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:

600 Physical and Environmental Security

601 Physical Areas Containing Protected Information

601-02

OREGON INSTITUTE OF TECHNOLOGY

Information Security Manual
OIT-30-007

Effective 04/05/11

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 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

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

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

OREGON INSTITUTE OF TECHNOLOGY

Information Security Manual
OIT-30-007

Effective 04/05/11

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 te and maintain an Information Security Program.

Scope

Information Systems are composed of three major components: data, applications, and infrastructure systems. All three must be ad96 Tm0 g0 G[(ORE)-2(G)rucst2150.0tŸ 1 90.024 33 0 0 1 90.02

a

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.

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.

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 9(y)10 -ac4(ti)-3(on wnr-5(e)44odume)-7(n./ a /P ¤ 144.02 554.14 Tm[( )] TJET EMC /P 2inatio

±

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 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

ISM 401: Transmission of Protected Information

Section 400: Network and Telecommunications Security

Purpose

The purpose of this section is to state OIT
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 mission and OIT

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
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

OREGON INSTITUTE OF TECHNOLOGY

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

OREGON INSTITUTE OF TECHNOLOGY

Information

OREGON INSTITUTE OF TECHNOLOGY

Information

within which to implement controls not covered by procedures.

HIPAA
The Health Insurance Portability and Accountability Act establishes an obligation for the

(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.

OREGON INSTITUTE OF TECHNOLOGY

Information Security Manual
OIT-30-007

Effective 04/05/11