POLICY

.100 POLICY STATEMENT

The Oregon University System (OUS) takes its responsibility to protect and care for the information entrusted to us by our students, faculty, staff, and partners seriously. This policy summarizes three requirements of OUS institutions in meeting our obligations pertaining to information security:
• Data identification and classification
• Incident response
• Training

In the absence of any other institutional specific policy governing information security, this policy will apply.

.110 POLICY RATIONALE

OUS seeks to ensure that the policies and procedures related to information security are documented, communicated, clearly understood, and consistently applied.

.120 AUTHORITY

• OAR 580-040-0205, Code of Ethics
• OAR 580-055-0000, OUS Information Security Policies
• Oregon 2007 Consumer Identity Theft Protection Act
• Family Educational Rights and Privacy Act (FERPA)

.130 APPROVAL AND EFFECTIVE DATE OF POLICY

Approved by the Vice Chancellor for Finance and Administration on 06/23/10.

.140 KNOWLEDGE OF THIS POLICY

All institutional and Chancellor’s Office personnel, in the absence of a campus-specific policy, should be knowledgeable of this policy.

.160 RESPONSIBILITIES

A. INSTITUTION

I. President:

The institutional president or designee has overall oversight responsibility for institutional provisions set forth in this policy.

II. Chief Information Security Officer or equivalent:

The campus CISO or equivalent is responsible for the institution’s security program and for ensuring that procedures and standards are developed, implemented, maintained, and adhered to.

III. Records Custodian:
The following Records Custodians have management responsibility for defined segments of institutional information:

**Director of Business Affairs** – Responsible for institutional financial records.

**Director of Human Resources** – Responsible for institutional employee and employment records.

**Provost or Designee** – Responsible for institutional student records.

University personnel who collect data that do not fit these categories are recognized as the appropriate records custodian for that data.

Records Custodians shall do the following:

1. Ensure compliance with contractual obligations and/or OUS, federal, state, and university policies and regulations regarding the release of, responsible use of, and access to information.
2. Provide communication and education to users on appropriate use and protection of information.
3. Develop and implement record and data retention requirements in conjunction with university archives.

**IV. Data Owner:**

The data owner, usually a director or department head, has the responsibility for the integrity, accurate reporting, and use of data in his/her department. The data owner shall:

1. Assign information classifications based on a determination of the level of sensitivity of the information. (See Information Identification and Classification, section .210 of this policy.)
2. Assign appropriate handling requirements and minimum safeguards which are merited beyond baseline standards of care. (See Information Handling -- Baseline Standards of Care, section .220 of this policy.)

**V. User:**

Individuals, including faculty, staff, other employees, and affiliated third party users, who are part of the OUS community, have a responsibility to understand the relative sensitivity of information they handle, and to protect the information entrusted to the institution.

Responsibilities include:

1. Complying with OUS policy, procedures, and guidelines associated with information security.
2. Implementing the minimum safeguards as required by the data owner and/or records custodian based on the information classification.
3. Complying with handling instructions for protected information as provided by the data owner and/or records custodian.
4. Reporting any unauthorized access, data misuse, or data quality issues to the data owner, who will follow incident response procedures. (See section .240.)

B. CHANCELLOR'S OFFICE

I. Chancellor

The OUS Chancellor or designee has oversight responsibility for the provisions of this policy.

II. Chief Information Security Officer (CISO):

The System CISO is responsible for ensuring that the institutional information security plans governing information systems, user and personal information security, physical and environmental security, and awareness and training are developed and adhered to in accordance with this policy. For OUS, this function is currently performed by the Vice Chancellor for Finance and Administration.

.200 INFORMATION IDENTIFICATION & DATA CLASSIFICATION

Each OUS institution will identify and classify its information assets into one of three levels of sensitivity and risk: Protected, Sensitive, and Unrestricted. Proper levels of protection will be implemented to protect these assets relative to the classification.

A. Protected Information

Protected information is information for which there are legal requirements for preventing disclosure or financial penalties for disclosure. e.g., personally identifiable information and student records. The highest levels of restriction apply due to the potential risk or harm that may result from disclosure or inappropriate use.

Protected information must be protected from unauthorized access, modification, transmission, storage, or other use, and should be disclosed to individuals on a need-to-know basis only. Disclosure to parties outside the university is generally not permitted and must be authorized by the data owner, as outlined in this policy.

Examples:

- FERPA-protected student information
- Employee data and certain personnel documents/records
- Credit/Purchasing card numbers
- Human subject information
- Lab animal care information
- HIPAA-protected health information

B. Sensitive Information

Sensitive information is information that would not necessarily expose the university to loss if disclosed, but that should 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 must be protected from unauthorized access, modification, transmission, storage or other use, and is generally available to members of the university community who have a legitimate purpose for accessing such information. Disclosure to parties outside of the university should be authorized by the data owner, as outlined in this policy.

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

C. 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:
- Publicly posted press releases
- High-level enrollment statistics
- Course catalog

.210 BASELINE STANDARDS OF CARE
Specific additional handling requirements above the baseline may be required by the records custodian to ensure compliance with law, policy, or contractual obligation. Advanced security practices beyond the baseline are encouraged where practicable (such as employing encryption technologies).

A. Baseline Standards for Protected Information

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

Under no circumstances shall protected information be disclosed to anyone outside OUS without authorization from the appropriate records custodian, as outlined in this policy.

If protected information needs to be transmitted, it must be encrypted using current encryption standards.

B. Baseline Standards for Sensitive Information

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

All personnel granted access to sensitive information shall not disclose this information to parties outside of OUS without authorization by the appropriate records custodian, as outlined in this policy.

If sensitive information needs to be transmitted, it must be encrypted using current encryption standards.

C. Baseline Standards for Unrestricted Information

All computer systems which store or process unrestricted information shall have write access restricted to authorized personnel only to ensure that information presented is not edited without appropriate authorization. Any such computer system should have fully patched operating systems and applications, and current antivirus software with current virus definitions.

D. Mobile Computing

All mobile computer systems or portable storage media which store protected and sensitive information shall be encrypted with at least the 128 bit encryption common in operating systems and encoding devices sold in the United States in addition to the baseline requirement prescribed in this policy. Those that cannot meet this requirement
due to the proprietary nature of how they are created, such as back-up tapes, must be stored in a physically secure area and shall only be transported in a manner commensurate with this policy.

.220 PERSONAL INFORMATION PRIVACY

Each element below merits extra protections beyond any baseline.

Social Security Number: All access and use of the social security number is prohibited except for meeting federal or state requirements, compliance and reporting.

VISA/Credit Card Numbers: All access and use of VISA/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 Affairs
  - Processing direct deposit transactions, both incoming and outgoing
  - Processing wire transfers
- Department Personnel
  - Processing wire transfers – Paper copies of this data may be stored during the processing phase. They should be kept in a physically secure location with limited personnel access. Departments are prohibited from storing electronic copies of this data. Once verification of transfer is complete, the paper copy should be redacted or destroyed through an approved confidential document destruction method, and in accordance with the OUS records retention schedule found at /about/records.

Driver’s License Numbers and/or National Identification Numbers: All access and use of state or national driver’s license and/or national identification numbers for Oregon residents will be reported to the campus CIO/CISO and all reasonable precautions will be taken to ensure the integrity and confidentiality of this information.

Specific procedures for handling these elements will be defined by the records custodians for student records, employee data, and business transactions.

.230 PROTECTING INFORMATION STORED ON PAPER

Paper documents that include protected or sensitive information such as social security numbers, 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.
• Do not leave paper documents containing protected or sensitive information unattended; protect them from the view of passers-by or office visitors.
• Store paper documents containing protected or sensitive information in locked files.
• Store paper documents that contain information that is critical to the conduct of university business in fireproof file cabinets. Keep copies in an alternate location.
• Do not leave the keys to file drawers containing protected or sensitive information in unlocked desk drawers or other areas accessible to unauthorized personnel.
• All records are subject to OUS records retention policies and should be only be disposed of in accordance with the retention schedule defined within those policies. More information can be found at /about/records. Once the retention schedule has been met, shred confidential paper documents and secure such documents until shredding occurs.
• Make arrangements to retrieve or secure documents containing protected or sensitive information immediately that are printed on copy machines, fax machines, and printers. If at all possible, documents containing protected information should not be sent by fax. Those documents should be sent via a trusted courier service and secured in transit.
• Double-check fax messages containing protected or sensitive information:
  o Recheck the recipient's number before you hit 'start.'
  o Verify the security arrangements for a fax's receipt prior to sending.
  o Verify that you are the intended recipient of faxes received on your machine.

.240 INCIDENT RESPONSE
Incident response flowchart in .pdf format

All information security incidents will be reported to the campus CISO or equivalent, who will complete an incident report. (See Appendix section .700, Sample Incident Response Form.)

Information security incidents involving protected information will be reviewed by legal counsel to ensure appropriate responses are taken in accordance with Oregon law, and a copy of the report will be shared with the appropriate records custodian(s), the university president, the OUS CISO, the OUS Internal Audit Division, and the OUS Communications Services as appropriate to deal with media implications.

Information security incidents involving sensitive information will be reviewed by the appropriate records custodian(s) along with a copy of the incident report to be shared as deemed appropriate by the records custodian(s).

.250 TRAINING

OUS campuses and the Chancellor's Office will do the following:

- integrate training for proper handling of protected information in the Banner training required by all employees seeking access to the Banner system.
- include information about stopping ID theft in new employee orientation.
The OUS CISO will:

- send OUS employees (via the campus CISO email Listserv) ad hoc bulletins regarding urgent threats, time sensitive initiatives, training opportunities and tools, etc.

.690 CONTACT INFORMATION

Direct questions about this policy to the following offices:

<table>
<thead>
<tr>
<th>Subject</th>
<th>Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>General questions from institutional personnel</td>
<td>Campus CISO or equivalent</td>
</tr>
<tr>
<td>General questions from institutional central administration and Chancellor's Office personnel</td>
<td>OUS CISO (currently the Vice Chancellor for Finance and Administration)</td>
</tr>
</tbody>
</table>

.695 HISTORY

06/23/10 - Approved

Policy Last Updated: 06/24/10

APPENDIX

.700 FORMS

Sample Incident Response Form

.995 HISTORY

06/23/10 Approved

Appendix Last Updated: 06/24/10