Oregon Institute of Technology
Information Security Manual v2.0

Table of Contents

ISM 001: Introduction

Section 000: Introductory Material

This Information Security Manual documents key elements of the Oregon Institute of Technology's Information Security Program required by Oregon law, Oregon University System Rules, and Information Security best practices. Oregon Tech takes its responsibility to protect and care for the information entrusted to us by our students, faculty, staff, and partners seriously. Policies 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 a 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 Oregon Tech 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 apply regardless of the media on which information resides. Specifically, they apply to traditional hard copy information, as well electronic records and data. 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 section is to clearly outline the roles of President, CIO, and CISO in fulfilling Oregon Tech's responsibilities with respect to information security as directed in the Information Security Policy.

Institutional Responsibilities

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

Chief Information Officer (CIO): As directed in the 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 policy.

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

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 Oregon Tech 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

Purpose
The purpose of this section is to clarify the role of “Records Custodian” as defined in Oregon Tech practices, 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.
Director of Payroll Services – Responsible for institutional payroll and employee tax 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 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 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.

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 to ensure overall security of these assets.

Information Security Program

Oregon Tech hereby establishes an Information Security Program by adopting and documenting within this Information Security Manual, policies, security controls and standards which govern Information Systems including data, applications, and infrastructure systems according to their relative sensitivity and criticality.

The foundation of this Information Security Program will be the guidelines for disclosure established in this manual; however, for these to be effective all three aspects of information systems must be addressed including data, storage, and associated processes.

ISM 202: Information Systems – Guidelines for Disclosure

Section 200: Information Systems Security

Purpose
The purpose of this section is to provide guidance and standards regarding the categorization 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 categorization provides the basis to apply an appropriate level of security to Oregon Tech's Information Systems. It is the Records Custodian's responsibility to review Institutional Information periodically and implement or revise appropriate security requirements.

Information Classifications: Critical, Confidential, Sensitive, and Public

202-01: Critical Information

Critical Information is information for which there are legal requirements for preventing disclosure or financial penalties for disclosure. Personally identifiable information (PII) is an example of critical data. 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.

Critical Information must be protected from unauthorized access, modification, transmission, storage, or other use. Critical Information should be disclosed to individuals on a need-to-know basis with appropriate approvals 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 Critical Information is granted.

202-02: Confidential Information

Confidential Information is information for which there may be legal requirements for preventing disclosure or financial penalties for disclosure. Student records are examples of confidential data. This information is protected by statutes, rules, regulations, University policies, and/or contractual language. High to moderate levels of restriction apply, both internally and externally, due to the potential risk or harm that may result from disclosure or inappropriate use.

Confidential Information must be protected from unauthorized access, modification, transmission, storage, or other use. Confidential Information should be disclosed to individuals on a need-to-know basis with appropriate approvals 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 Confidential Information is granted.

202-03: Sensitive Information

Sensitive Information is information that would not necessarily expose the University to loss if disclosed, but should be guarded against unauthorized access or modification due to proprietary 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. This data includes employee information that has been identified as sensitive according to university policies.

202-04: Public Information

Public 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 through appropriate channels. In some cases, general-public access to public information is required by law.

While the requirements for protection of Public (unrestricted information) are considerably less than for Confidential 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, hosted University enterprise applications, on-site enterprise servers, distributed departmental servers, or personal workstations and mobile devices.

This applies regardless of the media on which data resides. 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 practices conflict with university standards, University standards apply.

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.

203-04 Remote 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 Oregon Tech ISM 601-03.

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, to constitute enough information to establish credit or perpetuate other forms of fraud associated with Identity Theft.

Scope

This policy is applicable to all Oregon Tech community members including all employees, students, contractors, consultants, agents, and vendors working on Oregon Tech's behalf. It is applicable to all Oregon Tech 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 Oregon Tech 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 Oregon Tech 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 Oregon Tech is restricted to Business Affairs for the processing of wire transfers, ACH payments and direct deposit transactions; both incoming and outgoing.
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 Oregon Tech will be reported to the Governance Team which is made up of the CIO and all data owners. All reasonable precautions will be taken to ensure the integrity and confidentiality of this information.
Health Data
Employee, Student and Vendor Tax Data

Under no circumstance shall Social Security Number, Bank Account Numbers, or Driver's license/National Identification Numbers be stored in a non-redacted form on any portable electronic media.

All VISA/Credit Card transactions necessary to conduct business with Oregon Tech are completed through vendor payment gateways. Oregon Tech does not collect or store these numbers on any form of media.

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

All members of the Oregon Tech 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.

ISM 302: User Specific Policies

Section 300: User and Personal Information Security

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

Policies

302-01 Acceptable Use Policy (AUP)
Oregon Tech maintains the Computer Use Policy]here:
https://www.oit.edu/sites/default/files/2020/documents/computing-facilities-use-oit-30-005.pdf
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
Oregon Tech 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
Oregon Tech Information Technology Services creates system accounts for general access to Oregon Tech 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 enterprise information systems in accordance with parameters set by the appropriate Records Custodian.

302-04 Acceptable Email Practices

Oregon Tech email accounts shall be considered an official means for communicating University business. The contents of all email messages are subject to laws governing public records, users should exercise prudent judgment when sending messages that may include confidential information. Use of email should adhere to rules pertaining to Health Insurance Portability and Accountability Act of 1996 (HIPAA) or the Family Educational Rights and Privacy Act (FERPA).

302-05 File Storage Practices

Oregon Tech file storage shall be used primarily for University business. The contents of all stored files are subject to laws governing public records, users should exercise prudent judgment as to what is stored that may include personal or confidential information. Use of email should adhere to rules pertaining to Health Insurance Portability and Accountability Act of 1996 (HIPAA) or the Family Educational Rights and Privacy Act (FERPA). File storage includes Office 365 tools (OneDrive, SharePoint and Teams). It also includes mapped drives to file servers such as T: or R: drives. Also, removeable drives or media and local storage on computers. Any files that are shared within or outside the University need to adhere to security policies and are the responsibility of the user sharing the file.

302-06 Personal Device Use Guidelines

The BYOD (Bring Your Own Device) guidelines apply to personal devices used on campus or devices used while working from home. All personal devices used for work purposes should follow the same guidelines as Oregon Tech owned and managed devices. Following Oregon Tech guidelines pertaining to Oregon Tech-owned devices can help protect Oregon Tech data, personal data and personal devices.

ISM 401: Network and Telecommunications Security

Section 400: Transmission of Protected Information

Purpose
The purpose of this section is to state Oregon Tech'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 Oregon Tech mission and obligations to protect the information.

Policy
It is the policy of Oregon Tech that no Protected Information be transmitted over any network outside of the secured zones within the Oregon Tech network, unless appropriate and standard encryption techniques are used. Under no circumstances will Protected Information be transmitted across an unsecured network in clear text. Email sent within the Oregon Tech network between Oregon Tech employees is by default an encrypted transmission, however the data in the sent email is also by default viewable. All Oregon Tech employees are able to encrypt email prior to the transmission both inside and outside of the Oregon Tech system. Tools will also be set up to scan emails for Protected Information to limit exposure.

ISM 402: Secured Zones for Protected Systems

Section 400: Network and Telecommunications Security

Purpose
The purpose of this section is to state Oregon Tech's policies regarding network security and firewall architecture to protect Protected Information.

Policy
Oregon Tech's Information Technology Services will design and establish security zones on the network to segregate network traffic for the purpose of isolating and controlling access to Protected Systems and Information. Firewall technology will be utilized to protect and log access attempts to Protected Systems. The appropriate network access control rule sets will ensure that only authorized access is permitted to information systems which contain or will have access to Protected Information. Access to the Oregon Tech 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 Oregon Tech will conduct risk assessment.

Policy
Oregon Tech's Information Technology Services (ITS) will initiate information-security based risk assessments, both proactive and reactive, to help manage risks to University data and systems. Proactive risk assessments will be conducted 1.annually and 2.prior to any known and planned significant changes to critical or sensitive data or systems; reactive assessments will be conducted in response to significant security incidents involving critical or sensitive systems or data. The annual IT risk assessment may either be conducted by Oregon Tech ITS personnel or by a qualified third-party vendor.

ISM 502: Incident Response and Escalation

Section 500: Security Operations

Purpose

The purpose of this section is to clarify and formalize Security Operations and policies in the event of Information Security incidents.

Scope
The scope of this policy 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 apprised to ensure that Information Security specific aspects of any incident are addressed.

Policy
Oregon Tech's Information Technology Services (ITS) will handle information security incidents in accordance with an incident response plan and associated procedures published on an internal ITS wiki support site. Procedures for the most frequent security incidents currently exist on the wiki and are accessible by ITS personnel. The incident response plan includes references to the existing procedures.

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 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, and when electronic storage media is surplused from the university.

Policies

601-01 Systems Housed at Oregon Tech

The Oregon Tech data center 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). The data center will also be equipped with environmental monitoring and fire suppression. The data center will be monitored 7 days a week; 24 hours a day for availability.

601-02 Disposal of Surplus Property

All electronic storage media slated for disposal will follow a disposal procedure based on NIST SP 800-88. This will ensure that the previous data on the storage media is properly scrubbed and unrecoverable. Depending on sensitivity of the previous data that was stored on the media, documentation of sanitation and disposal should be recorded.

601-03 Transportation of Protected Information

Physical transportation of Protected Information should be avoided, if possible. In many cases forensic images can be created and securely transmitted via encrypted transmission. Any physical transportation of Protected Information shall be done by a trusted courier who can provide 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/drives are required. In situations requiring the transport of hardware, ITS will select an outside vendor for support as necessary and require appropriate traceability from point of pick-up to destination delivery.

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.

Policy

University data owners are responsible to provide training supporting the following protocols with their data:

- Ensure paper documents containing Protected Information or Sensitive Information are not left Unattended and are kept from the view of passers-by or office visitors while in use.
- Store paper documents containing Protected Information or Sensitive Information in locked files when not in use.
- When paper documents are required, store them in fireproof file cabinets. Keep copies in an alternate and equally secure 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.
- Retrieve or secure documents containing Protected Information or Sensitive Information immediately that are printed on copy machines, fax machines, and printers.
- 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: Business Continuity

Section 700: Business Continuity

Purpose

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

Background
The overall Oregon Tech disaster recovery 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 critical Enterprise Information and Communications System.

701-01 Hosted Information Systems
Information Technology Services does not maintain any critical information systems in local server rooms. All critical data and applications are hosted. Backups of systems and data within the hosted/cloud environment shall be maintained. If possible, backups will be maintained within a separate area of the hosted/cloud environment. In regard to Business Continuity and Disaster Recovery (BC/DR), documentation from the hosted/cloud environment vendor on their BC/DR policies and procedures should be periodically reviewed.

701-02 Communications Systems
Oregon Tech's Information Technology Services will maintain a Disaster Recovery Plan (DRP) based on the overall University's Business Continuity Plan. The DRP will encompass all IT systems including hosted/cloud systems and communication systems. The DRP will be managed by the CIO and reviewed annually.

ISM 801: Awareness and Training Action Plan

Section 800: Awareness and Training

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

Background
The first step in promoting Information Security awareness at Oregon Tech is the formation of this Information Security Program. By formalizing our policies 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, Oregon Tech will:

- Integrate training for proper handling of protected information in the Acceptable Use Agreement and departmental training defined and provided by data owners and required by all employees seeking access to the enterprise information assets.
- Include information about stopping ID theft in New Employee Orientation.
- Incorporate a statement of understanding and acceptance of policies included in this manual with every secure socket layer certificate credential issued on behalf of Oregon Tech and managed by Information Technology Services

ISM 802: Definitions

Section 800: Awareness and Training

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 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 , 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 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.

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 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.

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 the University's Polices 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. – Fred to add summary steps

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.