigate risk.~~Establish training standards for campus *IT security* awareness and education programs.~~
      6. Establishes a baseline for IT security training and awareness for all university employees, as well as IT service providers, and provides a method for tracking compliance.~~When *IT security* incidents affect multiple campuses, lead investigations and coordinate with and/or report to the *President*, Chancellors, , Legal, SAC, and others as appropriate.~~
      7. Provides coordination assistance via the Data Exposure Process when IT security events span multiple campus IT security programs.
      8. In coordination with campus IT security leadership, provides reporting about major IT security incidents to the President, Board of Regents, CRCC and others as appropriate.
   b. Chief Information Officer (CIO) or designated senior IT leaders
      1. Accountable for overall campus adherence to systemwide IT security policies, standards, and procedures.~~The CIO is an individual designated by the Chancellor on each campus with oversight authority for all IT operations on that campus. These individuals have the authority to enforce the requirements of University and campus policies for information security.~~
      ~~2. Authorize new IT operations, shut down IT operations that are out of compliance with policy, or transfer management of those operations to a department or service provider with the requisite capabilities.~~
   c. *ISOs or designated senior IT security leaders~~Information Security Officers~~*
      ~~Campus *Information Security Officers* serve in a variety of technical and non-technical roles for a specific University campus. The *Information Security Officers* shall:~~
      1. Provide day-to-day campus IT security ~~P~~program management and oversight in alignment with university and campus policies, standards and procedures~~for their campus, advise *Organizational Units* on *IT security* issues, and assist the CISO with Program reviews and reporting~~.

2. ~~Assist *Organizational Units* with evaluating risks to *University information* and the CISO~~ Collaborate with the CISO to conduct systemwide Program reviews and ~~with~~ IT security *risk management* reporting.
3. ~~Assist with the preparation, approval, and maintenance of campus-specific *IT security* policies, procedures, and guidelines as appropriate.~~ Advise *Organizational Units* on the evaluation and management of IT security risks and issues.
4. Lead the preparation, approval, and maintenance of campus-specific IT security policies, standards, and procedures. Provide implementation guidance ~~on implementation~~to IT service providers and department heads~~of unit-specific *IT security* policies, procedures, and guidelines~~ as appropriate.
5. Collaborate with the CISO on the systemwide IT security awareness and training program. Additional campus IT security awareness and training requirements may be established~~Establish and manage an *IT security* awareness and education program for campus *IT resource users* and provide guidance to *Organizational Units* on supplementing program events with unit-specific training~~.
6. Develop and maintain a campus ~~When~~ *IT security* incident~~s~~ response process and/or policy. ~~affect a single campus, lead investigations~~As appropriate, coordinate with systemwide response processes~~and issue timely reports to the Chancellor or designee, affected campus units, CISO, Legal, and others as appropriate~~.
7. In coordination with appropriate employee and student discipline groups, address non-compliance with the Program.

~~d. SAC (Security Advisory Committee)~~

~~The SAC provides oversight of and support for the *IT Security Program* and is composed of members representing a cross section of the University community. SAC members are appointed by the *President* or designee.~~

~~1. Advise, inform, and coordinate with the CISO as appropriate to promote and support the Program and to ensure that Program requirements reflect and support the functional requirements, external requirements, and the mission of the University.~~
~~2. Advise the *President* and the CISO as appropriate to ensure that University-wide *IT security* policies, procedures, and guidelines reflect and support the functional requirements, external requirements, and the mission of the University.~~
~~3. In collaboration with the CISO advise the University *President* and Chancellors on *risk management* decisions and Program direction to ensure alignment with University objectives.~~

d. CRCC

1. The CRCC provides steering and guidance for the Program. The CRCC shall be composed of members as defined in the CRCC charter. The CRCC shall provide systemwide IT security oversight and guidance as defined in the charter.

e. IT resource users

1. *IT resource users* shall ensure that their actions adhere to applicable university IT security policies, standards, and procedures.
2. To the extent that an individual establishes, manages, or oversees relationships with third parties that provide services handling university data, they must work with procurement and IT security teams to ensure third parties are required to adhere to applicable IT security policies, standards, and procedures.

~~2. Although campus *Information Security Officers* provide day-to-day management of the Program and general advice on *IT security* issues, the following campus support responsibilities are required:~~

~~a. *Organizational Unit* (typically a department with an independent budget represented in the Finance System) directors and chairs or their designees are responsible for ensuring that all applicable Program and *IT security* policy requirements are implemented in their respective units. While *Organizational Unit* directors and chairs may delegate these responsibilities, they may only be delegated to a single person in an *Organizational Unit* who has budget authority for the entire unit. *Organizational Unit* directors and chairs or their designees shall report any security weaknesses, concerns, or breaches to the campus *Information Security Officer*. The campus *Information Security Officer* will work with the appropriate campus Officer and CIO to determine if the risk caused by a security weakness may be accepted.~~

~~b. *IT service providers* (e.g., webmasters, network engineers, server administrators, application developers, desktop support staff, or database administrators) shall implement all applicable Program~~

~~and *IT security* policy requirements within their areas of responsibility. *IT service providers* shall evaluate the effectiveness of *IT security* safeguards in their areas of responsibility and report any security weaknesses, concerns, or breaches to the campus *Information Security Officer*.~~

~~c. *Data Trustee* is a party or entity identified with and widely recognized to have primary authority and decision responsibility over a particular collection of university data. Data trustees are accountable for managing, protecting, and ensuring the integrity and usefulness of university data. Data trustees have the primary responsibility to ensure the university is following its policies and is in compliance with federal and state laws and regulations. Data trustees typically are associated with the business functions of an organization rather than technology functions.~~

~~d. *Data Custodian* is any party charged with managing a data collection for a data trustee. Custodians typically have control over a data asset's disposition, whether stored (at rest), in transit, or during creation. Custodians will often have modification or distribution privileges. Data custodians carry a significant responsibility to protect data and prevent unauthorized use. Data custodians are often data providers to data users. Data trustees or data stewards may also exercise custodial roles and responsibilities. Data custodians typically are associated with IT units within the university, either central IT organizations or IT offices within academic and administrative units.~~

~~e. *Data Steward* is a party or entity possessing delegated authority to act on a data trustee's behalf. Data Stewards will often have data custodial responsibilities, but are distinguished from custodians by delegated decision-making authority regarding the data. Data stewards may represent data trustees in policy discussions, architectural discussions, or in decision-making forums. Data Stewards actively participate in processes that establish business context and quality definition for data elements. Data Stewards are more likely to be associated with business functions than IT functions.~~

~~f. *Data User* is any person or party that utilizes university data to perform his or her job responsibilities. To the degree that a data user creates university data and/or controls the disposition of university data, he or she has responsibility for the custodial care of that data. Data users share responsibility in helping data stewards and custodians manage and protect data by understanding and following the IT and information security policies of the university related to data use.~~

~~D. Any exceptions to this policy must be approved by the University CISO.~~

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

The IT Security Program serves as the core for the University's IT security activities and provides general guidance to the users and administrators of IT resources to help ensure the confidentiality of personal information, the availability of university information and IT resources, and the best practices and control activities that should be in place to help mitigate the risks of using technology associated with the University. The related documents that support this APS include:

Related documents	Effective Date	Compliance Date
APS 6001 – Providing and Using Information Technology		
IT Security Controls Standard (updated to 800-171)	**10/01/2023**	**10/1/2024**
IT Security Responsibilities (new)		
Campus Acceptable Use Policies (links)		
APS 6002 - Electronic Communications		
APS 6010 - Data Governance		
Data Classification		

IV. HISTORY

Effective October 1, 2023, this APS was rewritten to establish a new format for the creation of security-related standards within the University.

~~III. **DEFINITIONS** APS Glossary of Terms~~

~~A. Business Continuity~~

B. Disaster Preparedness
C. Employees
D. Encryption
E. IT Resource
F. IT Resource User
G. IT Security
H. Information Security Officer
I. IT Security Program
J. IT Service Provider
K. Organizational Unit
L. President
M. Highly Confidential Information
N. Confidential Information
O. Risk Management
P. Student
Q. University Information

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

A. Administrative Policy Statements (APS) and Other Policies

The IT Security Program serves as the core for the University's *IT security* activities and provides general guidance to the computing community on ensuring the privacy of personal information and the availability of *University information* and *IT resources* and encompasses all related IT Security requirements, including the following policy sections:

- **IT Resource User Responsibilities**
- **IT Security in Personnel Job Descriptions, Responsibilities and Training**
- **IT Security in University Operations, Business Continuity Planning, and Contracting**
- **IT Service Provider Security**

B. Other Resources (i.e. training, secondary contact information)

Educational information and resources are available on the information security website: http://www.cu.edu/ois

V. HISTORY

Effective March 1, 2011 the following policies were combined into the IT Security Program policy. Individual APS history for each is listed below:

IT Resource User Responsibilities
- Initial Policy Effective: January 1, 2007
- Rescinded March 1, 2011 and combined with IT Security Program.

IT Security in Personnel Job Descriptions, Responsibilities and Training
- Initial Policy Effective: January 1, 2007
- Rescinded March 1, 2011 and combined with IT Security Program.

IT Security in University Operations, Continuity and Contracting
- Initial Policy Effective: January 1, 2007
- Rescinded March 1, 2011 and combined with IT Security Program.

IT Service Provider Security
- Initial Policy Effective: September 1, 2007
- Rescinded March 1, 2011 and combined with IT Security Program.

IT Security Program
- Initial Policy Effective: January 1, 2007
- Revised January 7, 2010.

- ~~Revised as the parent policy and combined with above IT security related policies effective March 1, 2011.~~
- ~~Section 1 – IT Resource User Responsibilities was revised effective January 1, 2014.~~

~~On May 1, 2014 the title of "IT Security Principals" was replaced with the title of "Information Security Officers".~~

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

~~The title of "IT Security Principals" was replaced with the title of "Information Security Officers" effective May 1, 2014.~~

~~The term "data owner" was replaced with the term "data trustee" effective July 1, 2018.~~

Return to Main Policy Page

The following sections of the prior version of APS 6005 remain in effect until they have completed transition to other APS documents and associated standards. Once that work is complete (expected in early 2024), these sections will be removed from this document.

IT SECURITY PROGRAM

Section 1: IT Resource User Responsibilities[1,2]

Brief Description: Establishes *IT security* requirements for all *IT resource users* in protecting *University information* and *IT resources*.

Applies to: *IT Resource Users*

SECTION 1 – IT RESOURCE USER RESPONSIBILITIES

I. INTRODUCTION

This section of the IT Security Program Policy establishes the Information Technology (IT) security safeguards that must be taken by every person using a University *IT resource* or otherwise accessing *University information*. Additional safeguards may be appropriate, depending on the situation and its inherent risk to *University information* and *IT resources.*

This policy does not impose restrictions that are contrary to the University's established culture of sharing, openness, and trust. However, the University is committed to implementing the safeguards necessary to ensure the privacy of personal information, the availability of *University information* and *IT resources*, and the integrity of University operations.

CU has three levels of data classification. These are: *Highly Confidential*, *Confidential*, and *Public*. For more information, please review the University of Colorado Process for Data Classification and System Security Categorization.

II. POLICY STATEMENT

A. It is the responsibility of every *IT resource user* to know the University's *IT security* requirements and to conduct her/his activities accordingly. *IT resource users* shall comply with the following requirements:

1. **Protect the Privacy of Others.** Users shall respect the privacy of others when handling *Highly Confidential information* and shall take appropriate precautions to protect that information from unauthorized disclosure or use.

2. **Protect *Highly Confidential* or *Confidential Information* on Workstations and Mobile Devices.** Ordinarily, *Highly Confidential information* shall not be stored on workstations and mobile computing devices (laptops, flash drives, backup disks, etc.) unless specifically justified for business purposes and adequately secured. If *Highly Confidential information* is stored on a workstation or mobile computing device or transmitted to an external network or organization, *IT resource users* shall *encrypt* or adequately protect that information from disclosure. If *Confidential information* is stored on a workstation or mobile computing device or transmitted to an external network or organization, *IT resource users* shall adequately protect that information from disclosure. In addition to *encryption*, adequate protections may include the use of passwords, automatic logoffs, and secure Internet transmissions. IT Resource users are required to secure university information on personally owned and/or institutionally provided mobile devices in accordance with the mobile device security

[1] Section 1 – IT Resource User Responsibilities was revised effective January 1, 2014.

[2] The terms private information and restricted information were changed to highly confidential information and confidential information, respectively – as of April 2014.

standards. The protection of *Highly Confidential* or *Confidential information* shall be in accordance with campus *IT security* requirements and other guidance as available from the appropriate IT service center or help desk.

3. **Protect Highly Confidential Data from Unauthorized Physical Access.** *IT resource users* shall keep all *Highly Confidential* or *Confidential information* out of plain sight unless in use and shall not leave such information displayed when it is not needed.

4. **Protect Workstations and Other Computing Devices.** *IT resource users* are responsible for helping to maintain the security of workstations and other computing devices by striving to protect them from unauthorized access and malicious software infections (e.g., viruses, worms, and spyware). Users shall consult the appropriate IT service center or help desk for guidance on protecting their computing devices.

5. **Protect Passwords, Identification Cards, and Other Access Devices.** Passwords, identification cards, and other access devices are used to authenticate the identity of individuals and gain access to University resources. Each person is responsible for protecting the access devices assigned to her or him and shall not share passwords or devices with others. If a password or access device is compromised, lost, or stolen, the individual shall report this to the appropriate IT service center or help desk as soon as possible so that the access device is not used by an unauthorized person.

6. **Report Security Violations, Malfunctions, and Weaknesses.** *IT resource users* shall report security related events; known or suspected violations of *IT security* policy; and inappropriate, unethical, and illegal activities involving University *IT resources*. Users shall follow the reporting process applicable to their campus. If unsure of the local incident reporting process, users shall call the appropriate IT service center or help desk.

7. **Utilize *University Information* and *IT Resources* for Authorized Purposes Only**. *IT resource users* shall access or otherwise utilize *University information* and *IT resources* only for those activities they are specifically authorized and in a manner consistent with University policies, federal and state laws, and other applicable requirements.

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

A. Administrative Policy Statements (APS) and Other Policies

The IT Security Program serves as the core for the University's *IT security* activities and provides general guidance to the computing community on ensuring the privacy of personal information and the availability of *University information* and *IT resources* and encompasses all related IT Security requirements, including the following policy sections:

IT Resource User Responsibilities
IT Security in Personnel Job Descriptions, Responsibilities and Training
IT Security in University Operations, Business Continuity Planning, and Contracting
IT Service Provider Security

The Laws of the Regents, section 14.A.4 states that *employees* shall be responsible for the safekeeping and proper maintenance of university property in their charge. The administrative policy "Fiscal Code of Ethics" prohibits use of University property for personal gain.

The "Use of Electronic Mail" Administrative Policy Statement sets forth the appropriate use of University email and expectations for privacy in email communications.

System-wide Mobile Device Security Standards
Standards for Data classification and System security categorization[LM1]

B. Other Resources (i.e. training, secondary contact information)

Educational information and resources are available on the information security website: http://www.cu.edu/ois

Return to Main Policy Page

1037

PROPOSED POLICY CHANGES IN REDLINE FORMAT

IT SECURITY PROGRAM

Section 2: IT Security in Personnel Job Descriptions, Responsibilities and Training

Brief Description: Establishes requirements for incorporating employee responsibilities for *IT security* into performance management processes, as well as ensuring *employees* are aware of their *IT security* responsibilities and are adequately trained to fulfill those responsibilities.

Applies to: Supervisors

SECTION 2 – IT SECURITY IN PERSONNEL JOB DESCRIPTIONS, RESPONSIBILITIES AND TRAINING

I. INTRODUCTION

Information technology (IT) security responsibilities are, to various degrees, part of all duties within the University. For *employees* and job candidates it is important that the applicable *IT security* responsibilities are known, documented, and accepted as part of the terms and conditions of employment.

II. POLICY STATEMENT

A. *IT Security* Guidance and Support

1. Campus *Information Security Officers* shall, in collaboration with the Chief Information Security Officer (CISO), provide information and guidance to supervisors on implementing the requirements of this policy.
2. Campus *Information Security Officers* shall establish and oversee *IT security* awareness and education programs for their respective campuses.

B. Supervisor Responsibilities for *IT Security*

1. Supervisors shall ensure that all *employees* within their areas of authority are aware of their *IT security* responsibilities and that these responsibilities are incorporated into *employee* performance management processes and addressed in recruitment and hiring practices.
2. Supervisors shall ensure that *employees* provide a signed, written, or other documented acknowledgment of their *IT security* responsibilities as a condition of gaining access to *University information* and *IT resources*. Where feasible, acknowledgements should be provided prior to gaining access or as soon afterward as reasonably possible. Personnel supervising authorities shall track and/or maintain the records of *employee* acknowledgements.
3. Supervisors, in consultation with the campus *Information Security Officer*, are encouraged to make recommendations on the designation of positions with significant *IT security* responsibilities as "security-sensitive positions."

C. *Employee* Training

1. Supervisors shall ensure that *employees* are adequately trained to fulfill their *IT security* responsibilities. *Employees* with elevated computing privileges (e.g., server support technicians, user account managers, or web page administrators) may require additional, specialized training for carrying out their *IT security* responsibilities effectively.
2. All University *employees* including associates and other individuals, who require the use of University *IT resources* to perform their duties, shall receive initial training and periodic refresher training relevant to their *IT security* responsibilities.
3. Supervisors shall coordinate their local *IT security* training initiatives with the campus *Information Security Officer*.

D. Changes in *Employee* Duties or Employment Status

1. Supervisors shall provide timely notification to the appropriate service center or help desk when an *employee*'s duties or employment status changes so that access to *University information* and *IT resources* is adjusted accordingly.

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

A. Administrative Policy Statements (APS) and Other Policies

The IT Security Program serves as the core for the University's *IT security* activities and provides general guidance to the computing community on ensuring the privacy of personal information and the availability of *University information* and *IT resources* and encompasses all related IT Security requirements, including the following policy sections:

IT Resource User Responsibilities
IT Security in Personnel Job Descriptions, Responsibilities and Training
IT Security in University Operations, Business Continuity Planning, and Contracting
IT Service Provider Security

The "Use of Electronic Mail" Administrative Policy Statement sets forth the appropriate use of University email and expectations for privacy in email communications.

B. Procedures

IT Security Training Standards and Core Topics

C. Other Resources (i.e. training, secondary contact information)

Educational information and resources are available on the information security website: http://www.cu.edu/ois

Return to Main Policy Page

IT SECURITY PROGRAM

Section 3: IT Security in University Operations, Business Continuity Planning, and Contracting

Brief Description: Requires *IT security* safeguards to be integrated into University operations, asset management, contracting, *business continuity* planning, *disaster preparedness*, and enterprise *risk management* processes.

Applies to: *Organizational Unit* Directors/Chairs

SECTION 3 – IT SECURITY IN UNIVERSITY OPERATIONS, BUSINESS CONTINUITY PLANNING, AND CONTRACTING

I. INTRODUCTION

University operations are organized into *Organizational Units* that develop and execute strategic and tactical plans to carry out the University's mission and achieve its objectives. In doing so, these units collect, store, and process information that is essential to University operations and must be protected from unauthorized use and disclosure. To ensure that *University information* is protected in a manner consistent with other strategic assets, *Organizational Units* must implement Information Technology (IT) security safeguards as a part of normal University operations.

II. POLICY STATEMENT

A. *IT Security* Guidance and Support

1. Campus *Information Security Officers* shall, in collaboration with the Chief Information Security Officer (CISO), provide information and guidance to *Organizational Units* on implementing the requirements of this policy.

B. Information Classification

1. Campus *Information Security Officers* shall provide security standards based on the criticality and sensitivity of *University information* for their respective campuses.
2. *Organizational Unit* directors / chairs or their designees shall, following guidance from the campus *Information Security Officer*, ensure that appropriate *IT security* safeguards are in place for the *University information* and *IT resources* under their care. The appropriateness of the safeguards shall be determined by the criticality and sensitivity of information involved, campus policies and guidance, and applicable external requirements (e.g., state and federal laws, and industry standards).

C. Continuity of Operations

1. *Organizational Unit* directors / chairs or their designees, with guidance from the campus *Information Security Officer*, shall ensure that *business continuity* and *disaster preparedness* plans include all appropriate *IT security* requirements and are reviewed, tested, and updated as needed to ensure the viability of such plans.

D. *IT Security* Requirements in RFPs, Contracts, and Other Service Arrangements

1. *Organizational Unit* directors / chairs or their designees shall, with guidance from the Procurement Service Center and the *Information Security Officer*, ensure that Request for Proposals (RFP), contracts, or other service arrangements include adequate safeguards so that contractors and other third parties protect *University information* at a level that is equal to or greater than that required of University *employees*.
2. *Organizational Unit* directors / chairs or their designees, with guidance from the campus Information Security Officers, shall ensure that access to *University information* and *IT resources* by contractors and third parties follows established policies and procedures.

1179
1180

PROPOSED POLICY CHANGES IN REDLINE FORMAT

E. Risk Evaluation and Handling

1. *Organizational Unit* directors / chairs or their designees shall, with guidance from the campus *Information Security Officer*, evaluate risks related to the protection of *University information* and *IT resources* in their care. *Organizational Unit* directors / chairs or their designees shall forward issues of risk to campus authorities with appropriate jurisdiction over those affected by the risks.

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

A. Administrative Policy Statements (APS) and Other Policies

The IT Security Program serves as the core for the University's *IT security* activities and provides general guidance to the computing community on ensuring the privacy of personal information and the availability of *University information* and *IT resources* and encompasses all related IT Security requirements, including the following policy sections:

IT Resource User Responsibilities
IT Security in Personnel Job Descriptions, Responsibilities and Training
IT Security in University Operations, Business Continuity Planning, and Contracting
IT Service Provider Security

The Laws of the Regents, section 14.A.4 states that *employees* shall be responsible for the safekeeping and proper maintenance of university property in their charge.

B. Other Resources (i.e. training, secondary contact information)

Educational information and resources are available on the Office of Information Security[LM2] website.

Return to Main Policy Page

IT SECURITY PROGRAM

Section 4: IT Service Provider Security

Brief Description: Requires that *IT service providers* (e.g., server and workstation support, programmers, webmasters, user account administrators) incorporate *IT security* safeguards into the IT services and products provided to the University community.

Applies to: *IT Service Providers*

SECTION 4 – IT SERVICE PROVIDER SECURITY

I. INTRODUCTION

This section of the IT Security Program Policy sets forth the Information Technology (IT) security safeguards that must be taken by every *IT service provider*. These safeguards are necessary to protect *University information* from inappropriate access, disclosure and misuse; provide assurances that information resources are available as needed for University business; and comply with applicable policies, laws, regulations, rules, grants, and contracts. Campus *Information Security Officers* may require additional safeguards so as to address campus specific risks or compliance requirements.

II. POLICY STATEMENT

A. *IT Security* Oversight and Guidance

Campus *Information Security Officers* in collaboration with the Chief Information Security Officer (CISO) shall provide guidance and information as needed to *IT service providers* on implementing the requirements of this policy. *IT service providers* shall be aware that purchases of IT goods and services may be subject to a security review by the campus *Information Security Officer* or a designated campus authority.

Organizational Unit directors / chairs shall be aware of their responsibilities, as described by IT Security in University Operations, Continuity, and Contracting, to ensure that adequate safeguards are implemented for the *IT resources* under their control.

B. Life Cycle Management

Campus *IT service providers* shall ensure that *IT security* controls are appropriately implemented and managed throughout the life of the *IT resources* under their responsibility. This is to ensure that security is addressed in the design and purchase of new systems, implementation of new or modified systems, maintenance of existing systems, and removal from service of end-of-life systems.

C. *IT Resource* Security Management

Providing an IT service is a complex undertaking that requires continuous monitoring, maintenance, and system management to ensure that *University information* is adequately protected as it is processed, stored, and transmitted. Therefore, *IT service providers* shall implement the following controls where appropriate for the *IT resources* under their responsibility:

1. System and application security management. *IT resources* shall be maintained according to industry and vendor best practices to ensure that system and application updates, vulnerability fixes, security patches, and other modifications are applied in a timely fashion. Where applicable these practices shall include vulnerability management, system/application hardening, and security testing.

2. Malicious activity protection. *IT resources* that transmit or receive information on a University-managed network shall be adequately protected from malicious activities, such as viruses, worms, and denial of service attacks.

3. Data backup and recovery. *University information* shall be backed up and retained as appropriate for business needs, **retention** schedules, and legal requirements as provided by law or related university policy. Data backups shall be tested where appropriate to ensure the effective recovery of information.

4. Media handling and storage. Electronic storage media (e.g., CD-ROMs, memory sticks, disk drives, tapes, cartridges, etc.) shall be appropriately protected from loss and unauthorized access. All media containing Highly Confidential and *Confidential information* shall be stored in a secure location and adequately protected with a safeguard that restricts access to authorized personnel only. In addition, Highly Confidential information stored on portable electronic media shall be encrypted or otherwise adequately protected based on security standards and guidance from the campus Information Security Officers.

5. Disposal of electronic equipment and media. Computing and network equipment and storage media shall be purged of all *University information* so that information is not recoverable, or destroyed before disposal or release from University control to a third party. In the rare event the information is not purged prior to release or the device destroyed prior to disposal, the *IT service provider* shall acquire confirmation from the contracted third party that the information is properly purged. For equipment and media that is to be redeployed within the University, the *IT service provider* shall purge all information not authorized for access by the receiving person(s) prior to redeployment.

D. **Access Management**

Although *students*, faculty, and staff require access to *University information* resources for academic and business purposes, this access must be limited to what is needed for his/her work. Use of resources beyond that which is authorized results in unnecessary risks to *University information* with no corresponding academic or business value.

1. User access management. *IT service providers* shall manage user access to the *IT resources* under their responsibility, so that such access is appropriately authorized, documented, and limited to that which is needed to perform authorized tasks. Because a user's responsibilities and relationships with the University change over time, *IT service providers* shall ensure that user access privileges are regularly reviewed and adjusted to comply with currently authorized activities.

2. *IT resource* access controls. *IT service providers* shall ensure that *IT resources* under their responsibility (developed, purchased or otherwise used to handle *University information*) have adequate features and controls to support the proper management of user access as described in section II.D.1.

3. Network security controls. *IT service providers* shall ensure that electronic access to and use of the campus data networks under their responsibility is adequately controlled to protect data network equipment and other networked *IT resources*.

E. **Physical and Environmental Security**

University data centers and *IT resources* shall be sufficiently protected from physical and environmental threats to prevent the loss, damage, or compromise of assets, and interruption to business activities.

1. Data centers. Data center owners, managers, or their designees shall, following guidance from the campus *Information Security Officer*, ensure that data center facilities under their responsibility have adequate physical security safeguards. These safeguards may include: physical barriers (e.g., walls, gates, locked doors), access controls (e.g., identification cards, visitor escorts and logs, facility/equipment repair records), environmental controls and protections (e.g., uninterruptible power supplies, generators, temperature and humidity systems, fire suppression units).

2. *IT resources*. *IT service providers* shall ensure that all *IT resources* under their responsibility have adequate physical security safeguards. While the value of these *IT resources* may not rise to that found in a data center, the physical protections normally afforded to *IT resources* within a data center should be employed where reasonable and appropriate.

F. **Incident Detection and Reporting**

IT service providers shall monitor for and report security breaches or other significant security events involving the *IT resources* under their control, following guidance from the campus *Information Security Officer*.

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

A. Administrative Policy Statements (APS) and Other Policies

The IT Security Program serves as the core for the University's *IT security* activities and provides general guidance to the computing community on ensuring the privacy of personal information and the availability of *University information* and *IT resources* and encompasses all related IT Security requirements, including the following policy sections:

IT Resource User Responsibilities
IT Security in Personnel Job Descriptions, Responsibilities and Training
IT Security in University Operations, Business Continuity Planning, and Contracting
IT Service Provider Security

The Laws of the Regents, section 14.A.4 states that employees shall be responsible for the safekeeping and proper maintenance of university property in their charge.

B. Other Resources (i.e. training, secondary contact information)

Educational information and resources are available on the *Office of Information Security* website.

Return to Main Policy Page