Policy Title:	Information Security Policy

Governing Body:	Finance and Administration	Policy Number:	FAD.040
Policy Contact:	Chief Information Officer	Date Revised:	6/16/2016
Custodial Office:	Information Technology	Date Approved:	
Approved By:	President/Cabinet	Next Review:	
Related Policy:	SOU Surplus Computer Equipment Disposal Policy FAD.041 SOU Acceptable Use Policy FAD.038 Oregon Identity Theft Protection Act 646A.600 http://www.cbs.state.or.us/dfcs/id_theft.html		

Revision History

Revision Number:	Change:	Date:
1.1	Update to template format, significant changes.	**9/19/2013**
1.2	Template update, removal of OUS references	**6/16/2016**

A. Purpose

The purpose of this policy is to document Southern Oregon University's requirements around information security and data handling. SOU has a responsibility to protect information entrusted to it, ensure the effective operation of business critical processes, and abide by the laws and regulations at the federal, state, and local level relating to information security. No part of this policy is meant to conflict with existing federal, state, local laws or regulations. In the event of a conflict, the existing law and higher-level policy will take precedence.

B. Definitions

Protected Information

Protected Information is information for which there are legal requirements for preventing disclosure or financial penalties for disclosure. Personally identifiable information, financial records, and student records are examples of institutional information in this class. This information is protected by statutes, rules, regulations, university policies, and/or contractual language. The highest levels of restriction apply, both internally and externally, due to the potential risk or harm that may result from disclosure or inappropriate use.

Examples:
FERPA-protected student information

Employee data and certain personnel documents/records
Credit/Purchasing card numbers
Human subject information
HIPAA-protected health information

Sensitive Information

Sensitive Information is information that will not necessarily expose the university to loss if disclosed, but that the Records Custodian feels shall be guarded against unauthorized access or modification due to proprietary, ethical, or privacy considerations. High or moderate levels of restriction apply, both internally and externally, due to the potential risk or harm that may result from disclosure or inappropriate use. This classification applies even though there may not be a statute, rule, regulation, university policy, or contractual language prohibiting its release. Sensitive Information is generally only available to members of the University community who have a legitimate purpose for accessing such information.

Examples:
Research data where the corresponding research is unpublished
Responses to a Request for Proposal before decision is reached
Financial transactions
Library transactions

Unrestricted Information

Unrestricted Information, while subject to university disclosure rules, may be made available to members of the university community and to individuals and entities external to the University. In some cases, general public access to unrestricted information is required by law.
While the requirements for protection of Unrestricted Information are considerably less than for Protected or Sensitive Information, sufficient protection will be applied to prevent unauthorized modification of such information.

Examples:
Press releases
High-level enrollment statistics
Course catalog
FERPA defined directory information

C. Policy Statement

1. Introduction

Information Security Policies apply to all members of the SOU Community; however, in certain circumstances specific restrictions on information may be required by the terms of a grant, federal law, or departmental policies. In the event of an inconsistency or conflict, applicable law supersede University policies and University policies supersede college, department or lower unit bylaws, policies, or guidelines. This section applies to all University community members, whether students, faculty, staff, volunteers, contractors, affiliates, or agents, who have access to University Information Systems and to all University units and their agents including external third-party relationships.

2. Scope

This policy applies to all university information and all systems and processes that may access this information, regardless of the environment where the data resides or is processed; for example, the university enterprise system, other enterprise servers, distributed departmental servers, or personal workstations and mobile devices.

This policy applies regardless of the media on which data resides, for example electronic, microfiche, paper, CD, DVD, or other media. It also applies regardless of the form the information may take, for example text, graphics, video or audio, or their presentation.

University units may have additional policies for information within their areas of operational or administrative control. In the event these local policies conflict with university policy, this policy applies.

3. Institutional Responsibilities

a. President: The President has overall oversight responsibility for institutional provisions set forth in this policy. The President will hold the Chief Information Officer and CISO accountable for instituting appropriate policy and programs to ensure the security, integrity, and availability of SOU's information assets.

b. Chief Information Officer: The Chief Information Officer is responsible for ensuring that the institutional policies governing information systems, user and personal information security, security operations, network and telecommunications security, physical and environmental security, disaster recovery, and awareness and training are developed and adhered to in accordance with this policy.

c. Chief Information Security Officer (CISO): The CISO is responsible for the university's security program and for ensuring that institutional policies, procedures, and standards are developed, implemented, maintained and followed.

4. Records Custodians

Records Custodians are designated by the University President to ensure accountability and proper records handling for institutional data regardless of which individual collects this information on behalf of the university. These data include student records, financial records, and human resource records. For the purposes of this policy, university personnel who collect data that do not fit these categories are recognized as the appropriate Records Custodian for that data. Faculty members who collect, store, or supervise the collection of data, including that of their students, are considered the records custodians for that information.

The following Records Custodians have planning, management, and policy-level responsibility for institutional information within their functional areas:

- Director of Business Services – Responsible for institutional financial records.
- Registrar – Responsible for institutional student records.
- Director of Finance and Administration, SOU Foundation– Responsible for fundraising, alumni, and donor records.
- Director of Human Resources – Responsible for institutional employee and employment records.
- Director of Student Health and Wellness Center – Responsible for protected health information maintained by the Student Health and Wellness Center.

All Records Custodians have the responsibility to ensure appropriate handling of information entrusted to the institution. Records Custodians with student record, employee data, or business transactions responsibilities have a responsibility to ensure that those business needs that require handling these elements are limited to the employees required to handle this information and that reasonable controls and precautions to protect these elements are in place.

Records Custodians shall do the following:

- Develop, implement, and manage information access policies and procedures.
- Ensure compliance with contractual obligations and/or federal, state, and University policies and regulations regarding the release of, responsible use of, and access to information.
- Assign information classifications based on a determination of the level of sensitivity of the information.
- Assign appropriate handling requirements and minimum safeguards which are merited beyond baseline standards.
- Promote appropriate data use and data quality, including providing communication and education to data users on appropriate use and protection of information.
- Develop and implement record and data retention requirements in conjunction with university archives.

5. University Community Responsibilities

All members of the university community, including faculty, staff, other employees, and affiliated third party users, have a responsibility to understand the relative sensitivity of information they handle, protect the information entrusted to the institution, and abide by university policy regarding protections afforded that information. These protections are designed to comply with all federal and state laws, regulations, and policies associated with information security.

These responsibilities include:

- Comply with university policies, procedures, and guidelines associated with information security.
- Implement the minimum safeguards as required by the designated Records Custodian and Chief Information Security Officer based on the information classification.
- Comply with handling instructions for protected information as provided by the designated Records Custodian and Chief Information Security Officer.
- Report any data misuse or data quality issues to your supervisor, who will contact the Records Custodian and/or Chief Information Officer for remediation.
- Report any suspected data breaches or unauthorized access to the Chief Information Security Officer as soon as they are discovered.
- Participate in education, as required by the designated Records Custodian(s), on the required minimum safeguards for protected information.

All personnel granted access to protected or sensitive information shall be instructed on the proper use and handling of this information and are subject to SOU policies regarding security sensitive personnel. Under no circumstances shall protected or sensitive information be disclosed to anyone outside SOU without authorization from the appropriate supervisory personnel.

6. Information Systems Security Requirements

a. Baseline Standards for Protected Information

All computer systems (workstations and servers) which store or process protected information shall have: restricted access to only authorized personnel; fully patched operating systems and applications; antivirus software with current virus definitions; and, if attached to the network, will be in a secured zone protected by appropriate firewall rules.

b. Baseline Standards for Sensitive and Unrestricted Information

All computer systems (workstations and servers) which store or process sensitive or unrestricted information shall have: restricted access granted only to authorized personnel; fully patched operating systems and applications, and current antivirus software with current virus definitions.

c. Additional Requirements for Specific Protected Information

Certain data elements pose an additional risk of identity theft to our community members should they be compromised through unauthorized access. Additional guidelines are provided below for each of these data elements.

- **Social Security Number**: All access and use of the Social Security Numbers is prohibited except for meeting Federal or state requirements, compliance and reporting.
- **Credit Card Numbers**: All access and use of credit card numbers shall meet Procurement Card Industry (PCI) security standards.
- **Bank Account Numbers**: All access and use of bank account numbers is restricted to the following uses:
  Business Services
  Processing direct deposit transactions; Processing wire transfers
  Human Resources/Payroll
  Enrolling employees in direct deposit.
- **Driver's License Numbers and/or State Identification Numbers**: All access and use of driver's license and/or state identification numbers will be reported to the CISO and all reasonable precautions will be taken to ensure the integrity and confidentiality of this information.

d. Mobile Computing and Removable Media

All protected information stored on mobile computer systems or removable media shall be protected by encryption. Media or computers systems that cannot meet this requirement must be stored in a physically secure area and shall only be transported in a secure manner.

e. Protection of Paper Records

Paper documents that include protected or sensitive including student education records, an individual's medical information, benefits, compensation, loan, or financial aid data, and faculty and staff evaluations are to be secured during printing, transmission (including by fax), storage, and disposal.

f. **Transmission and Transportation of Protected Information**

Encryption must be used when required by law, regulatory requirement or University policy, and when determined necessary by the Records Custodians and the CISO. Protected information should not be transmitted over any network outside of secured zones within the SOU network, unless appropriate and standard encryption techniques are used. Under no circumstances will this information be transmitted across an unsecured network in clear text.

All physical transportation of protected information shall be done by a trusted courier who can provide document and pouch-level traceability. In the case where person information for more than fifty individuals is to be transported either in paper or unencrypted electronic form; sealed pouches for paper documents and lock boxes for transport of removable media are required.

g. Disposal of Surplus Property

All electronic storage media are subject to the SOU Surplus Computer Equipment Disposal Policy.

7. Incident Response and Escalation

All suspected data breaches must be reported to the Chief Information Security Officer immediately.

Incident response will follow the guidelines established in the SOU Information Technology Incident Response Plan.

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

D. Policy Consultation

Business Affairs Council, Tech Council, Provost's Advisory Council

E. Other Information

ISO 27000 Series (www.27000.org):
The ISO 27000 series of standards have been specifically reserved by ISO for information security matters and will be populated with a range of individual standards and documents
Control Objectives for Information and related Technology (COBIT) (www.isaca.org/cobit):
COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks.

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.