

Policy Title: Information Security Policy
Policy Owner: Information Technology Services
Effective Date: 10/01/2026
Last Updated: 09/18/2026
Scheduled Review 01/15/2028
Related Policies:
Related Forms:

I. POLICY STATEMENT

Seattle University is committed to managing information security risk and protecting the confidentiality, integrity, and availability of its Institutional Data, IT Resources, and technology-dependent operations. Information security is a shared responsibility.

The University will maintain a risk-based information security program and safeguards proportionate to the sensitivity of the information, the criticality of the system or service, and the potential impact on individuals and the University.

II. PURPOSE & BACKGROUND

This policy establishes University-wide authority, accountability, and requirements for protecting the information and technology that support teaching, learning, research, scholarship, administration, and community engagement.

It complements the Acceptable Technology Use Policy, Data Privacy Policy, Data Privacy and Handling Standard, Identity and Access Management Standard, and Cybersecurity Incident Response and Business Continuity Policy.

III. APPLICABILITY/RESPONSIBILITY

This policy applies to all Personnel, students, contractors, vendors, guests, affiliates, and other individuals who access, use, administer, or support Seattle University IT Resources or Institutional Data.

It applies regardless of location or whether University-owned or personally owned devices are used. This policy does not prohibit authorized use of personally owned devices.

Information security responsibilities include:

- **Information Technology Services (IT Services):** Owns and administers this policy and maintains the University information security program. The Chief Information Officer provides executive oversight, and the Information Security Officer oversees information security risk, requirements, monitoring, incident response, awareness, and recommendations concerning exceptions.
- **University Leaders, System Owners, Technical Custodians, and Data Stewards:** Ensure that systems, services, information, and activities within their areas of responsibility comply with applicable security requirements and that identified risks are appropriately addressed.
- **University Technology Committee and Academic Technology Committee:** Advise on material information security matters affecting University administration, teaching, learning, research, and technology.
- **Supervisors, Project Leads, and Principal Investigators:** Ensure that individuals, projects, and activities under their direction follow applicable information security requirements.

- Users:** Protect their accounts, devices, and information; comply with applicable security requirements; and promptly report suspected incidents, vulnerabilities, or unauthorized activity.
- Third Parties:** Protect University systems and information in accordance with their agreements and applicable University requirements.

IV. DEFINITIONS

Information Security: The protection of information and technology against unauthorized access, use, disclosure, disruption, alteration, or destruction to preserve confidentiality, integrity, and availability.

Institutional Data: Information that documents, describes, or supports University functions, decisions, or operations, including instruction, research, scholarship, administration, financial management, human resources, and governance.

IT Resources: Technology resources owned, managed, licensed, provided, or approved by the University, including networks and internet access; computers and mobile devices; software, applications, systems, accounts, and communication services; classroom, laboratory, and virtual computing environments; Institutional Data; and cloud, storage, collaboration, and artificial intelligence services.

Personnel: Faculty, staff, fellows, student employees when acting within the scope of their University employment, and other individuals performing work for the University. This term does not include contractors or vendors.

System Owner: A University official accountable for the purpose, operation, access, risk, and appropriate use of a system or service.

Technical Custodian: An individual or unit responsible for the technical administration, operation, maintenance, or support of a system or service.

Users: Individuals who use University IT Resources, whether or not they are authorized to do so.

V. POLICY REQUIREMENTS

A. Information Security Governance and Risk Management

IT Services will maintain a risk-based information security program that supports the University's mission and addresses applicable legal, regulatory, contractual, research, and University requirements.

Information security risks must be identified, assessed, prioritized, and addressed based on the sensitivity of the information, criticality of the system or service, reasonably foreseeable threats, and potential consequences to individuals and the University.

University units must cooperate with authorized information security assessments and address identified risks within a reasonable period based on their severity. Material risks that cannot be addressed promptly must be documented and reviewed by the Chief Information Officer (Information Security Officer, responsible University leader, and other appropriate offices).

Security requirements must be proportionate to risk and, when reasonably possible, implemented in ways that support academic freedom, accessibility, teaching, learning, research, innovation, and University operations.

B. Protection and Secure Technology Lifecycle

Information security must be addressed throughout the lifecycle of systems, services, projects, and technologies, including planning, acquisition, design, implementation, operation, material change, and retirement.

University systems and services must have an identified System Owner and, as appropriate, a Technical Custodian, and must be inventoried and managed at a level appropriate to their function, risk, and criticality.

IT Resources and Institutional Data must be protected through reasonable administrative, technical, and physical safeguards appropriate to their risk. Access must comply with the Identity and Access Management Standard. The collection, use, storage, transmission, sharing, retention, and disposal of Institutional Data must comply with the Data Privacy Policy and Data Privacy and Handling Standard.

New or materially changed technologies and third-party services must receive applicable privacy, security, procurement, and contractual reviews. Third-party access to University systems or information must be authorized, limited to what is necessary, and removed when no longer required.

Known vulnerabilities, unsupported technologies, insecure configurations, and material system changes must be evaluated and addressed based on risk. Systems and services that cannot be adequately secured may be restricted, isolated, replaced, or removed from service. Systems and services must be securely retired when no longer needed.

Users may not disable, bypass, or interfere with University security safeguards without authorization.

C. Security Monitoring and Protective Action

IT Services may monitor IT Resources and security-related activity when reasonably necessary to identify vulnerabilities, investigate suspected misuse or compromise, protect University systems and information, maintain operations, or comply with applicable requirements.

Monitoring and investigations must be conducted by authorized personnel, limited to legitimate University purposes, and consistent with the Acceptable Technology Use Policy and applicable law.

When reasonably necessary to protect individuals, Institutional Data, IT Resources, or University operations, IT Services may take proportionate protective action. This may include restricting access, isolating systems or devices, blocking harmful activity, resetting credentials, preserving relevant information, or temporarily suspending a service.

D. Resilience, Incident Response, and Awareness

IT Services and responsible University units must maintain recovery and continuity capabilities proportionate to the criticality of their systems, services, information, and operations. Critical technology dependencies and recovery needs must be identified, and recovery arrangements must be documented, maintained, and periodically tested as appropriate to the risk.

Actual or suspected Cybersecurity Incidents and other security concerns must be promptly reported and handled in accordance with the Cybersecurity Incident Response and Business Continuity Policy, Cybersecurity Incident Response Plan, and established University reporting procedures.

Users must complete information security education or training required for their responsibilities and level of access. Individuals with privileged, technical, supervisory, or specialized responsibilities may be required to complete additional training.

E. Implementation and Exceptions

IT Services may establish and maintain risk-based security requirements, technical baselines,

procedures, and safeguards necessary to implement this policy. IT Services will communicate applicable requirements to affected University units and Users.

Exceptions to this policy or its supporting requirements must be documented, time-limited, and approved by the Chief Information Officer or designee. The Information Security Officer, responsible University leader, System Owner, Data Steward, Office of University Counsel, or other appropriate office must be consulted based on the nature of the exception.

Approved exceptions must identify the requirement involved, justification, affected systems and information, associated risks, compensating safeguards, and expiration date. Exceptions may not waive applicable legal, regulatory, contractual, research, or other binding requirements.

VI. VIOLATIONS

Violations of this policy may result in restriction or revocation of access, required training, disciplinary action, contract remedies, or other appropriate measures in accordance with applicable student, faculty, employment, contractual, and University policies and established processes.

Violations may also result in civil or criminal consequences when provided by law.

VII. RELATED INFORMATION

University Policies and Standards

- Acceptable Technology Use Policy
- Cybersecurity Incident Response and Business Continuity Policy
- Data Privacy Policy
- Data Privacy and Handling Standard
- Identity and Access Management Standard

Item	Description
University Links	Acceptable Technology Use Policy Seattle University Public Safety: Call (206) 296-5990 Seattle University IT Services Information Security: Email infosec@seattleu.edu or call (206) 220-8300 Human Resources Policies Faculty Handbook Code of Student Conduct Law Student Code of Student Conduct Data Privacy and Handling Standards
Forms	Security exception request form
Related Links	
Procedures	

