**UNIVERSITY OF DENVER**
**POLICY MANUAL**
**INFORMATION SECURITY**

| | | |
|---|---|---|
| **Responsible Department:** Information Technology<br>**Recommended By:** Provost, SVC Business and Financial Affairs and VC for Information Technology (CIO)<br>**Approved By:** Chancellor | **Policy Number**<br>IT 13.10.080 | **Effective Date**<br>4/12/2023 |

## I. INTRODUCTION

The University's information systems collect, manage, and store sensitive information regularly to support business operations. The University is committed to preserving the confidentiality, integrity, and availability of its information resources while preserving and nurturing its academic culture's open, information-sharing requirements.

## II. POLICY OVERVIEW

**A.** The purpose of this Policy is to:

1. Authorize the creation of the University Information Security Program (the "Program") to support this Policy. The Program will establish, implement, and maintain information security-related policies, procedures, and standards. The Program will use the guiding principles outlined in **Appendix A** in the evaluation and implementation of security controls and processes.
2. Assign roles and responsibilities to support this Policy and Program.
3. Confirm the University's compliance with applicable laws and regulations and support the implementation of information security best practices.
4. Authorize the creation of the University Information Security Steering Committee (ISSC) to support this Policy and the Program. The ISSC will provide guidance and support to the University's Vice Chancellor for Information Technology (CIO) and the Assistant Vice Chancellor and Chief Information Security Officer (CISO) to maintain the Program.

## III. POLICY PROCESS

**A.** The Information Security  Program established by this Policy addresses the following areas:

### 1. Security Organization and Governance

The University will:

**a.** Develop and implement a reporting structure that will define responsibilities for establishing and implementing technical and non-technical information security standards, procedures, and guidelines on an enterprise-wide basis.

**b.** Identify and define security roles and responsibilities for protecting the University's information resources. *See Section III. B: Roles and Responsibility.*

**c.** Maintain appropriate subordinate policies, procedures, standards, and other materials sufficient to create, implement, and maintain the Program. These supporting elements will be periodically updated to reflect changes in technology and the University.

**d.** Classify information resources based on information sensitivity criteria – Public, Internal, Confidential, and Restricted based on University Policy IT 13.10.051- *Data Classification.*

**e.** Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and adequately skilled to reduce cybersecurity risks to the University. *See* University Policy IT 13.10.015 - *Security Awareness Training.*

**f.** Monitor and periodically report on elements of the Program and the overall security posture of the University. This information will be provided to the Board of Trustees, senior leadership, or other groups as requested.

### 2. Asset Management

The University will establish and maintain processes to:

**a.** To accurately inventory and manage the lifecycle of its physical devices and systems, including end-user devices connected to the University infrastructure physically, virtually, remotely, and within cloud environments.

**b.** To accurately inventory and manage the lifecycle of software platforms and applications.

**c.** Identify unauthorized and unmanaged software, devices, and systems to remove or remediate.
**d.** Manage and control the installation of user-installed software.

3. **Risk Management**

The University will establish and maintain processes to:

**a.** Perform periodic risk assessments to identify, evaluate, prioritize, and treat risks that may threaten the confidentiality, integrity, or availability of Information Resources to an acceptable level (within the organization's risk tolerance levels).
**b.** Evaluate the existing policies, procedures, technology solutions, and other arrangements to determine the effectiveness of the controls and will make recommendations for changes and improvements.
**c.** Document the University's risk tolerance and communicate the risk tolerance to organizational stakeholders.
**d.** Evaluate and manage supply chain risks - to identify, assess and manage security risks associated with establishing relationships with business partners, vendors, and contractors.
**e.** Monitor and confirm compliance with all applicable federal, state, and local laws and regulations, including grants and University contractual obligations relating to information security.

4. **Account Management, Authentication, and Access Control**

The University will establish and maintain processes and tools to:

**a.** Limit access to Information Resources to authorized persons based on business and security requirements and the principles of "least privilege" and "minimum necessary."
**b.** Assign and manage authorization to credentials for user account access, including administrator and service accounts, to Information Resources.
**c.** Create, assign, manage, and revoke access credentials and privileges for users, including administrators, and service accounts, for Information Resources.
**d.** Use multifactor authentication for local and network access.
**e.** Enforce password management policies, including minimum password length, password complexity, password reuse, temporary password use and secure password storage.
**f.** Use separate accounts for executing privileged functions.
**g.** Manage and monitor remote access to Information Resources.

**h.** Manage and control sessions and inactivity timeouts for applications and services.
**i.** Manage and control mobile device access to University Data, including configuration and connection requirements.
**j.** Manage and control access to external systems such as SaaS and other cloud-based services.
**k.** Periodically review access and monitor access activities. *See User Account & Access Management Policy*.

## 5. Data Security

The University will establish and maintain processes and technical controls to:

**a.** Control, handle, retain, and dispose of University Data. The processes and technical controls will address University Data, in process, in transit, and at rest.
**b.** Prevent University Data from leaking inappropriately.

## 6. Personnel Security

The University will establish and maintain a process to:

**a.** Screen individuals before authorizing access to Information Resources.
**b.** Periodically re-assess individuals with access to Information Resources.

## 7. Information Protection Processes and Procedures

The University will establish and maintain processes and procedures to:

**a.** Maintain secure baseline configuration images for Information Resources, including a process to review and update documentation annually or when significant changes occur.
**b.** Confirm changes to information processing facilities, equipment, systems, and applications are controlled through formal management responsibilities and procedures appropriate for the risks involved.
**c.** Confirm data recovery practices are sufficient to restore in-scope Information Resources to a pre-incident and trusted state.
**d.** Confirm Information Resources are housed securely and protected against identified risks, including an audit log of physical access and managing visitor access for on-prem and alternate, on-prem, and remote processing facilities.

**e.** Confirm that information systems are sufficiently resilient. This includes confirming the continuity of critical University business processes despite minor incidents and confirming that proven disaster recovery arrangements are in place to minimize the impact of serious incidents.

**f.** Develop, document, and periodically update system security plans.

**g.** Require that all persons accessing University information systems comply with University information security principles, policies, standards, procedures, and guidelines, requirements identified in the terms and conditions of their employment or service contracts, and applicable laws and regulations.

**h.** Continuously assess and track vulnerabilities on all Information Resources within the enterprise's infrastructure to remediate and minimize the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

**i.** Track, manage, and deploy security patches, updates, and security configuration changes for all Information Resources.

**j.** Evaluate service providers, who hold or are responsible for Information Resources, to confirm that these providers are protecting Information Resources appropriately.

**k.** Test the effectiveness and resiliency of Information Resources by identifying and exploiting weaknesses in controls (people, processes, and technology) and simulating the objectives and actions of an attacker.

**l.** Evaluate, approve, use, track, manage, and protect cryptographic controls used to protect the confidentiality and integrity of University Data.

## 8. Security Protection Technology

The University will establish and maintain processes to:

**a.** Collect, manage, and protect audit logs. At a minimum, address the collection, review, access retention, synchronizing time, and protection of audit logs for Information Resources. The audit logs shall be protected against tampering and unauthorized access.

**b.** Secure and manage access to University Data on removable media, including controlling its use on Information Resources, encryption, labeling, sanitization, and disposal processes.

**c.** Secure against security threats across the University's network infrastructure and user base through secure configuration, network architecture, network segmentation, and network monitoring and defense.

**d.** Implement and manage secure wireless access to the University network and systems.

**e.** Prevent and control the installation, spread, and execution of malicious applications, code, or scripts on Information Resources.

**f.** Provide system redundancy and high availability of Information Resources.

### 9. Threat and Anomaly Detection and continuous Monitoring

The University will establish and maintain processes, services, and technology for comprehensive monitoring and defense against security threats across the enterprise network infrastructure, endpoints, and user base.

### 10. Incident Response Management

The University will establish and maintain processes to:

**a.** Respond to security incidents, including capabilities to prepare, detect, and respond to potential and real-time threats to Information Resources.

**b.** Track, document, and report security incidents to internal and external stakeholders.

**c.** Test the organizational incident response capabilities.

### 11. Application Software Security

The University will establish and maintain secure development practices for all in-house applications developed or externally and commercial shelf packages purchased to include security controls to prevent unauthorized access or modification of the system or information coded or stored.

## B. Roles and Responsibility

| **Role** | **Scope** | **Responsibilities** |
|---|---|---|
| Board of Trustees | Strategic | • Is presented with the annual IT state and risk update.<br>• Consults with Executive Leadership to understand the University IT mission and risks and provide guidance to bring them into alignment. |
| Executive Leadership | Strategic | • In collaboration with the Board of Trustees, establishing the organization’s risk tolerance. |

| | | |
|---|---|---|
| | | • Approve Capital Expenditures for Information Security.<br>• Communication path to Deans, Faculty and Staff.<br>• Aligns Information Security Policy and posture based on the University's mission and risks. |
| Vice Chancellor/CIO | Strategic | • Sponsors the Information Security Office (ISO) that is responsible implementing the information security risk process for University activities, processes, and projects.<br>• Coordinates with the CISO to confirm that IT puts into practice the Information Security Program and Plan. |
| Assistant Vice Chancellor/CISO | Strategic | • Developing and managing the University's information security program.<br>• Communicates information security risks to Executive Leadership.<br>• Reports information security risks annually to University leadership and gains approval to bring risks to acceptable levels.<br>• Coordinates the development and maintenance of information security policies and standards.<br>• Works with the ISO to execute the Information Security Program.<br>• Serve as liaison to the Board of Trustees, Internal Audit, and General Council. |
| Data Trustees | Strategic | • Has oversight responsibility for information related to the University's mission that is managed, administered, or run by the depts. and schools.<br>• Authorizes/Defines policies, standards, and guidelines regarding business definitions of information, access, and usage of that information.<br>• Appoints a data custodian(s) for their subject area.<br>• In some cases, responsible for the context, content, and associated business rules and use.<br>• Examples: deans, department heads, managers, supervisors, or designated staff. |

| | | |
|---|---|---|
| Data Custodians | Tactical | • Implement and enforces University policies, standards, and guidelines for Information Assets within their designated data sets.<br>• Accountable for the security, privacy, data definitions, data quality, and compliance with data management policies and standards for a specific data domain.<br>• Has the primary responsibility for the accuracy, privacy, and security of a designated data set.<br>• Confirm access to the data is authorized and controlled; technical processes sustain data integrity, and technical controls safeguard data.<br>• Works with the System Custodian to confirm that information that has been classified as confidential or protected adheres to University Information Security controls. |
| Information Security Office (ISO) | Tactical | • Responsible for conducting risk assessments, documenting the identified threats, and maintaining the risk register.<br>• Assist University departments and schools in assessing their data for classification as defined in the Information Classification Policy and advises them of required controls.<br>• Develop policy, standards, processes, and solutions to mitigate identified risks to an acceptable level.<br>• Assists the CISO with the development of the Information Security Program.<br>• Works with IT, faculty, and staff to embed the Program into operations.<br>• Monitors the infrastructure and data repositories for malicious activity.<br>• Works with the incident manager in the investigation of security incidents.<br>• Responsible for establishing the Vulnerability Management program.<br>• Provide consulting services for information security throughout the University. |
| Internal Audit | Tactical | • Conduct audits to evaluate and confirm compliance with information security policies and risk mitigation efforts. |

| | | |
|---|---|---|
| | | • Interfaces with external auditors to provide an independent audit of IT and cybersecurity practices. |
| System Owners | Operational | • Manage the confidentiality, integrity, and availability of the information systems for which they are responsible. This shall include developing and implementing a process for managing access to information systems for which they are responsible, and other processes or controls in compliance with University policies on information security and privacy.<br>• Advise executive leadership on the financial resources necessary to develop and implement information systems and controls, including those specifically required by grants or contracts.<br>• Maintain critical information system documentation and apply security controls per policies and standards<br>• Formally appoint and delegate responsibility to system custodians. |
| System Custodians | Operational | • Making and being accountable for operational decisions about the use and management of an information system.<br>• Responsibilities as delegated by system owners and data custodians to implement controls.<br>• System Custodians may be the same as the owners. |
| University Faculty, Staff and Students | Operational | • Acting at all times in a manner that does not place at risk the health and safety of themselves, another person in the workplace, and the information and resources they have use of.<br>• Helping to identify areas where risk management practices should be adopted.<br>• Taking all practical steps to minimize the University's exposure to contractual and regulatory liability. |

## IV. DEFINITIONS

A. **"Information Resources"** means means all devices, services, networks and other resources and technology related to the transaction of University business, regardless of form or location, that are owned, provided, or administered by or through the University, or used to electronically store, process, or transmit information.

| **Revision**<br>**Effective Date** | **Purpose** |
|---|---|
| *6/28/2021* | *Minor revisions* |
| *4/12/23* | *Major revisions to Policy IT 1.10.080 to use the NIST 800-171 Security Framework as a basis for this Policy.* |

# Appendix A

## Information Security Program Principles

The Program is designed to address enterprise-wide security compliance while retaining the flexibility required to address relevant changes in technology. The following guiding principles are the cornerstone upon which the Program is built:

1. **Cybersecurity is everyone's responsibility** - promote collective and individual responsibility to create and maintain mature cyber-engaged security culture.
2. **Cybersecurity is an enabler** – Information security is a business enabler that allows us to enter more confidently into and maintain business relationships. Minimizing information security incidents supports our financial bottom line. It also enhances our image as a trustworthy, open, honest, and ethical organization.
3. **Secure by design** – Provide leadership, governance, and oversight with the goal of meeting cybersecurity requirements during the design, development, selection, and management of information systems.
4. **Defense in depth** – adopt a layered mix of physical, technical, and administrative controls to detect, prevent, mitigate, and recover from cyber threats
5. **Balanced security management** - We invest wisely in proven information security controls that were justified based on lifecycle cost-benefit assessment and risk analysis.
6. **Manage complexity** – Confirm that cybersecurity controls and solutions integrate and work with underlying information systems and processes to reduce risk and minimize complexity.
7. **Support compliance** - establishing an information security landscape that supports the University Privacy Policy and applicable privacy laws.
8. **Continuous adaptation** – Review and improve information security management in response to security incidents and keep pace with changes to the University, information technology, security technology, and threat landscape.
9. **Engage and collaborate** – Build and engage in mutually beneficial partnerships throughout the cyber and higher education industries to enhance protection against common threats.
10. **Value of information** – Information is a critical business asset of the University. It must be protected to a degree appropriate to its vulnerability and its importance or value to the organization. This includes our information assets and those placed in our care.
11. **Promote the University's values and mission** – Establish best practices in information security that support the University's values and mission.
12. **Good Governance** – Information security is a core element of enterprise governance. It is closely related to IT management, physical site security, risk management, legal and regulatory compliance, and business continuity. It supports various obligations to our students, employees, business partners, and the community.