

# **Western Oregon University**

## **Information Security Manual v1.0**

**Please direct comments to:  
Bill Kernan, Chief Information Security Officer**

### **Table of Contents:**

- 000 Introductory Material
    - 001 Introduction
    - 002 Definitions
    - 003 Reference Documents
  - 003-01 ISO 27000 Series
  - 003-02 Control Objectives for Information and Related Technologies (COBIT)
  - 003-03 OUS Information Security Policy
  - 003-04 Oregon's Consumer Identity Theft Protection Act
  - 004 Frequently Asked Questions
- 
- 100 Information Security Roles and Responsibilities
    - 101 Institutional Responsibilities
    - 102 University Community Responsibilities
    - 103 Records Custodians
- 
- 200 Information Systems Security
    - 201 Information Systems Security – General
    - 202 Classification Standards Information Systems
      - 202-01 Protected Information
      - 202-02 Sensitive Information
      - 202-03 Unrestricted Information
    - 203 Baseline Standards
      - 203-01 Protected
      - 203-02 Sensitive
      - 203-03 Unrestricted
      - 203-04 Mobile Computing
- 
- 300 User and Personal Information Security
    - 301 Personal Information
    - 302 User Specific Policies
- 
- 400 Security Operations

- 401 Incident Response and Escalation
- 402 Risk Assessment

- 500 Network and Telecommunications Security
  - 501 Secured Zones for Protected Systems
  - 502 Transmission of Protected Information

- 600 Physical and Environmental Security
  - 601 Physical Areas Containing Protected Information
    - 601-01 Milne Computer Center and Banner systems
    - 601-02 Disposal Procedures for Surplus Property
    - 601-03 Transportation of Protected Information Assets
  - 602 Protecting Information Stored On Paper

- 700 Disaster Recovery
  - 701 Campus DR Plan
    - 701-01 Banner DR Plan
    - 701-02 Communications Systems DR Plan

- 800 Awareness and Training

## **WOU ISM 001: Introduction**

Information Security Manual Section 000: Introductory Material Effective: 08/01/2008

The WOU Information Security Manual documents key elements of WOU'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](http://www.cbs.state.or.us/dfcs/id_theft.html)).

WOU 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 legal, moral, and intellectual responsibilities as stewards of information entrusted to us as an Institution of Higher Education.

Information Security Policies apply to all members of the WOU 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. It also applies regardless of the form the information may take, for example text, graphics, video or audio, or their presentation.

## **WOU ISM 002: Definitions**

Information Security Manual Section 000: Introductory Material Effective: 08/01/2008

### **128-Bit Encryption**

Encryption key that is 128 bits in length. This form of encryption is commonly found as the default encryption level on commercially available software.

### **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 Privacy Act establishes an obligation to the University to keep student records private and accessible only to those with an educational need to know; other 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.

### **HIPPA**

The Health Information Privacy and Portability Act establishes an obligation to 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 procedure, 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**

Records Custodians are designated by the University President. Record Custodians (or their delegates) have planning and policy-level responsibility for data within their functional areas and management responsibility for defined segments of institutional data. *From the Oregon Statute:* A public body mandated, directly or indirectly, to create, maintain, care for or control a public record. (ex. The Registrar is the records custodian of FERPA 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.

## **WOU ISM 003: Reference Material**

Information Security Manual Section 000: Introductory Material Effective: 08/01/2008

### **003-01 ISO 27000 Series**

From [www.27000.org](http://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.

### **003-02 Control Objectives for Information and related Technology (COBIT)**

From [www.isaca.org/cobit](http://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.

### **03-03 US 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](http://arcweb.sos.state.or.us/rules/OARS_500/OAR_580/580_055.html)

This policy identifies 8 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 8 areas.

#### **03-04 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](http://www.cbs.state.or.us/dfcs/id_theft.html)

## **WOU ISM 004: Frequently Asked Questions**

Information Security Manual Section 000: Introductory Material Effective: 08/01/2008

### 004 Frequently Asked Questions

What do I need to protect?

How do I protect it?

How do I figure out who the records custodian is?

What do I do if I suspect a security breach?

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

Who is responsible for information security?

# WOU ISM 101: Institutional Responsibilities

Information Security Manual Section 100: Information Security Roles and Responsibilities Effective: 08/01/2008

## **Purpose**

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

## **Intitutional 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 WOU'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.

# **WOU ISM 102: University Community Responsibilities**

Information Security Manual Section 100: Information Security Roles and Responsibilities Effective: 08/01/2008

## **Purpose**

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

## **Background**

The University is held accountable to protect certain information by federal laws (such as FERPA and HIPPA), state laws (such as the Oregon Consumer Identity Theft Protection Act of 2007), and State Board of Higher Education administrative rules. However, ready access to information is a requirement for the effective operation of the institution and 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.

## **Policy**

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. All members of the WOU 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. Protected Information will be designated by the appropriate Records Custodian(s) along with requirements for handling them and minimum safeguards.

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.

**Cross Reference**

See 002 Definitions –FERPA, HIPPA, Records Custodians, and University Community Members

See 202 Information Systems Classification Standards – Protected Information

See 203 Baseline Standards (“handling instructions” and “required minimum safeguards” as referenced above.)

## WOU ISM 103: Records Custodians

Information Security Manual Section 100: Information Security Roles and Responsibilities Effective: 08/01/2008

### **Purpose**

The purpose of this policy is to clarify the role of “records custodian” as defined in WOU policy and practice, to ensure that specific University obligations are met.

### ----- **Background Information** -----

WOU policy on Acceptable Use of University Information currently defines a specific set of Records Custodians in accordance with state law and University standard practice to ensure accountability and proper records handling.

### **Policy**

A Records Custodians is designated by the University President in order to ensure that specific institutional responsibilities are met. Record Custodians (or their delegates) have planning and policy-level responsibility for Information Systems within their functional areas and management responsibility for defined segments of Institutional Information. Record Custodians are documented in the [Acceptable Use of University Information policy](#).

Responsibilities include:

1. Develop, implement, and manage information access policies and procedures.
  2. Assign information classifications based on a determination of the level of sensitivity of the information, considering the level of security required for protecting the information from unauthorized access; and the level of security required for protecting the information from unauthorized creation, deletion, or modification collectively termed “modification” for purposes of this policy.
  3. Ensure that data quality and data definition standards are developed and implemented.
  4. Ensure compliance with federal, state, and University policies and regulations regarding the release of, responsible use of, and access to Institutional Information.
  5. Resolve stewardship issues and data definitions of data elements that cross multiple functional units.
  6. Promote appropriate data use and data quality, including providing communication and education to data users on appropriate use and protection of Institutional Information.
  7. Develop and implement record and data retention requirements in conjunction with University Archives.

Cross Reference

## **WOU ISM 201: Information Systems Security - General**

Information Security Manual Section 200: Information Systems Security Effective:  
08/01/2008

### **Purpose**

The Purpose of this section is to define in general terms what is meant by Information Systems Security.

### **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.

### **Policy**

WOU will establish policy, procedures, security controls, and standards which govern Information Systems including data, applications, and infrastructure systems as those assets are classified according to the OUS Information Security Policy. These policies 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 them to be effective all three aspects of information systems must be addressed. This is not just about data, it is also about how data is stored and processed.

### **Cross Reference**

See 003-01 ISO 27000 Series

See 003-02 Control Objectives for Information and related Technology (COBIT)

See 003-03 OUS Information Security Policy

# **WOU ISM 202: Information Systems – Classification Standards**

Information Security Manual Section 200: Information Systems Security Effective: 08/01/2008

## **Purpose**

The purpose of this policy is to provide guidance and policy standards regarding the classification of Information Systems to ensure the protection of WOU's Information Systems from accidental or intentional unauthorized access, damage, alteration or disclosure while preserving authorized users' ability to access and use Institutional Information. Information classification standards provide a basis for understanding and managing Institutional Information based on the level of confidentiality and criticality of the information. Accurate classification provides the basis to apply an appropriate level of security to WOU's Information Systems.

## **Scope**

This policy 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 policy 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.

## **Policy**

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.

University Records Custodians will classify all information systems under their functional area of responsibility commensurate with the relative sensitivity of the information and any specific obligation the University has to protect the information. Three categories have been identified below and Records Custodians are responsible for reviewing these classifications as systems, processes, and data sets are added, removed, or as regulations change. Individuals who handle Institutional Information in any form are responsible for understanding the classification of the Information they deal with and for ensuring University policy regarding the security of that Information is followed.

### **Information Classifications**

Electronic and physical information is classified into various levels of sensitivity and risk. Records Custodians are responsible for periodically classifying information into one of three levels of sensitivity and risk: Protected, Sensitive, Unrestricted. These classifications take into account the legal protections, contractual agreements, strategic or proprietary worth, ethical and privacy considerations, and possible harm to or loss of reputation of an individual or the institution.

#### **202-01: 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.

Protected Information must be protected from unauthorized access, modification, transmission, storage or other use.

Protected Information may 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 Records Custodian.

Access to Protected Information must be authorized by the Records Custodian responsible for the information. Only those University employees designated with approved access and who have signed non-disclosure agreements will be provided access to Protected Information.

Examples: FERPA – protected student information  
Employee data and certain personnel documents/records  
Prospective student data  
Credit card numbers  
Purchasing card numbers

Human subject information  
Lab animal care information  
HIPAA – protected health information

### **202-02: 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.

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 must be authorized by the appropriate department or unit head.

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

### **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.

Examples: Publicly posted press releases  
High-level enrollment statistics  
Course catalog  
Financial statements

# **WOU ISM 202: Information Systems – Baseline Standards of Care**

Information Security Manual Section 200: Information Systems Security Effective: 08/01/2008

## **Purpose**

The purpose of this section is to define the baseline standards of care based on the general information classification.

## **Policy**

The following standards are a minimum for people and machines that have access to and/or process information that has been classified by the appropriate Records Custodians. 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.

### **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 antivirus 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 will be instructed on the proper use and handling of this information as defined by the Records Custodian and will be subject to WOU Policies regarding security sensitive personnel. Under no circumstances shall Protected Information be disclosed to anybody without authorization from the appropriate Records Custodian.

### **203-02 Baseline Standards for Sensitive Information**

All computer systems which store or process Sensitive Information shall have restricted access granted only to authorized personnel affiliated with WOU, 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 University Computing Services' [network security policy](#).

All personnel granted access to sensitive information shall not disclose this information to parties outside of WOU without appropriate authorization by university legal counsel, appropriate Records Custodian, or by the appropriate WOU Department Head if no specific Record Custodian has been designated by the President.

### **203-03 Baseline Standards for Unrestricted Information**

All computer systems which store or process Unrestricted Information shall 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 to University Computing Services' [network security policy](#) 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 128bit 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 can not 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 WOU ISM 601-03.

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

# WOU ISM 301: Personal Information Privacy

Information Security Manual Section 300: User and Personal Information Security  
Effective: 08/01/2008

## Purpose

WOU has a responsibility to all members of the WOU community and all people who entrust personal information to WOU, to protect that information from potential misuse. The purpose of this policy is to establish clear guidelines for handling specific data elements which pose a special and specific risk to Western Oregon University, or our community members, should those data elements be compromised through unauthorized access due to a breach of security.

## Scope

This policy is applicable to all WOU community members including all employees, students, contractors, consultants, agents, and vendors working on WOU's behalf. It is applicable to *all* WOU 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 Western Oregon University 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 Western Oregon University 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 at Western Oregon University of bank account numbers is restricted to the following uses:

### Business Affairs

- Processing direct deposit transactions; both incoming and outgoing
- Processing wire transfers

### Department Personnel

- Processing wire transfers – Paper copies of this data may be stored during the processing phase. They should be kept in a physically secure location with limited personnel access. Departments are prohibited from storing electronic copies of this data. Once verification of transfer is complete the paper copy should be redacted or destroyed through approved WOU 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 Western Oregon University 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 WOU 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 employee's required to handle this information and that reasonable controls and precautions to protect these elements are in place.

## **WOU ISM 302: User Specific Policies**

Information Security Manual Section 300: User and Personal Information Security  
Effective: 08/01/2008

### **Purpose**

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

### **Policies and Procedures**

#### **302-01 Acceptable Use Policy (AUP)**

WOU maintains and the Acceptable Use of University Computing Resources as part of the General Policies of the institution with the official and current copy residing at <http://www2.wou.edu:7777/pls/wou2/policy.woupolicy.main> . As stated in the AUP, it applies to "all users of university computing resources, whether affiliated with the University or not, and to all use of those resources, whether on campus or from remote locations. Additional policies may apply to computing resources provided or operated by individual units of the University or to uses within specific units." 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**

WOU 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**

WOU creates system accounts, referred to as WOU Network login, for general access to WOU centralized 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 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.

# WOU ISM 401: Incident Response and Escalation

Information Security Manual Section 400: Security Operations Effective: 08/01/2008

## **Purpose**

The purpose of this section of 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 and where physical security overlaps the appropriate coordination with Public Safety is assumed and will be conducted in accordance with Public Safety established protocols and procedures. Where Information Security overlaps with personnel action or student confidentiality, the appropriate coordination with Human Resources, The Registrar's Office, and Student Affairs is assumed and will be conducted with established protocols and procedures.

These procedures do apply to all Information Security incidents which involve Institutional Information classified as Protected Information and may be used for incidents involving Institutional Information classified as Sensitive Information depending on the nature of the incident and the asset involved.

## **Procedure**

In compliance with RFC2142, WOU does and shall maintain an appropriate email alias for the reporting of various activity originating from hosts on WOU's network. The [abuse@wou.edu](mailto:abuse@wou.edu) alias in particular is widely accepted across the internet and specifically identified by WOU in our network registration as the appropriate alias to notify when a breach is suspected. Network Engineering will maintain this email alias; respond to and track all reports and incidents; and will ask that responsible parties verify whether or not Personal Information, Protected Information, or Sensitive Information was involved.

In the case where Personal Information or Protected Information is involved, these incidents will be initially escalated to the Chief Information Security Officer or the appropriate Records Custodian who will initiate an incident response report in concert with the CISO. 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 University Provost, the Executive Vice President for Finance and Administration, and Public Relations as appropriate to deal with media implications. Incidents involving Protected Information will be reviewed by the appropriate Records Custodian(s) along with a copy of the report to be shared as deemed appropriate by the Records Custodian(s).

As stated in the scope statement, 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.

## **WOU ISM 402: Risk Assessment**

Information Security Manual Section 400: Security Operations Effective: 08/01/2008

### **Purpose**

The purpose of this section is to articulate how WOU will conduct risk assessment in 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.

## **WOU ISM 501: Secured Zones for Protected Systems**

Information Security Manual Section 500: Network and Telecommunications Security  
Effective: 08/01/2008

### **Purpose**

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

### **Procedure**

WOU Network 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. Departmental zones are established for local services and authority to manage the rules set for those zones is delegated to authorized departmental personnel. Network Services monitors and audits all rule sets.

Access to the WOU data network is controlled and restricted to authorized personnel only by means of WOU user account credentials and a registration process for computers. This includes remote trusted zone for Virtual Private Network connections from individual machines and satellite trusted networks. All machines connected to the WOU network are subject to the [WOU Network Security Policy](#)

## **WOU ISM 502: Transmission of Protected Information**

Information Security Manual Section 500: Network and Telecommunications Security  
Effective: 08/01/2008

### **Purpose**

The purpose of this section is to clearly state WOU'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 WOU's mission and WOU's obligations to protect the information.

### **Policy**

It is the policy of WOU that no Protected Information be transmitted over any network outside of the secured zones within the WOU 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.

# WOU ISM 601: Physical Areas Containing Protected Information

Information Security Manual Section 600: Physical and Environmental Security  
Effective: 08/01/2008

## 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 is, 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 surplus from the university, and where Protected Information is physically transported such as when tape backups are taken off site.

## Policies and Procedures

### 601-01 UCS Server Farm and Banner Systems

The machine room located in ITC006 is to be considered a restricted area where authorized personnel only are allowed. Standard security measures such as name badges and audited door access codes shall be employed for physical access to the room. Given the critical nature of the systems, the facility shall also be equipped with standby emergency power (both stored and generated) and shall be monitored 7x24 for availability.

### 601-02 Disposal of Surplus Property

All electronic storage media are subject to the WOU Policy on [Disposal of Data Storage Equipment](#) maintained by WOU Business Services. This policy states that information shall be purged from all electronic media prior to surplus.

### 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.

## **WOU ISM 602: Protecting Information Stored on Paper**

Information Security Manual Section 600: Physical and Environmental Security  
Effective: 08/01/2008

### **Background**

Paper documents that include Protected Information or Sensitive Information like social security numbers; student education records; an individual's medical, 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://retentionLink> . 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.

Make arrangements to immediately retrieve or secure sensitive documents that are printed on copy machines, fax machines, and printers.

Double-check fax messages containing confidential 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.

# **WOU ISM 701: Disaster Recovery**

Information Security Manual Section 700: Disaster Recovery Effective: 08/01/2008

## **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 WOU. 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 Enterprise Computing**

Enterprise Computing maintains a disaster plan for the Banner systems. The current copy is managed by the Director of Enterprise Computing and can be reviewed upon request.

### **701-02 Communications Systems**

University Computing Services is responsible for both the phone and data networks on campus and maintains a disaster plan for those networks. The current copy is managed by the Director of University Computing Services and can be reviewed upon request.

## **WOU ISM 801: Awareness and Training**

Information Security Manual Section 800: Awareness and Training Effective:  
08/01/2008

### **Purpose**

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

### **Background**

The first step in promoting Information Security awareness at WOU 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, WOU 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 WOU and managed by University Computing Services.