Policy Title:	Information Security Policy

Policy Number:	FAD.040	Date Approved:	January 16, 2024

A. Description

The purpose of this policy is to establish a security framework designed to protect Southern Oregon University's information assets from accidental or intentional unauthorized access, loss, alteration, or damage while supporting the open information-sharing needs of our academic culture.

SOU has a responsibility to protect the information entrusted to it, ensure the effective operation of business-critical processes, and abide by all laws and regulations governing the security of our information systems and the data they store, process, or transmit. Any part of this policy found to conflict with federal law, state law, local law, or any third-party regulation applicable to Southern Oregon University shall be superseded by the law or regulation governing that policy item.

B. Definition(s)

Southern Oregon University's information security program will adopt a policy structure building on industry best practices and terminology. The policy structure used by our information security program is as follows:

- **Policies:** These are high-level documents that outline an organization's overarching goals, objectives, and principles related to information security. Policies provide a framework for decision-making and guide the creation of more detailed documents further down the hierarchy. They are usually approved by senior management and are meant to be enduring and stable.
- **Standards:** Standards are more specific than policies. They provide detailed requirements that must be met to comply with the policy. Standards define what needs to be achieved and maintained to ensure security. They are often derived from industry best practices and may be influenced by regulations or legal requirements.
- **Baselines**: Baselines are a set of security configurations and settings that are considered the minimum acceptable level of security for various systems, applications, or devices within an organization. They are practical implementations of the standards and help maintain a consistent level of security across the organization.
- **Guidelines:** Guidelines offer recommendations, suggestions, and advice on how to implement the standards and baselines effectively. They provide more flexibility and context compared to standards and baselines.
- **Procedures:** Procedures are step-by-step instructions that detail the actions to be taken to perform specific tasks or processes. They are highly specific and operational documents that guide individuals in implementing security measures and responding to incidents in a consistent and standardized manner.
- **Policy Documents:** The term "policy documents" shall refer collectively to the set of policy documents

listed above (policies, standards, baselines, guidelines, and procedures).

Other terms used in this document include:

- **Information Security Program:** An information security program is a structured and comprehensive approach that an organization follows to manage and protect its sensitive information, data, systems, and assets from unauthorized access, disclosure, disruption, and modification. It involves a combination of policies, procedures, technologies, training, and ongoing assessment to mitigate security risks and ensure the confidentiality, integrity, and availability of information.
- **Asset:** An asset is any system, hardware or software, or any piece of information in any form, physical or electronic, belonging to the university.
- **Risk:** Risk refers to the potential for adverse consequences or negative impacts that may arise from uncertainties or events. In the context of information security, risk involves the likelihood and potential impact of security breaches, data loss, unauthorized access, and other threats to an organization's information systems and assets. It encompasses the evaluation of vulnerabilities, threats, and potential consequences to make informed decisions and implement measures that minimize or mitigate the impact of these risks.
- **Breach:** A breach, in the context of information security, occurs when there is an unauthorized or unintended access, disclosure, alteration, or destruction of sensitive or confidential information.

C. Policy Statement

This policy benefits the university by defining a framework that will assure appropriate measures are in place to protect the confidentiality, integrity, and availability of data and will assure all members of the Southern Oregon University community understand their roles and responsibilities, have adequate knowledge of security policy, procedures, and practices, and know how to protect the information entrusted to our care.

1. Scope

This policy is applicable to all members of the Southern Oregon University community and applies to all locations and operations of the institution. Specifically, the scope of this policy includes:

- All faculty, staff, students, contractors, consultants, temporary, and other workers using Southern Oregon University's network and/or systems, and/or any other persons who are acting on, for, or on behalf of Southern Oregon University
- All institutional data, whether individually controlled or shared, stand-alone or networked, including but not limited to administrative, teaching and learning, licensed, or any other data related to Southern Oregon University
- All computer and communication facilities owned, leased, operated, or contracted by Southern Oregon University and all devices that access or maintain institutional data, including but not limited to personal digital assistants, cell phones, personal computers, workstations, minicomputers, other wireless devices such as tablet computers, and any associated peripherals and software, regardless of whether used for administration, research, teaching, or other purposes
- Third-party vendors who collect, process, share, transmit, or maintain Southern Oregon University's institutional data, whether managed or hosted internally or externally.

2. Organizational Security

This policy establishes institution-wide strategies and responsibilities for ensuring the confidentiality, integrity, and availability of information assets that are created, accessed, managed, and/or controlled by Southern Oregon University. Information Assets addressed by the policy include, but are not limited to institutional data, information systems, computers, network devices, as well as paper documents and verbal communications.

This policy and corresponding standards will:

- Establish and maintain an institution-wide information assurance program and cybersecurity risk management framework
- Establish and maintain institution-wide security policies, standards, baselines, guidelines, and procedures which provide boundaries within which individuals and departments will operate
- Protect institutional data, systems, resources, and services against unauthorized access, unintended disclosure, and other threats or attacks that could potentially result in financial, legal, or reputational harm to Southern Oregon University, members of the Southern Oregon University community, or third parties to which Southern Oregon University owes a reasonable duty of care
- Educate faculty, staff, students, and departments on the need for appropriate cybersecurity and protecting themselves against breach of their systems
- Establish an exception process for individuals and departments with unique needs
- Support compliance with applicable federal, state, or local laws or regulations
- Implement security safeguards to fulfill Southern Oregon University's policies, guidelines, contracts, and agreements, and any safeguards required to comply with applicable laws and regulations
- Ensure Southern Oregon University's core mission is not impeded while ensuring the confidentiality, integrity, and availability of Southern Oregon University's information assets
- Reduce and better manage cybersecurity risks by implementing the measures outlined in this document and reviewing those security controls periodically to ensure their continued effectiveness

3. Institutional Roles and Responsibilities

a. **Executive Management:** Executive Management at Southern Oregon University, including the President and the President's Cabinet, with ultimate responsibility belonging to the President, have overall responsibility for:

   - Oversight of the provisions set forth in this policy
   - Holding the Chief Information Officer (CIO) and the Information Security Manager (ISM) accountable for implementing the provisions set forth in this policy and fulfilling their responsibilities as defined herein
   - Evaluating and accepting risk on behalf of Southern Oregon University, and empowering the Chief Information Officer to evaluate and accept certain risks on their behalf
   - Identifying high-level information security responsibilities and goals

- Supporting the consistent implementation of information security policies and standards
- Supporting security through clear direction and demonstrated commitment of appropriate resources
- Implementing the governing process for determining information classification and categorization, based on industry recommended practices, organization directives, and legal and regulatory requirements, to determine the appropriate levels of protection for that information
- Determining who will be assigned and serve as data owners while maintaining ultimate responsibility for the confidentiality, integrity, and availability of Southern Oregon University's data
- Participating in the response to security incidents
- Complying with notification requirements in the event of a breach of private information
- Adhering to specific legal and regulatory requirements related to information security
- Communicating legal and regulatory requirements to the Chief Information Officer, Information Security Manager, or designated security representative
- Supporting the communication of the requirements of this policy and the associated standards, including the consequences of non-compliance, to the workforce and third parties, and addressing adherence in third-party agreements.

b. **Department Leaders:** Department Leaders include 1) faculty department chairs; 2) administrators responsible for overseeing academic schools, divisions, or colleges; and 3) administrators who oversee administrative departments such as Business Services, Human Resources, and Campus Public Safety. They play a pivotal role in determining the affairs of their respective departments. Department Leaders are responsible for:

- Understanding information security responsibilities and goals within their areas and integrating them into relevant policies and processes with the assistance of the Chief Information Officer, the Information Security Manager, or a designated security representative
- Supporting the consistent implementation of information security policies and standards within their areas
- Acting as data owners and ensuring the confidentiality, integrity, and availability of all information under their care with support from the Information Technology department
- Cooperating with the response to security incidents

c. **Chief Information Officer (CIO):** The Chief Information Officer is responsible for:

- Maintaining familiarity with business functions and requirements
- Evaluating and accepting risks delegated to the Information Technology department by Executive Management
- Developing policy documents that fulfill the provisions of this policy and protect Southern Oregon University from risk
- Developing the security program and strategy, including measures of effectiveness
- Allocating resources needed to maintain a level of information security control consistent with this

policy

- Fostering the participation of information security and technical staff in protecting information assets, and in identifying, selecting, and implementing appropriate and cost-effective security controls and procedures
- Supporting the design and implementation of Southern Oregon University's disaster recovery plans

d. **Information Security Manager (ISM):** The Information Security Manager is responsible for:

- Assisting the Chief Information Officer with all of the duties of that position defined above.
- Maintaining an adequate level of current knowledge and proficiency in information security to provide in-house expertise
- Developing and implementing policy documents that fulfill the provisions of this policy and protect Southern Oregon University from risk
- Enforcing SOU's information security policies
- Providing incident response coordination and expertise

e. **Information Technology Staff:** Information Technology Staff are responsible for:

- Acting honorably, honestly, justly, responsibly, and legally with respect to their privileges and their roles as data custodians
- Implementing all processes, policies, and controls relative to security requirements defined by the business and this policy with assistance from the Information Security Manager
- Supporting the Information Security Manager in enforcing compliance with SOU's information security policies

f. **All members of the Southern Oregon University community:** All faculty, staff, students, contractors, consultants, temporary, and other workers using Southern Oregon University's network and/or systems, and/or any other persons who are acting on, for, or on behalf of Southern Oregon University are responsible for:

- Understanding the baseline information security controls necessary to protect the confidentiality, integrity, and availability of information entrusted to them
- Protecting university information and technology resources from unauthorized use, modification, tampering, or disclosure
- Abiding by all Southern Oregon University security policies and standards, especially the Acceptable Use of Information Technology Resources Policy.
- Promptly reporting suspected information security incidents, weaknesses, or violations of security policy to the Information Security Manager or an appropriate manager, advisor, or other person in a position to act on a report and refer it to the Information Security Manager
- Cooperating with security incident investigations and response

4. Exceptions and Exemptions

Southern Oregon University recognizes that campus departments will have unique needs and security concerns. Exceptions to any provision of Southern Oregon University's security policies or supplemental standards must be approved in accordance with the Security Policy Exceptions Procedure.

Any questions about the contents of this policy or supplemental policies or standards should be referred directly to the Information Security Manager (infosec@sou.edu).

5. POLICY VIOLATIONS

Violations of Southern Oregon University's information security policy may result in:

- Responsibility for remediation costs associated with a security incident
- Regulatory non-compliance penalties
- Disciplinary action up to and including termination of employment or affiliate status with Southern Oregon University
- Academic discipline
- Other penalties including but not limited to financial penalties, civil or criminal proceedings, legal fees, and other costs

This policy may be revised at any time without notice. All revisions supersede prior policy and are effective immediately upon approval.

D. Relevant Authority

Reviewed and updated by Chief Information Officer Tom Battaglia and David Raco, Information Security Manager.

E. Other Information

none

The Policy Contact, defined above, will write and maintain the procedures related to this policy and these procedures will be made available within the Custodial Office.