UNIVERSITY OF DENVER	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** 5/15/2026

I. INTRODUCTION

This Policy establishes University-wide expectations for information security practices and supports compliance with legal, regulatory, contractual, and ethical obligations. This policy applies to all faculty, staff, students, contractors, and affiliates who access, store, process, or transmit University data across any platform or location.

II. POLICY OVERVIEW

The following policy statements establish the University's information security objectives and control expectations across all security domains. They are informed by risk management principles and adapted from the National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), and Center for Internet Security (CIS) frameworks.

A. Security Objectives

1. **Governance and Risk Management:** The University will maintain an information security governance framework that provides oversight and accountability, aligning information security decisions with University priorities.

2. **Risk Management:** The University will conduct regular risk assessments and apply risk-based methodologies to guide information security decisions, using identified threats, vulnerabilities, and business impacts to inform prioritization and resource allocation.

3. **Third-party and Cloud Security:** Vendors, contractors, and cloud security providers with access to University data or systems must

comply with the University's security requirements to protect University data.

4. **Security Awareness Training:** Information security is a shared responsibility, and every member of the University community plays a critical role in protecting institutional data and systems. All users of IT Resources (as defined below) must complete regular information security training on a schedule established by the University in University Policy IT 13.10.015 – Security Awareness and Training.

5. **Asset and Data Management:** The University will inventory, classify, and protect IT Resources and data according to their sensitivity, regulatory requirements, and institutional value. Data classification requirements are defined in University Policy IT 13.10.051 - *Data Classification* and supported by the Data Security Standards (DSS) (*See* Resources below).

6. **Data Retention and Destruction:** The University will manage the retention and secure destruction of information in a manner that protects data, complies with legal and regulatory requirements, supports operational and academic needs, and minimizes unnecessary storage of sensitive information. The University will retain data only for as long as required by the University Record Retention Schedule, and dispose of data securely when no longer needed.

7. **Access Control, Authentication, and Passwords:** The University restricts access to University systems and data to authorized individuals based on role, necessity, and least-privilege principles. Access to University systems and data will be protected through approved identity verification and authentication methods. The University requires strong passwords and the secure management of authentication credentials in accordance with University Security Standards (*See* Resources below). IT will configure University systems to enforce password protections and multi-factor authentication to safeguard access to IT Resources.

8. **Host and Endpoint Security:** The University will protect servers, workstations, laptops, virtual machines, and other computing hosts through approved security configurations, monitoring, and protective controls. IT will maintain hosts in a secure state, including the use of University-defined hardening standards, timely patching, malware protection, least-privilege access, and, where appropriate, continuous monitoring. The University may restrict access to University systems for any device that does not meet University security requirements.

9. **Mobile Device and BYOD Security:** The University permits the use of mobile devices—including personally owned devices—to access University systems and data when such use supports academic, research, or operational activities. Users of mobile devices must follow University security requirements to protect University data, maintain compliance with legal and regulatory obligations, and reduce risks associated with portable and personally managed technologies.

10. **Security Configuration and Hardening:** The University will establish and maintain secure configuration and hardening requirements for all information systems, devices, applications, and services that create, store, process, or transmit University data. Secure configuration reduces the risk of unauthorized access, data compromise, and service disruption by minimizing vulnerabilities and limiting the attack surface.

11. **Network and System Security:** The University will configure, maintain, and monitor Information systems and networks to prevent, detect, and respond to unauthorized access, malware, and other threats.

12. **Incident Response and Reporting:** The University will maintain an incident response program to detect, contain, investigate, and recover from security incidents, as well as to comply with any associated reporting obligations.

13. **Vulnerability Management:** The University will operate a continuous vulnerability management program to identify, assess, prioritize, and remediate security weaknesses across systems, applications, and devices. Remediation timelines will be based on risk level, regulatory requirements, and operational impact.

14. **Change Management and Patch Management:** The University will maintain formal, risk-based change and patch management processes to evaluate, approve, implement, and document modifications to technology systems. IT will use patch deployment according to defined schedules and emergency procedures to reduce exposure to threats and maintain system stability and availability.

15. **Application Security and Secure Software Development:** The University will apply secure development practices to all applications and software services that create, store, process, or transmit University data. The University will integrate application security controls throughout the software development lifecycle to minimize vulnerabilities, support regulatory compliance, and protect

the confidentiality, integrity, and availability of University IT resources and University data.

16. **Logging and Auditing Requirements:** The University will maintain logging and auditing capabilities sufficient to support threat detection, incident response, forensic investigation, accountability, and compliance obligations. The University will conduct logging and auditing activities in a manner that respects individual privacy, supports academic freedom, and aligns with applicable laws, regulations, and University policies.

17. **Business Continuity and Disaster Recovery:** The University will support critical information systems and data through documented and tested continuity and recovery plans to improve resilience and minimize disruption during adverse events.

18. **Continuous Monitoring and Threat Management:** The University will implement continuous monitoring and threat detection capabilities to identify, assess, and respond to malicious activity or anomalous behavior across its information systems and networks.

19. **Compliance and Monitoring:** The University will monitor University IT resources and practices for compliance with this policy and applicable laws and will conduct audits and assessments to verify the effectiveness of security controls.

20. **Privacy and Security Balance**: The University is committed to protecting individual privacy while maintaining the security of University data. Information security measures will be implemented in a manner that balances privacy obligations with operational needs, academic freedom, and legal obligations.

III. POLICY PROCESS

A. Roles and Responsibilities

The following roles have key responsibilities for implementing, maintaining, and supporting the University's Information Security Program.

1. The **Chief Information Security Officer (CISO)** will direct the Information Security Program, manage risk assessments, monitor compliance, and coordinate incident response.
2. **Unit-based Information Technology Personnel** will implement and operate security controls, maintain security configurations, and monitor for threats.

3. **Data Owners and Data Custodians** will classify data, determine access rights, and protect data assets.
4. **Users** must follow security policies, complete required training, protect credentials, and report suspected incidents promptly.

B. Policy Governance

1. **Policy Updates:** The CISO will initiate updates to this Policy when necessary or desirable to maintain alignment with best practices and compliance obligations, and to address emerging threats, new technologies, audit findings, regulatory changes, or institutional priorities.

2. **Relationship to Standards, Procedures, and Guidelines:** This Policy is supported by IT departmental policies (available on the University's IT website), which identify standards and procedures that define specific security requirements, controls, and implementation expectations, as well as guidelines with recommended practices.

C. Enforcement

1. Suspected violations of this Policy must be reported to the IT Security Office at info-security@du.edu. The IT Security Office will take the following actions:
   - For allegations that a Student has violated this Policy, refer the matter to the Office of Student Rights & Responsibilities (SRR) for consideration of action under the Honor Code.
   - For allegations that an Employee has violated this Policy, refer the matter to Human Resources & Inclusive Community for investigation and to determine appropriate corrective action.

If a User of University IT Resources is found to have violated this Policy, the University may:

1. Suspend or terminate their access to University IT Resources;
2. Impose Outcomes for Students through the SRR process as set forth in the Honor Code;
3. Impose corrective action on Employees.

In addition, Users of University IT Resources may face civil or criminal liability under federal, state, or local laws, regulations, or ordinances.

In the case of suspected criminal activity, the IT Security Office will notify the Department of Campus Safety and the Office of General Counsel.

IV. DEFINITIONS

A. "IT Resources" means all hardware, software, systems, services, and data that are provided by or connected to University networks. This includes computing and networking infrastructure—whether shared or individual—that transmits or processes information using text, voice, images, or video. IT Resources also includes all University-owned or operated computers, devices, networks, accounts, and associated digital assets.

V. REFERENCES

A. University Policy 13.10.051 – *Data Classification*

B. University Policy 13.10.010 – *Acceptable Use*

C. *University Policy RISK 1.10.025 – Records Management*

D. *University of Denver Record Retention Schedule*

E. Security Frameworks

- NIST Cybersecurity Framework (CSF)
- ISO/IEC 27000 Series: Information Security Management Standards
- CIS Critical Security Controls v8 (IG2)
- NIST SP 800-207: Zero Trust Architecture

F. IT Policies, Standards, and Guidelines

- Malware Protection and Management Policy
- Removable Media Protection Policy
- User Account and Access Management Policy
- Vulnerability Management Policy
- Security Incident Response Policy
- Third-Party Security Management Policy
- Log Management Policy
- Password Management Standard
- Media Sanitization and Disposal Standard
- Mobile Device Security Standard
- Endpoint and Host Security Standard
- Data Security Standard
- Application Security Standard

Revision Effective Date	Purpose
6/8/2018	*Original Policy added to the Policy Library*
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.*
5/15/2026	*Major revisions to align with updated security frameworks and best practices*