OREGON INSTITUTE OF TECHNOLOGY

Information Security Manual
OIT-30-007

Effective 04/05/11

Oregon Institute of Technology

Information Security Manual v1.7

Table of Contents:

OREGON INSTITUTE OF TECHNOLOGY

Information Security Manual
OIT-30-007

Effective 04/05/11

ISM 001: Introduction

Section 000: Introductory Material

This Information Security Manual documents key elements of the Oregon Institute of Technology's Information Security Program, including Policies and Procedures required by Oregon law, Oregon University System Rules, and Information Security best practices. Its formation was specifically dictated by the Oregon University System Information Security Policy (OAR 580-055-0000) and the Oregon Consumer Identity Theft Protection Act of 2007 (more info at http://www.cbs.state.or.us/dfcs/id_theft.html).

OIT takes its responsibility to protect and care for the information entrusted to us by our students, faculty, staff, and partners seriously. Policies and Procedures outlined in this manual are meant to document how we will meet our responsibilities as stewards of information entrusted to us as an institution of higher education. This manual is not intended to be step by step guide for faculty and staff; however, elements of it may be required reading in certain circumstances.

Information Security Policies apply to all members of the OIT 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 and the State Board of Higher Education's policies supersede University policies and University policies supersede college, department or lower unit bylaws, policies, or guidelines.

These policies and procedures apply regardless of the media on which information resides. Specifically they apply to paper and traditional hard copy information, as well information on electronic, microfiche, CD\DVD, or other media. They also apply regardless of the form the information may take; for example: text, graphics, video or audio, or their presentation.

ISM 101: Institutional Responsibilities

Section 100: Information Security Roles and Responsibilities

Purpose

The purpose of this Institutional Responsibilities document is to clearly outline the roles of President, CIO, and CISO in fulfilling OIT's responsibilities with respect to information security as directed in the OUS Information Security Policy.

Institutional Responsibilities

President: As directed in the OUS Information Security Policy, the President has overall oversight responsibility for institutional provisions set forth in that policy. The President will hold the CIO and CISO accountable for instituting appropriate policy and programs to ensure the security, integrity, and availability of OIT's information assets.

Chief Information Officer (CIO): As directed in the OUS Information Security Policy, the CIO 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 the OUS policy.

Chief Information Security Officer (CISO): Reporting to the CIO, the CISO is responsible for the member institution's security program and for ensuring that institutional policies, procedures, and standards are developed, implemented maintained and adhered to.

Currently the CIO is also the CISO at OIT.

ISM 102: University Community Responsibilities

Section 100: Information Security Roles and Responsibilities

Purpose

The purpose of this section is to clarify individual responsibility in handling information entrusted to the institution.

Background

The University is required to protect certain information by federal laws, state laws, and State Board of Higher Education administrative rules. However, ready access to information is a requirement for academic inquiry and the effective operation of the institution. Current information technology makes it easier than ever for individuals to collect, process, and store information on behalf of the University; therefore, all individuals acting on behalf of the university need to understand their responsibilities.

Responsibilities

Individuals, including faculty, staff, other employees, and affiliated third party users, who are part of the University Community have a responsibility to protect the information entrusted to the institution. When special protections are warranted, the appropriate Records Custodian will define appropriate handling requirements and minimum safeguards. All members of the OIT Community have an obligation to understand the relative sensitivity of information they handle, 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.

Responsibilities include:

- Comply with University policies, procedures, and guidelines associated with information security.

- Implement the minimum safeguards as required by the Records Custodian based on the information classification.

- Comply with handling instructions for Protected Information as provided by the Records Custodian.

- Report any unauthorized access, data misuse, or data quality issues to your supervisor, who will contact the Records Custodian for remediation.

- Participate in education, as required by the Records Custodian(s), on the required minimum safeguards for Protected Information.

ISM 103: Records Custodians

Section 100: Information Security Roles and Responsibilities

OREGON INSTITUTE OF TECHNOLOGY

Information Security Manual
OIT-30-007

Effective 04/05/11

Purpose

The purpose of this section is to clarify the role of "Records Custodian" as defined in OIT policy and practice, to ensure that specific University obligations are met.

Background Information

In accordance with state law and University standard practice, certain 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 Information Security Policy, University personnel who collect data that do not fit these categories are recognized as the appropriate Records Custodian for that data.

Responsibilities

The following Records Custodians have planning and policy-level responsibility for Information Systems within their functional areas and 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.

Registrar – Responsible for institutional student records.

All Records Custodians have the responsibility to ensure appropriate handling of information entrusted to the institution.

Records Custodians should do the following:

1. Develop, implement, and manage information access policies and procedures.
2. Ensure compliance with contractual obligations and/or federal, state, and University polices and regulations regarding the release of, responsible use of, and access to information.
3. Assign information classifications based on a determination of the level of sensitivity of the information (see OIT ISM 202: Information Systems – Classification Standards.)

4. Assign appropriate handling requirements and minimum safeguards which are merited beyond baseline standards of care as defined in OIT ISM 203.
5. Promote appropriate data use and data quality, including providing communication and education to data users on appropriate use and protection of information.
6. Develop and implement record and data retention requirements in conjunction with University Archives.

OU ISM 201: Information Systems Security - General

Section 200: Information Systems Security

Purpose

The purpose of this section is to define in general terms what is meant by Information Systems Security and to set forth the University's commitment to create and maintain an Information Security Program.

Scope

Information Systems are composed of three major components: data, applications, and infrastructure systems. All three must be addressed in order to ensure overall security of these assets.

Information Security Program

OIT hereby establishes an Information Security Program by adopting and documenting within this Information Security Manual, policies, procedures, security controls, and standards which govern Information Systems including data, applications, and infrastructure systems as those assets are classified according to their relative sensitivity and criticality. This program should ensure that fundamental security principles, such as those embodied in the ISO 27000 series standards or those generally incorporated into the COBIT framework, are established and maintained.

The foundation of this Information Security Program will be the established information classification system and baseline standards of care established in this manual; however, for these to be effective all three aspects of information systems must be addressed. This is not just about data, it is also about how data are stored and processed.

OREGON INSTITUTE OF TECHNOLOGY

Information Security Manual
OIT-30-007

Effective 04/05/11

ISM 202: Information Systems – Classification Standards

Section 200: Information Systems Security

Purpose

The purpose of this section is to provide guidance and standards regarding the classification of Institutional Information. Institutional Information is defined as all information created, collected, maintained, recorded, or managed by the University, its staff, and all agents working on its behalf. It is essential that Institutional Information be protected. There are, however, gradations that require different levels of security and accurate classification provides the basis to apply an appropriate level of security to OIT's Information Systems. It is the Records Custodian's responsibility to review Institutional Information periodically and classify each according to its use, sensitivity, and importance and to implement appropriate security requirements.

Information Classifications: Protected, Sensitive, and Unrestricted

202-01: 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.

Protected Information must be protected from unauthorized access, modification, transmission, storage, or other use. Protected Information 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 appropriate supervisory personnel. Employees may be required to sign non- disclosure agreements before access to Protected Information is granted.

202-02: Sensitive Information

Sensitive Information is information that would not necessarily expose the University to loss if disclosed, but that the Records Custodian feels 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. Sensitive Information 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 appropriate supervisory personnel.

202-03: 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.

Scope

This section applies to all Institutional Information and all systems, processes, and data sets that may access this information, regardless of the environment where the data resides or is processed; for example the University mainframe enterprise server, other enterprise servers, distributed departmental servers, or personal workstations and mobile devices. All information with a designated Records Custodian must meet the same classification level and utilize the same protective measures as prescribed by the Records Custodian for the central systems.

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, University Policy applies.

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.

ISM 203: Information Systems – Baseline Standards of Care

Section 200: Information Systems Security

Purpose

The purpose of this policy is to define the baseline standards of care based on the designated classification of Information Systems.

Standards of Care

The following standards apply to people and machines that have access to and/or process information according to its classification as Protected, Sensitive, or Unrestricted. Specific additional handling requirements above the baseline may in fact 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).

203-01 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; 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. Workstations used by authorized personnel with direct write access to Protected Information will also be configured to automatically apply patches and current anti-virus definitions and will not be accessed via a local system administrator or domain administrator account on the local machine for day-to-day activities.

All personnel granted direct access to Protected Information should be instructed on the proper use and handling of this information and are subject to OIT Policies regarding security sensitive personnel. Under no circumstances should Protected Information be disclosed to anyone outside OIT without authorization from the appropriate supervisory personnel.

203-02 Baseline Standards for Sensitive Information

All computer systems which store or process Sensitive Information should have restricted access granted only to authorized personnel affiliated with OIT, and shall have fully patched operating systems and applications, and current antivirus software with current virus definitions. Any such computer system is also subject to general configuration requirements established by [Information Technology Services].

All personnel granted access to sensitive information should not disclose this information to parties outside of OIT without authorization by appropriate supervisory personnel.

203-03 Baseline Standards for Unrestricted Information

All computer systems which store or process Unrestricted Information will have write access restricted only to authorized personnel to ensure that information presented is not edited without appropriate authorization. Any such computer system is also subject general configuration requirements established by [Computing Services] and should have fully patched operating systems and applications, and current antivirus software with current virus definitions.

203-04 Mobile Computing

All mobile computer systems or portable storage media, which store Protected 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 203-01. 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 OIT ISM 601-03.

As noted in the Personal Information Privacy Policy (OIT ISM 301), certain highly sensitive data elements are strictly prohibited from portable media.

Oregon Institute of Technology ISM 301: Personal Information Privacy

Section 300: User and Personal Information Security

Purpose

The purpose of this policy is to establish clear guidelines for handling specific data elements which pose a risk of Identity Theft to our community members, should those data elements be compromised through unauthorized access due to a breach of security. These data elements are generally used in conjunction with other information, such as full name, which may constitute enough information to establish credit or perpetuate other forms of fraud associated with Identity Theft.

Scope

This policy is applicable to all OIT community members including all employees, students, contractors, consultants, agents, and vendors working on OIT's behalf. It is applicable to *all* OIT Information Assets, regardless of form or media. It applies to information gathering, protection, use, processing, storage, communications, and transit.

Policy

Each element below merits extra protections beyond any baseline.

Social Security Number: All access and use at OIT 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 at OIT of VISA/Credit Card numbers shall meet Procurement Card Industry (PCI) security standards and any system handling these numbers shall have a responsible party of record who will be accountable to the Director of Business Affairs for ensuring compliance.

Bank Account Numbers: All access and use of bank account numbers at OIT 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 approved OIT confidential document destruction method.

.

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 at OIT will be reported to the Chief Information Security Officer and all reasonable precautions will be taken to ensure the integrity and confidentiality of this information.

Under no circumstance shall Social Security Number, VISA/Credit Card Numbers, Bank Account Numbers, or Driver's License/National Identification Numbers be stored in a non-redacted form on any portable electronic media including but not limited to laptops, flash drives, CDROMS.

Procedures

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

Responsibilities

All members of the OIT community have a responsibility to protect these elements and ensure that they are handled with the utmost care. All efforts should be made to avoid the direct storage and use of these elements unless required by business need.

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.

OREGON INSTITUTE OF TECHNOLOGY

Information Security Manual
OIT-30-007

Effective 04/05/11

ISM 302: User Specific Policies

Section 300: User and Personal Information Security

Purpose

The purpose of this section is to outline existing OIT User specific policies which fulfill OIT's obligations under the OUS Information Security Policy.

Policies and Procedures

302-01 Acceptable Use Policy (AUP)
OIT maintains the [Computer Use Policy] here: [30-005] Acknowledgement of this policy and agreement to abide by it are part of the account activation process for all central computer systems.

302-02 Security Sensitive Personnel
OIT maintains a policy regarding criminal background checks for Security Sensitive Personnel in compliance with Oregon Administrative Rules and as part of the Office of Human Resources Policy and Procedure Manual.

302-03 Account Management
OIT Information Technology Services creates system accounts for general access to OIT computer resources. These accounts are generated and disabled programmatically based on information stored in the Student and Human Resources Information Systems about current status as employee or student. In addition to these accounts, local system accounts are created for access to specific systems such as banner, and in the case of the Banner Human Resources, Student, and Financial Information System, accounts are authorized and revoked in accordance with parameters set by the appropriate Records Custodian.

ISM 401: Transmission of Protected Information

Section 400: Network and Telecommunications Security

Purpose

The purpose of this section is to state OIT’s policy regarding the transmission of protected information over the network.

Background

Once information is classified as Protected Information, established baseline standards ensure that the information resides and is processed within a secured zone of the network. However, normal business operation does from time to time require the transfer of Protected Information to other authorized parties for purposes consistent with OIT’s mission and OIT’s obligations to protect the information.

Policy

It is the policy of OIT that no Protected Information be transmitted over any network outside of the secured zones within the OIT network, unless appropriate and standard encryption techniques are used. Under no circumstances will Protected Information be transmitted across an unsecured network in clear text. In particular, it should be noted that Email is not by default an encrypted means of transmission and any Email sent outside of the protected university Email system is subject to this restriction.

ISM 402: Secured Zones for Protected Systems

Section 400: Network and Telecommunications Security

Purpose

The purpose of this section is to state OIT’s procedures regarding network security and firewall architecture to protect Protected Information.

Procedure

OIT Information Technology Services establishes Secured Zones using current firewall technology and the appropriate network access control rule set to ensure that only authorized access is permitted to information systems which contain or will have access to Protected Information. The overall architecture is based on separation of servers and workstations and the creation of various security zones based on the relative sensitivity. Access to the OIT data network is controlled and restricted to authorized personnel only.

ISM 501: Risk Assessment

Section 500: Security Operations

Purpose

The purpose of this section is to articulate how OIT will conduct risk assessment by first proactive and then reactive means.

Procedure

The proactive component of risk assessment will be the actual categorization of Information Systems and specifically the identification of Protected Information Assets. As discussed in section 200 of this manual, Protected Information Assets will be those assets which the university has an obligation to protect and will be identified by the appropriate Records Custodian and will have handling instructions/baseline security measures defined. This will ensure that critical elements are identified and appropriate security measures defined to protect them.

The reactive component of risk assessment will be a periodic review of information security incidents. The Chief Information Security Officer will periodically review the tracked information security incidents and will identify problem areas to be addressed in an Annual Information Security report to the Chief Information Officer.

ISM 502: Incident Response and Escalation

Section 500: Security Operations

Purpose

The purpose of documenting this procedure in the Information Security Manual is to clarify and formalize Security Operations and Procedures in the event of Information Security incidents.

Scope

The scope of these procedures is limited to Information Security Incidents. Incidents overlapping with physical security, personnel action, or student conduct will be handled in accordance with established protocols and procedures; however, the CISO will be appraised to ensure that Information Security specific aspects of any incident are addressed.

Procedure

All suspected data breaches where Sensitive, Protected, or Personal Information is involved will be reported to the Chief Information Security Officer. If the incident is determined by the CISO to involve Protected or Personal Information, he/she will create an incident response report.

Information Security Incidents involving Personal 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 Provost, the Oregon University System Vice Chancellor for Finance and Administration, the Oregon University System Internal Audit Division, and University News and Communications Services as appropriate to deal with media implications.

Information Security Incidents involving Protected 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).

Information Security Incidents involving Sensitive Information will be logged and noted in the annual Information Security Report.

ISM 601: Physical Areas Containing Protected Information

Section 600: Physical and Environmental Security

Purpose

The purpose of this section is to outline specific physical security policies and procedures which overlap with Information Security.

Background

In general, physical security is the responsibility of Public Safety on campus. There are, however, areas where special attention is needed where Information Security can be affected. Specifically, the buildings where central servers are housed, office space where Protected Information is regularly accessed and visible to people in the immediate proximity, when electronic storage media is surplused from the university, and where Protected Information is physically transported such as when tape backups are taken off site.

Policies and Procedures

601-01 Systems Housed at OIT.

The OIT machine room where systems reside is to be considered a restricted area where only authorized personnel are allowed. Standard security measures such as audited door access codes shall be employed for physical access to the room. Given the critical nature of these systems, the facility shall also be equipped with standby emergency power (both stored and generated) and shall be monitored 7 days a week; 24 hours a day for availability.

601-02 Disposal of Surplus Property

All electronic storage media are subject to the OIT Policy on Disposal of Data Storage Equipment.

601-03 Transportation of Protected Information

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 Personal Information for more than 1000 individuals is to be transported either in paper or electronic form; sealed pouches for paper documents and lock boxes for transport of tapes/CDs are required.

ISM 602: Protecting Information Stored on Paper

Section 600: Physical and Environmental Security

Background

Paper documents that include Protected Information 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.

Procedure

University employee and supervisor responsibilities include:

Do not leave paper documents containing Protected Information or Sensitive Information unattended; protect them from the view of passers-by or office visitors.

Store paper documents containing Protected Information 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 Information 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 http://www.ous.edu/dept/recmgmt/ . Once the retention schedule has been met, shred confidential paper documents and secure such documents until shredding occurs. If using the University pulping service, ensure that the pulping bin is locked and that it is accessed only by individuals identified by Business Services as those who are responsible for picking up pulping bins and who will be attentive to the confidentiality requirements.

- Make arrangements to retrieve or secure documents containing Protected Information 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 as per OIT ISM 601-03.
- Double-check fax messages containing Sensitive Information:

  Recheck the recipient's number before you hit 'start.'

  Verify the security arrangements for a fax's receipt prior to sending.

  Verify that you are the intended recipient of faxes received on your machine.

ISM 701: Disaster Recovery

Section 700: Disaster Recovery

Purpose

The purpose of this section is to outline the Disaster Recovery Plans that are in place or in progress.

Background

Disaster Recovery is part of planning for every department at OIT. The overall campus plan envisions coordination in an Emergency, with the expectation that university departments are ensuring the survivability of their critical assets, maintain the functioning of their critical assets as long as possible, and will be able to resume their normal function after the Emergency is over and the recovery begins. For Information Security there are two critical areas where planning is required to meet these objectives: the Banner System (with critical Enterprise Information) and the campus Communications System.

701-01 Information Systems Housed at OIT.

Information Technology Services maintains a disaster plan for the systems hosted at Oregon Institute of Technology. The current copy is managed by the Manager of Technical Services at Oregon Institute of Technology and can be reviewed upon request.

701-02 Communications Systems

Computing Services is responsible for both the phone and data networks on campus and will maintain a disaster plan for those networks. Once completed, the current copy will be managed by the CIO and can be reviewed upon request.

ISM 801: Awareness and Training Action Plan

Section 800: Awareness and Training

Purpose

The purpose of this section is to identify the activities OIT is engaged in to promote Information Security awareness among members of the University Community.

Background

The first step in promoting Information Security awareness at OIT is the formation of this Information Security Program. By formalizing our policies and procedures with respect to Information Security and posting this manual on the web for employees to read, we hope to initiate the discussion of Information Security and what we all can do to better protect the information entrusted to the institution. Beyond this and related discussion events, OIT will:

- 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.

- Incorporate a statement of understanding and acceptance of policies and procedures included in this manual with every secure socket layer certificate credential issued on behalf of OIT and managed by Information Technology Services

ISM 802: Definitions

Section 800: Awareness and Training

Baselines

Baselines are mandatory descriptions of how to implement security packages to ensure a consistent level of security throughout the organization. Different systems have different methods of handling security issues. Baselines are created to inform user groups about how to set up the security for each platform so that the desired level of security is achieved consistently.

Chief Information Security Officer (CISO)

The CISO is responsible for the University's information security program and for ensuring that policies, procedures, and standards are developed, implemented and maintained.

Clear Text

Non-encrypted data

FERPA

The Family Educational Rights and Privacy Act establishes an obligation for the University to keep student records private and accessible only to those with an educational need to know, rather than information designated as directory information which is public.

Guidelines

General statements designed to achieve a policy's objectives by providing a framework within which to implement controls not covered by procedures.

HIPAA

The Health Insurance Portability and Accountability Act establishes an obligation for the University to secure and protect all Individually Identifiable Health Information which we possess.

Information Security Incidents

Information security incidents include virus infections, spam generation reports, computers that have been "hacked", sharing of Protected Information to unauthorized personnel, etc. Incidents may have Information Security, student confidentiality, and/or personnel action implications. Student confidentiality and personnel actions take precedence and should be addressed first and in the standard manner.

Information Systems

Information Systems are composed of three major components: data, applications, and infrastructure systems. All three must be addressed in order to ensure overall security of these assets.

Institutional Information

Institutional Information is all information created, collected, maintained, recorded or managed by the university, its staff, and all agents working on its behalf.

Personally Identifiable Information

In the context of this set of policies and procedures, this term will be used as defined in Oregon's 2007 SB583 the Consumer Identity Theft Protection Act:

"(11) 'Personal information':

(a) Means a consumer's first name or first initial and last name in combination with any one or more of the following data elements, when the data elements are not rendered unusable through encryption, redaction or other methods, or when the data elements are encrypted and the encryption key has also been acquired:

(A) Social Security number;

(B) Driver license number or state identification card number issued by the Department of Transportation;

(C) Passport number or other United States issued identification number; or

(D) Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to a consumer's financial account.

(b) Means any of the data elements or any combination of the data elements described in paragraph (a) of this subsection when not combined with the consumer's first name or first initial and last name and when the data elements are not rendered unusable through encryption, redaction or other methods, if the information obtained would be sufficient to permit a person to commit identity theft against the consumer whose information was compromised.

(c) Does not include information, other than a Social Security number, in a federal, state or local government record that is lawfully made available to the public."

Policy
An information security policy is a set of directives established by the University administration to create an information security program, establish its goals and measures, and target and assign responsibilities. Policies should be brief and solution-independent.

Procedures
Step by step specifics of how standards and guidelines will be implemented in an operating environment.

Protected Information
Protected Information is information protected by statutes, rules, regulations, University policies, contractual language, and/or is considered to be personally identifiable. 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.

Records Custodian
Certain Records Custodians are designated by the University President and documented in the Information Security Manual and cover financial records (Director of Business Affairs), employment records (Director of Human Resources), and student records (Registrar). These Record Custodians (or their delegates) have planning and policy-level responsibility for data within their functional areas and management responsibility for these defined segments of institutional data. For the purposes of this Information Security Policy, any university personnel collecting data not falling under these definitions will be considered the appropriate Records Custodian for that data.

Secured Zones

Segments of data networks which have network level security rules applied to restrict access to authorized personnel only. This is done typically with Firewall rules and Virtual Private Networks.

Sensitive Information

Sensitive Information is information that must be guarded due to proprietary, ethical, privacy considerations, or whose unauthorized access, modification or loss could seriously or adversely affect the University, its partners, or the public. 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.

Standards

Standards are mandatory activities, actions, rules or regulations designed to provide policies with the support structure and specific direction they require to be meaningful and effective.

University Community Members

Students, faculty, staff, volunteers, contractors, affiliates, or agents, who have access to University Information Systems and all University units and their agents including external third-party relationships. This access is granted solely to conduct University business.

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 Information or Sensitive Information, sufficient protection will be applied to prevent unauthorized modification of such information.

ISM 803: Reference Material

Section 800: Awareness and Training

803-01 ISO 27000 Series

From 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. The following series is currently planned or already published:

ISO 27001 – Specification for an information security management system (ISMS).

ISO 27002 – Potential new standard for existing ISO 17799, which is a code of practice for Information Security.

ISO 27003 – New standard for guidance on the implementation of an ISMS.

ISO 27004 – New standard for information management measurement and metrics.

ISO 27005 – New standard for information risk management.

ISO 27006 – New standard to provide guidelines for the accreditation of organizations offering ISMS certification.

803-02 Control Objectives for Information and related Technology (COBIT)

From 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.

OUS Internal Audit will be using COBIT as their auditing standard for Information Security.

803-03 OUS Information Security Policy

Formally adopted by the Board of Higher Education in June 2007, the Oregon University System Information Security Policy has been incorporated as OAR 580-055-0000 and is available at:

http://arcweb.sos.state.or.us/rules/OARS_500/OAR_580/580_055.html

This policy identifies eight areas where policies and procedures are required to be adopted by each institution in the system and contains some minimum requirements for each area. This manual is organized to address all eight areas.

803-04 Oregon's 2007 Consumer Identity Theft Protection Act

Passed by the 2007 Oregon Legislature as Senate Bill 583 and signed into law by the Governor, this law requires entities who collect "personal information" on Oregon residents to adopt administrative and technical safeguards to protect it. It also requires notification in the event of a security breach involving this information. More information can be found at:

http://www.cbs.state.or.us/dfcs/id_theft.html

ISM 804: Frequently Asked Questions

Section 800: Awareness and Training

Q. What is the purpose of this Manual?

A. The purpose of this manual is to document all of the University's Polices and Procedures around Information Security to ensure that we comply with all of the federal and state regulations that we are required to.

Q. Who is responsible for Information Security?

A. Given the nature of Information and how we all use it every day, it is everyone's responsibility to protect information that we use. Certain roles and responsibilities have been defined within this document to help give guidance on how to do that but it really must be an activity we all take seriously to be effective.

Q. What do I need to protect?

A. This manual outlines three classifications for Information Systems. Protected, Sensitive, and Unrestricted. Each class has different levels of security applied and need to be protected in different ways.

Q. How do I protect it?

A. Baseline standards for each of the classifications are defined within this document and minimum requirements are explained along with some basic rules of thumb for paper documents as well as electronic information.

Q. I am an employee of the University; how do I figure out what classification applies to information I deal with?

A. In general, if the information you deal with can be considered financial, employment, or student records, it will be considered protected and must be handled in accordance with guidelines established by the records custodian. If you collect information directly (web forms for example), the classification still applies and you will be required to determine both who the Records Custodian is and whether or not the information you collect would be considered Protected. In general, other than Student Records, Financial Information, and Personnel Records, it would be at the department's discretion as to whether or not information is to be classified as Sensitive or Unrestricted if it is not already classified as Protected by a Records Custodian.

Q. What do I do if I suspect a security breach?

A. Report it to your department head and/or the CISO who will escalate to appropriate administrative departments.

Q. How do I decide if a public notification is required by the new ID Theft law in Oregon?

A. That determination will be done by legal counsel.