	UNIVERSITY OF DENVER POLICY MANUAL INFORMATION SECURITY	
Responsible Department: Information Technology **Recommended By:** Provost, SVC Business and Financial Affairs and VC for Information Technology (CIO) **Approved By:** Chancellor	**Policy Number** IT 13.10.080	**Effective Date** 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 0 G[The)3(purpos)-4(e of)-3(this)]TJETQq(ss)]TJETQq(ss)]TJE

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

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 455.5 543.1 Tm0 g0 G[(Inf)-2(orm

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.

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 **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** - 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 managee to 3(for)-2((4.p.uri)-2(ty)11(managemen)8(t)]TETQ0.000009 12 0 612 7

. /F20T /F2 12 .3 s q -711partn 1 0.00 -711 G [(minimize)4(com)-2(pl)3(exity.)] TJ ET Q q 0.00000912 0 612 7