



Portland State  
UNIVERSITY

# Information Security Policy

# PSU Information Security Policy

## Table of Contents

1.0	Introduction and Purpose.....	3
2.0	Authority and Scope.....	3
2.1	Authority .....	3
2.2	Scope .....	3
3.0	Roles and Responsibilities .....	3
3.1	PSU President .....	3
3.2	Chief Information Officer (CIO).....	3
3.3	Chief Information Security Officer (CISO).....	4
3.4	Information Asset Managers .....	4
3.5	Technology Administrators .....	4
3.6	Network or System Administrators .....	5
3.7	OIT Management .....	5
3.8	Data Owners .....	5
3.9	Data Related Roles and Responsibilities .....	5
3.10	All Users .....	5
4.0	Policies.....	5
4.1	User Accounts .....	5
4.2	Risk Analysis .....	6
4.3	Personnel Security .....	6
4.4	Physical Security .....	8
4.5	Data Security .....	10
4.6	Network and Telecommunications Security .....	13
4.7	Acceptable Use .....	15
4.8	Server and Unix System Administration .....	15
4.9	Windows Workstation Administration .....	16
4.10	Remote Access .....	17
4.11	Authentication Credentials .....	17
4.12	Application Security .....	17
4.13	Security Operations.....	19
4.14	Security Awareness, Training, and Education .....	20
4.15	Disaster Recovery/Business Continuity .....	21
4.16	Law and regulatory compliance.....	22
5.0	Exceptions.....	22
6.0	Enforcement .....	22
6.1	Organizations.....	22
6.2	Faculty/Staff .....	23
6.3	Students.....	23
6.4	Non-PSU.....	23
7.0	Related Policies/Procedures.....	23
8.0	Policy Update Requirements .....	23
	Appendix A – Definitions.....	24
	Appendix B – Relevant legislation, regulation, and industry standard .....	27

# 1.0 Introduction and Purpose

Portland State University (PSU) has a responsibility to protect information entrusted to it, ensure the effective operation of business critical processes, and must abide by the security policies established by Oregon University System (OUS) and the State Board of Higher Education as well as laws and regulations at the federal, state, and local level relating to information security. PSU must meet a standard of due care regarding the protection of institutional information assets as well as those belonging to users of PSU information assets.

The purpose of this policy is to document PSU management's intent regarding the protection of these Information Assets. It is to be used by PSU management to develop, document, implement, and maintain local information security policy and programs.

No part of this policy is meant to conflict with existing federal, state, local laws or regulations, or OUS policy. In the event of a conflict, the existing law and higher-level policy will take precedence.

## 2.0 Authority and Scope

### 2.1 Authority

This policy applies to Portland State University as organized and empowered by ORS Chapters 351 and 352, and is specifically authorized under ORS 351.087. This PSU policy is specifically required for compliance with the OUS Information Security Policy (OAR 580-055-0000).

### 2.2 Scope

- 2.2.1 This policy is applicable to all PSU colleges, schools, organizations, and departments as well as all users of PSU information assets and users working on the behalf or at the behest of PSU.
- 2.2.2 It is applicable to all OUS and PSU Information Assets, regardless of form or media. It applies to information gathering, protection, development, use, processing, storage, communications, destruction and transit.
- 2.2.3 PSU, college, school, program, organizational, and departmental policies, procedures, standards, and work instructions are required to comply with this policy, with Federal, State, Local laws, as well as with other PSU, OUS, and Oregon State Board of Higher Education policies
- 2.2.4 In general, policies should be made readily available to all interested parties

## 3.0 Roles and Responsibilities

All university community members have a responsibility to help ensure security of PSU's information assets. The following specific roles and responsibilities have been individually identified.

### 3.1 PSU President

The PSU President is responsible for establishing the information security program and ensuring that it is effective. The President shall have overall oversight responsibility for institutional provisions set forth in this policy.

### 3.2 Chief Information Officer (CIO)

The PSU Chief Information Officer (CIO), or equivalent, shall be responsible for ensuring that institutional policies are developed and enforced in accordance with this policy. The CIO will assign

CISO duties to a qualified (as defined by industry and University expectations) individual.

### 3.3 Chief Information Security Officer (CISO)

Under the direction of the CIO, the Chief Information Security Officer (CISO) shall be responsible for PSU's security program and for ensuring that institutional policies, procedures, and standards are developed, implemented, maintained, and monitored for compliance.

- 3.3.1 Develop, refine, champion and enforce PSU information security policies
- 3.3.2 Provide security expertise to staff, faculty, student groups, etc.
- 3.3.3 Promote awareness of Information Security issues in the PSU community
- 3.3.4 Develop a security education, training and awareness program
- 3.3.5 Act as a contact point for PSU information security issues
- 3.3.6 Coordinate PSU information security investigations
- 3.3.7 Ensure accountability for compliance with institution level infosec policy.

### 3.4 Information Asset Managers

- 3.4.1 Organizations which manage all or portions of their own PSU information assets (called information asset managers) shall appoint qualified information technology staff to provide liaison between their users and the PSU Office of Information Technology (OIT) and to ensure compliance with PSU information security policies.
- 3.4.2 These organizations shall articulate the rights, responsibilities, and roles of anyone interacting with PSU information assets.
- 3.4.3 Information asset managers must complete a physical inventory of information assets and maintain them in accordance with section 55.100 of the OUS Fiscal Policy Manual.
- 3.4.4 Organizations which manage all or a portion of their PSU information assets will ensure that their users are made aware of their roles and responsibilities within the organization as they relate to the security of Information Systems. Users will also be informed of all policies and procedures, which may apply to them. Contact information for central IT Security personnel, as well as department IT personnel, will be made available. Users will be informed whom to contact, and appropriate measures to take in the event of a security incident. Organization policies and procedures will be made readily available in accessible locations.
- 3.4.5 Educational or training materials will be made available in order to educate users on standard security practices. Training on basic computer security concepts will be provided. These concepts include the following: operating system patching, built-in firewalls, anti-virus software, password management, and browser and e-mail security. Additional training will be offered in areas that are of particular concern to PSU OIT and each organization.

### 3.5 Technology Administrators

Organizations which manage all or portions of their own PSU information assets shall appoint qualified information technology staff to provide liaison between their users and the PSU Office of Information Technology (OIT) and to ensure compliance with PSU information security policies. These organizations shall articulate the rights, responsibilities, and roles of anyone interacting with their PSU information assets. These technology administrators will participate in the Technology Administrators Group as their organization's representative. Technical Administrators are security sensitive personnel.

### 3.5.1 Technology Administrators Group, Chair

The OIT CTO or CIO designee will organize and conduct monthly (at the least) meetings with the Technology Administrators Group.

### 3.6 Network or System Administrators

These technical staff who are responsible for the administration of networking or computing platforms. Network and System administrators are responsible for ensuring that platform security baselines, which meet the security requirements of PSU, are developed, adhered to, and maintained.

### 3.7 OIT Management

Directors, managers, and supervisors charged with establishing, developing, operating, and maintaining the PSU information technology infrastructure. OIT management is also charged with the responsibility to develop and enforce security standards for all IT systems used by or for PSU students, faculty, and staff.

### 3.8 Data Owners

#### 3.8.1 Responsibilities

3.8.1.1 Identify the significant electronic information resources under their control

3.8.1.2 Identify the custodian of any significant data sets under their control

3.8.1.3 Ensure that requisite security measures are implemented for information resources

### 3.9 Data Related Roles and Responsibilities

OIT will develop specific policy related to roles, which document important relationships to data (e.g. Data owner, Data Custodian, Data Provider, etc.) The policy will include accountability of the individual, accountability of the information assets, identification of stakeholders, responsibility for the security of the information, responsibility for compliance with law, internal, and external requirements.

### 3.10 All Users

3.10.1 Become knowledgeable about relevant security requirements and guidelines.

3.10.2 Protect the resources under their control, such as access passwords, computers, media they create, reports they generate, and data they download.

3.10.3 Be aware that they are responsible for all actions performed by their User IDs.

## 4.0 Policies

### 4.1 User Accounts

#### 4.1.1 Account management Polices.

PSU organizations, which manage information assets, are required to develop policies, which ensure appropriate management of user accounts. These polices shall:

- a) Establish and maintain accountability;
- b) Ensure timely notification of access changes and terminations;
- c) Ensure timely response to these notifications; and

- d) Ensure that access is granted in accordance with the least privilege principle.
  - e) Ensure that positions and user responsibilities are assessed, by those creating or assigning positions or responsibilities and by business or function owners, to determine appropriate levels of rights and privileges.
  - f) Ensure that individuals are assigned levels of rights and privileges that are appropriate to their position or their responsibilities.
  - g) Ensure that business or function owners identify separation of duty requirement.
  - h) Periodic reconciliation, No Less Than (NLT) annually, of accounts to active users, privileges, and separation of duty requirements. This includes all users (including but not limited to students, employees, contractors, vendors) of PSU information assets.
- 4.1.2 All PSU accounts must be accountable to an individual (e.g. no shared or generic accounts).
  - 4.1.3 Individuals will be held accountable for all actions performed using their account.
  - 4.1.4 All non-PSU student, Faculty, and staff requiring access to PSU information assets must have an active PSU Sponsor. These accounts must include an accurate expiration date, no greater than 6 months from the date the access is granted.
  - 4.1.5 To the greatest extent possible, accounts associated with applications should be service accounts (accounts that do not permit individuals to login).
  - 4.1.6 OIT shall develop an account management policy to implement the processes necessary to meet this policy.

#### 4.2 *Risk Analysis*

Each organization managing PSU information assets must establish an ongoing risk assessment program. This program should identify and track all Essential and/or Highly Sensitive Information Assets, and verify no less than annually that all essential and highly sensitive information assets have been identified and the relevant security baselines are in place and being followed with respect to those Information Assets.

#### 4.3 *Personnel Security*

- 4.3.1 Everyone interacting with information assets has a responsibility to ensure the security of those assets.
- 4.3.2 Personal Information Policies
  - 4.3.2.1 Organizations which manage PSU information assets are required to specifically define procedures for handling and protecting personally identifiable information. The CISO shall work with PSU General Counsel, HR, FADM, contract officers, and other major stakeholders to develop implementing policy which describes the information to be protected in order to comply with contracts, legislative rules, OUS and PSU policy, and current law, including but not limited to FERPA, HIPAA, GLBA, FACTA and the Oregon Identity Theft Prevention Act.
    - 4.3.2.1.1 The PSU ID number is to be used in place of a social security number (SSN) as the university's primary identifier. Information Asset managers that believe, about any system for which they are accountable, that their

- 4.3.2.1.1 system must include the SSN, or that they need access to SSNs must contact the PSU CIO for review and approval.
- 4.3.2.1.2 Organizations that use the SSN must develop, implement and maintain reasonable safeguards, which meet PSU security standards to protect the security and confidentiality of the information.
- 4.3.2.1.3 These safeguards must include the proper disposal of this information and media containing this information.
- 4.3.2.1.4 Organizations that maintain SSN must ensure that processes and systems comply with prohibitions regarding printing, posting, or displaying SSNs.
- 4.3.2.2 Any loss or suspected loss of personally identifiable information must be reported to the PSU CISO. The CISO will document the incident. The CISO and the General Counsel with the consultation of the CIO and other major stakeholders will determine whether the incident is reportable under law and if so, take required actions.
- 4.3.2.3 Credit and debit card numbers will not be collected, stored, or transmitted by any electronic or paper systems. Contracts or applications, which provide credit and debit card services, must be reviewed to ensure PSU's PCI compliance is not compromised. Only PCI compliant offerings, peripherals, and applications documented in an industry-vetted list of applications that follow credit card application best practices may be considered for use supporting PSU.

#### 4.3.3 Acceptable Use Policies.

PSU has established an Acceptable Use Policy (AUP). All organizations and users of PSU information assets are required to accept and comply with the official PSU AUP. At a minimum, the AUP will provide examples of acceptable and unacceptable use. These examples must be drawn from this and other existing policy. The AUP is not intended to state new policy, only to re-state policy in example form.

Organizations that wish to extend the AUP must ensure that conflicts are not introduced. Organizational AUPs may be more stringent but not less stringent than the PSU AUP or other PSU policy. AUPs must include definitions of enforcement mechanisms in case of violation. They must also make it clear that prior notification is not a requirement for applicability of the policy.

#### 4.3.4 Personnel Practices

- 4.3.4.1 HR, OIT, and other managers of information assets should define acceptable levels of employee performance and experience consistent with the security requirements of the planned work assignment.
- 4.3.4.2 The PSU CISO shall develop a PSU Code of Confidentiality, which describes the permitted, and the disallowed activities related to monitoring; in order to enable operations and security while limiting the exposure of sensitive or privacy protected information.
- 4.3.4.3 A successful criminal background check will be a prerequisite for any prospective employee, contractor or vendor who will be working with critical or sensitive data.
- 4.3.4.4 All new users should complete information security awareness training prior to receiving an account.

- 4.3.4.5 All non-PSU students or non-employees requiring access to PSU information assets must have an active PSU sponsor and an account expiration date no more than 6 months from the current date.
- 4.3.4.6 Upon any personnel action (transfer, promotion, etc.), access privileges will be reviewed by both the new and previous supervisors, as well as function owners (e.g. Banner module coordinators) and adjusted as appropriate.
- 4.3.4.7 OIT will be notified of every employee termination prior to the effective date or immediately in the case of a hostile termination, so that access may be terminated as appropriate.
- 4.3.4.8 Accounts must be reconciled by the organization managing each information asset no less than annually to ensure that every account is accountable to an authorized current user. Essential and/or Highly Sensitive information assets should be reconciled more frequently but no less than annually (e.g. FIS access is required to be reviewed every 90 days).
- 4.3.4.9 Access privileges granted to users will be reconciled for conflict of interest or fraud potential (e.g., internal control standards) by managers, sponsors, and function owners (e.g. Banner module coordinators) no less than annually.
- 4.3.4.10 Access privileges assigned to roles will be reconciled for conflicts of interest and fraud potential (e.g., internal control standards) by the role owner no less than annually.
- 4.3.4.11 The PSU CISO shall develop a process for requesting and granting access to user's files. The process shall guard against the potential for abuse or retribution during complaints between two individuals (e.g. subordinate-superior relationships) or legal proceedings (e.g. lawsuits) by coordinating with HR for staff and non-faculty union cases, FADM for contractor/vendor cases, and the Provost's office for faculty and faculty union cases. To ensure consistency, the CISO or the CISO designee should coordinate all requests and direct all activities to service these requests. Questions of law should be referred to General Counsel for resolution before honoring the requests.
- 4.3.4.12 Security Sensitive Personnel are employees that have access to essential or highly sensitive data and processes should be designated as serving in critical or security-sensitive capacities as per OAR 580-023-0005 and be subject to the appropriate employment policies (e.g. background checks) of the institution.

#### 4.4 *Physical Security*

##### 4.4.1 Physical Access Control

- 4.4.1.1 Managers of information assets must identify areas for housing essential or highly sensitive information assets and designate specific personnel who require access to these areas.
- 4.4.1.2 Managers and sponsors shall arrange for identification of temporary employees and visitors who access secure areas, (e.g., through introductions to regular staff).
- 4.4.1.3 All personnel are responsible for ensuring that unauthorized individuals are not permitted access to restricted areas (e.g. no tailgating). In

- restricted areas, all personnel are required to display badges in a manner that is easily observed by all.
- 4.4.1.4 Change lock combinations used for access control on a regular basis, as determined by the sensitivity or criticality of the asset being protected. In any event, no less often than once a year. An inventory of combination locks and the dates of combination changes will be sent to Facilities by combination lock users no less than annually.
  - 4.4.1.5 Establish a system to ensure identification of the individuals having possession of keys, access cards, and badges at any given time. Organizations issuing identification badges, accounts, or which need to establish identity before acting on a request must comply with Oregon Administrative Rules governing the rigor required for proving identity.
  - 4.4.1.6 Areas housing essential or highly sensitive information assets shall be protected using accountable access control.
  - 4.4.1.7 Managers should perform unscheduled assessments of physical access control procedures.
  - 4.4.1.8 Upon notification from HR, managers must limit a terminated employee's position related physical and system access according to the notification instructions.
  - 4.4.1.9 Managers must provide for prompt reporting of any actual or suspected hostile act to the appropriate security or law enforcement agency.
  - 4.4.1.10 All server systems containing essential or highly sensitive information assets must be located inside secure and accountable areas.
  - 4.4.1.11 All physical areas containing information assets will meet or exceed PSU standards for fire, water, electric power faults, physical damage, environmental, and theft protection.
  - 4.4.1.12 A unique PSU manager (building owner, room owner, or building liaison) shall be accountable for each physical access control area, for the purpose of granting, revoking, enforcing, and reconciling access to that area.
  - 4.4.1.13 The manager of PSU-wide physical access control systems will ensure that Managers, who are responsible for granting physical access, perform reconciliation no less than annually, for locations or areas for which they authorize access.
  - 4.4.1.14 Managers shall reconcile physical access lists to authorized individuals no less than annually.
  - 4.4.1.15 Individuals operating physical security access control and video monitoring systems shall be required to agree to the PSU Code of Confidentiality.
  - 4.4.1.16 Video Surveillance and access control information is confidential. Therefore, access to and storage of that information should be tightly controlled. Requests to review video surveillance and access control information should require an incident report. Only the investigator should actually see the data, to preserve separation of duty and to limit the potential exposure of potential sensitive information. This also ensures that witnesses of video surveillance data are trained investigators. Due care should be used when determining when to honor a request for investigators to view surveillance videos or access

control records to ensure no conflict of interest exists and to ensure the request is appropriate. Questions of law should be referred to General Counsel for resolution before honoring the requests.

4.4.1.17 Individuals who can alter or monitor access control (physical or logical) systems or video surveillance are considered Security Sensitive Personnel.

4.4.1.18 Video cameras operated for surveillance or monitoring must be managed by the PSU CPSO to ensure compliance with law (e.g., laws regarding the placement of permanent and temporary video cameras, prohibitions against collecting audio, etc.).

#### 4.4.2 Mobile Computing

4.4.2.1 Prior to being assigned a PSU laptop or PDA, employees must complete and sign an Equipment Loan Agreement (from the Business Affairs Office/Property Control).

4.4.2.2 Ensure that the use of laptops and mobile computing devices such as USB memory sticks and personal digital assistants (PDA) are in compliance with PSU Mobile Computing Standards. Appropriate encryption solutions will be provided to prevent the compromise of both transmitted and stored data.

4.4.2.3 Mobile computing devices should not be left unattended except in a secure area.

4.4.2.4 Mobile devices (e.g., PDAs, USB memory sticks, laptops) without encryption should not be used for storing or transmitting essential and/or highly sensitive information.

### 4.5 Data Security

#### 4.5.1 Information Asset Classification

4.5.1.1 Managers of information assets are responsible for classifying these assets to ensure that they are adequately protected. Every type of information asset must be identified by a designated Accountable Authority (chosen from the set of primary stakeholders of the information asset) into one or more classifications. The Designated Accountable Authority must be designated by a management representative sufficiently high enough to encompass all stakeholders.

4.5.1.2 OIT is responsible for developing an information asset classification standard, which will specify minimum controls for fundamental classifications roles and responsibilities related to information asset classification, and minimum requirements for other information asset classification standards and policies.

##### 4.5.1.2.1 Fundamental Classifications

**Unclassified** – Information that may be seen by anyone. Only default security measures apply or security measures taken by the possessor or owner.

**Public** - May be seen by anyone, but requires protection against unauthorized modification. This would include information such as class schedules or material appropriate for publishing on a publicly accessible website.

**Essential** – Information Assets that are critical to the function of PSU and without which normal business functions of PSU cannot occur. These information assets would be a subset of PSU or department production information assets

**Sensitive** - Only authorized individuals may see or modify this information. Requires customized access control procedures. Improper disclosure may result in harm to the organization or to individuals. This would include most personal information such as addresses and phone numbers.

**Highly Sensitive** – Information Assets that are owned by PSU, information that PSU is obligated to keep secure by applicable law or by contract, and information exempt from disclosure under public records laws. PSU Information assets are found in written, spoken, electronic, printed, magnetic, optical and other mediums. This would include information such as but not limited to access credentials (passwords), Social Security Numbers, student financial information, video surveillance, audit trail logs for Sensitive, Essential or above systems, and credit card information.

**Audit Trail logs** - Audit trail logs should be considered at least as sensitive as the data whose activity it records. Audit trails containing access control and authentication data should be considered the highest classification of any data on a system.

4.5.1.3 Managers of information assets are responsible for the creation of classifications and related standards and policies governing the safe use and handling of their assets in accordance with relevant law including but not limited to the following:

**Digital Millennium Copyright Act (DMCA)**

**Family Educational Rights and Privacy Act (FERPA)**

**Health Insurance Portability and Accountability Act (HIPAA)**

**Payment Card Industry-Data Security Standard (PCI –DSS)**

**Personally Identifiable Information (PII) related to the Oregon ID Theft Protection Act and others**

**e-Discovery related to the 2006 US Supreme Court amendment to the Federal Rules of Civil Procedure and Oregon Department of Justice guidance regarding e-Discovery.**

**Attorney-Client privileged**

These standards and policies are subject to review and approval by the PSU CISO to ensure appropriateness of the security choices and compatibility with enterprise security and systems.

4.5.2 Care of Data

- 4.5.2.1 An accountable authority must be responsible for each sensitive or confidential type of information asset.
  - 4.5.2.1.1 All data should be protected from unauthorized modification.
  - 4.5.2.1.2 All data should be transferred using a secure transport.
- 4.5.2.2 Essential or Highly sensitive data must be protected from unauthorized modification.
- 4.5.2.3 Essential or Highly sensitive data must be transferred using a secure transport.
- 4.5.2.4 Essential or Highly sensitive data must be protected from unauthorized access or disclosure.
- 4.5.2.5 Essential or Highly sensitive data should be stored in a manner that meets standards of due care for Essential or Highly sensitive data.
- 4.5.2.6 Users extracting essential or highly sensitive data from protected systems (e.g. Banner) must be informed of their obligations to protect that data to the same degree as the protected system, as required by law and PSU/OUS policies.
- 4.5.2.7 All encrypted PSU information or encrypted information stored or transmitted on behalf of PSU must include a PSU escrow key (or equivalent), where technically possible.
- 4.5.2.8 OIT will develop a PSU Encryption policy to implement the encryption infrastructure necessary to comply with this policy.
- 4.5.2.9 All losses of highly sensitive information and PII must be reported to the CISO. Loss reports should include a description of the information lost, how the loss occurred, estimated value of the loss, and remediation measures taken. CISO will establish procedures to ensure that CPSO, General Counsel, and the accountable information asset manager are informed and will assist in determining whether these losses are reportable under relevant law.
- 4.5.2.10 All managers of information assets must develop procedures in accordance with (IAW) 580-040-0311, "Disposal of Computer and Other Electronic Storage Devices and Media" to ensure that systems transferred, submitted for disposal, or released for donation are erased to meet the NIST standards for effectively removing data on storage media. OIT and Facilities provide a common mechanism and process which managers of information assets may use to meet this requirement.
- 4.5.2.11 OIT will develop standards, capabilities or contractors for the destruction of paper and other media to an acceptable degree as determined by the sensitivity of the content.
- 4.5.2.12 Information collected in response to DMCA violation related requests/subpoenas for information must be collected in a timely manner and preserved as evidence to meet DMCA and the US Supreme Court rules of e-discovery.
- 4.5.2.13 The US Supreme Court rules of e-discovery require OIT and relevant departments to develop and execute an evidence preservation plan any time there is a perceived or actual potential for a civil suit.

## 4.6 Network and Telecommunications Security

### 4.6.1 Network and Telecommunications Management

- 4.6.1.1 All telecommunications equipment and information systems are subject to disconnection or quarantine when they pose a threat to the security or integrity of the PSU network.
- 4.6.1.2 Unauthorized network equipment, telecommunications equipment, or systems are subject to disconnection at PSU OIT's discretion.
- 4.6.1.3 Equipment which links the PSU network and any outside network may only be made with approval from OIT.
- 4.6.1.4 Protocols or systems, which require authentication data to be transmitted in the clear, are prohibited on PSU networks.
- 4.6.1.5 Systems that provide authentication using Odin Account Manager (OAM credentials must be authorized by OIT and meet OAM security standards.
- 4.6.1.6 Highly Sensitive information assets must be placed in a secure, isolated network zone.
- 4.6.1.7 Highly Sensitive information is not to be transmitted outside of the secure zone without appropriate encryption.
- 4.6.1.8 Only authorized PSU users and users officially sponsored by a PSU Faculty or staff may use the PSU private network. PSU maintains a private network for its users to qualify for a waiver from CALEA compliance. Resnet, vendors, and others that require connections to other networks must be hosted on networks that are segregated from the PSU main IP address space.

### 4.6.2 Security of Communications Equipment

- 4.6.2.1 Production network and communications equipment shall be installed in a secure location according to OIT standards for security, environment, space, and power.
- 4.6.2.2 Access to network and/or telecommunications equipment and spaces is restricted to authorized persons (whether student, staff, vendor or contractor) with the appropriate responsibility and knowledge.
  - 4.6.2.2.1 Access to network and or telecom equipment is managed by OIT/NTS
  - 4.6.2.2.2 A signed telecom closet access agreement, approved by NTS must be on file with NTS before access to any network and/or telecom closet.

### 4.6.3 Intrusion Detection

- 4.6.3.1 Critical or sensitive networks, systems, and data shall be carefully monitored in order to detect illicit activity. The following elements shall be included in the monitoring process:
  - Provisions for actual consent to monitoring for users (e.g. logon banners).
  - Notification to users of monitored systems that they should not have any expectations of privacy regarding their use of these systems.

- Activation of operating system and application software audit logging
- Automated alerts
- Analysis of network traffic or system access anomalies
- Use of intrusion detection technologies (network and host-based)
- Monitoring systems to ensure availability of critical services
- Regular reviews of audit logs
- Mechanisms for end-user reporting of anomalies in system performance
- Use of intelligence sources for identifying known hostile threats

#### 4.6.4 Security Incident Handling/Response

4.6.4.1 The CISO will develop, implement, and maintain a PSU Security Incident Response Plan.

4.6.4.2 Information security incidents will be handled in accordance with the PSU Security Incident Response Plan.

4.6.4.2.1 All investigations involving information assets must be performed under the auspices of the CISO.

4.6.4.3 The PSU Security Incident Response plan will document the process for responding to and reporting losses of PII as required by law and regulation.

#### 4.6.5 Security Contacts

4.6.5.1 Each department that provides technology support for its users should appoint a security contact and one or more backup contacts. Groups of departments may agree to share contacts for the sake of efficiency. While contacts need to have some familiarity with the computers in their department and be able to determine the responsible technical person, it is not necessary for the contact to have extensive security expertise. The departmental security contact will:

4.6.5.1.1 Respond to security incident reports from OIT security staff and pass them on to responsible departmental or third party support personnel as appropriate.

4.6.5.1.2 Ensure that appropriate personnel take action in response to each security incident (including escalating the incident to an appropriate departmental authority if action is not taken) and that resolution of each incident is reported to the PSU Chief Information Security Officer.

4.6.5.1.3 Act as a liaison between the CISO and department faculty/staff for information security issues.

4.6.5.1.4 Assist in the presentation and distribution of security awareness training and education of department members.

- 4.6.5.1.5 Develop and execute implementation plans for new PSU information security policies.
- 4.6.5.1.6 Agree to either abide by OIT implementing policies or develop departmental implementing policies to comply with this policy.

#### 4.7 *Acceptable Use*

##### 4.7.1 PSU AUP

4.7.1.1 PSU has established and documented the parameters of acceptable use for all users of PSU information in the PSU Acceptable Use Policy (AUP). The AUP ensures that:

- 1) The use of Information Assets is consistent with standard security practices.
- 2) Information Assets will be operated effectively.
- 3) Information Assets are used in compliance with relevant laws

For example the AUP will include user resource use limitation, definitions of inappropriate behavior, copyright restrictions, commercial use restrictions, and confidentiality requirements.

4.7.1.2 The AUP will include definitions of enforcement mechanisms in case of violation.

4.7.1.3 The AUP will state that prior notification is not a requirement for applicability of the policy and that there should be no expectation of privacy while using PSU resources.

4.7.1.4 To assist users in meeting the AUP, PSU provides anti-virus software, operates a system to distribute current A/V definitions, and a system for distributing security patches as needed.

##### 4.7.2 Extending the AUP

4.7.2.1 Organizations that manage information assets may extend the AUP to address issues that are unique to their situation. Extensions to the AUP may be more restrictive but not less restrictive than the PSU AUP.

4.7.2.2 Departments that do not provide technology support for their users should establish a liaison (non-technical) for coordination of security incidents and to assist in communications between the department and the CISO.

4.7.3 University student residence hall and University Place rental agreements shall include a copy of the AUP.

#### 4.8 *Server and Unix System Administration*

4.8.1 The number of users with total administrative privileges for each administration domain will be limited to the smallest number necessary.

4.8.2 Server and system administrators will monitor for updates and patches for the server OS and applications on a regular basis. New patches will be reviewed by the system administrators and applied as appropriate.

4.8.3 Only the required services will be available on a given server, e.g., file transfer, mail, www.

- 4.8.4 Critical servers will not include less critical functionality, since the less critical functionality might add vulnerabilities, which could impact the critical functions.
- 4.8.5 Virus scanners will be implemented on individual servers where appropriate.
- 4.8.6 Server and system administrators will develop and implement security baselines for each server platform and version. The server security baselines will meet or exceed industry standards for their respective platform. The security baseline specifications will be submitted to the CISO for review and approval. To the greatest extent possible the Windows security baselines should be enforced by domain policy.
- 4.8.7 All servers must be registered with OIT, and are subject to security review. Unregistered servers may be disconnected from the PSU network without notice.
- 4.8.8 OIT will develop server security standards and a process for conducting security reviews
- 4.8.9 Production servers shall be installed in an accountable, secure location according to OIT standards for security, environment, space, and power

#### 4.9 *Windows Workstation Administration*

- 4.9.1 The applications installed on a workstation should be limited to those necessary to accomplish its business function. Information asset managers should use a standard PSU workstation image whenever possible.
- 4.9.2 No one may install networking hardware or software (e.g. VPNs, wireless networking) without prior approval from OIT.
- 4.9.3 All workstations shall use appropriate and current malware protection software and be configured to automatically update using PSU's anti-virus server.
- 4.9.4 Workstations containing sensitive or confidential data must use only PSU officially installed software.
- 4.9.5 Workstations containing sensitive or confidential data must store that data in encrypted form (e.g. using EFS to encrypt a directory).
- 4.9.6 Workstations shall have the most recently available and appropriate security patches and should be configured to automatically update patches using PSU's patch service.
- 4.9.7 Workstations being left unattended shall be automatically logged out or "locked" after 10 minutes to prevent unauthorized access. Users should never leave an unlocked workstation unattended.
- 4.9.8 PSU non-kiosk workstations may not be configured to log in automatically (without a entering a password).
- 4.9.9 All organizations that manage IT assets must configure their PC workstations that connect to PSU enterprise networks to be configured in such a way that they automatically receive appropriate policy changes.
- 4.9.10 Local or Domain administrator privileges should only be granted to TAG or OIT staff. Any request for exceptions must be accompanied by business justification submitted by the requestor, signed by the requestor's Director to be approved by the CISO.
- 4.9.11 Accounts with local or domain administrator privileges should not be used for or any activity that does not require administrative privileges (e.g. browsing the Internet). Users should use their non-privileged accounts for normal day-to-day use. The "Run-as" command should be used when elevated privileges are required.

Logging in as local/domain admin should only be used when the above alternatives are not sufficient.

- 4.9.12 Workstation should be configured to only connect to one network at a time. Requests for exceptions to this policy should explain the need for the exception and should be sent to the CISO for review and approval.
- 4.9.13 Workstations should be configured to record success and failure audit trail records related to accounts and account management.
- 4.9.14 The firewall should be turned on and configured to record log records.
- 4.9.15 Workstation administrators will develop and implement security baselines for each workstation platform and version. The workstation security baselines will meet or exceed industry standards for their respective platform. The security baseline specifications will be submitted to the CISO for review and approval. To the greatest extent possible the Windows workstation security baselines should be enforced by domain policy.
- 4.9.16 The configuration of all systems to be used as Kiosks must be reviewed and approved by OIT and the CISO. Organizations which manage information assets and who grant users local administrator accounts must formally document the business justification. Lack of sufficient justification is grounds for revocation of local administrator access.

#### 4.10 *Remote Access*

The following standards apply to systems accessing PSU resources from outside the PSU network:

- 4.10.1 The remote host must have current protection against malware (virus, spyware, adware, etc.).
- 4.10.2 The remote host may not act as a conduit for traffic to and from the PSU network on behalf of other systems (e.g. using a split tunnel instead of a full VPN tunnel).
- 4.10.3 The remote host must have the most recently available and appropriate security patches.
- 4.10.4 Any remote system, which is to be used to process, store, or transmit critical or sensitive information must permit PSU security measures to be enforced through domain policy.
- 4.10.5 OIT will develop policy and practices to govern special cases, such as UPL customers, HVAC contractors, food service contractors, etc.

#### 4.11 *Authentication Credentials*

- 4.11.1 CISO shall develop and enforce an authentication credentials standard based on NIST SP 800-63 "Electronic Authentication Guidelines."

#### 4.12 *Application Security*

- 4.12.1 PSU organizations that manage information assets should establish policy, procedures, security controls, and standards, which govern these assets. These policies should ensure that fundamental security principles, such as those documented as pervasive principles in the Generally Accepted Information Security

Principles<sup>1</sup> or those generally incorporated into the COBIT<sup>2</sup> framework, are established and maintained.

- 4.12.2 All applications, programs or scripts developed for production use at PSU should use a system development life cycle that includes peer reviews as part of the normal quality review process. Such reviews should look for any unintended consequences of program code that could allow improper access or authorization to any IT asset. Application reviews should ensure that developed applications are free from widely known vulnerabilities, such as those documented in the System Administration and Network Security (SANS) top 20 list and the Open Web Application Security Project (OWASP) Top Ten list of known web application vulnerabilities.
- 4.12.3 Departmental web sites will be developed in accordance with PSU web development standards. OIT is responsible for the development and maintenance of web technology and security standards. University Communications will be responsible for the development and maintenance of content management tools and standards and the PSU official templates. Organizations that do not use UComm content management tools must still comply with UComm and OIT web technology and security standards and policy.
- 4.12.4 Departments that have a web presence must ensure that they have a qualified individual in their department that will maintain the web presence and respond to incidents. That individual may be on staff for the department or on retainer via a Service Level Agreement with OIT or a 3rd party vendor. Departments are responsible for the websites established for or by their staff.
- 4.12.5 Developers requesting a new web presence must be informed about PSU web development standards.
- 4.12.6 All logins for PSU systems must be implemented using an OIT approved authentication method.
- 4.12.7 Adequate (as interpreted by the CISO) authentication and authorization functions must be provided, commensurate with appropriate use and the acceptable level of risk. Use of authentication mechanisms other than that provided by the Odin Account Manager, must be reviewed and approved by OIT prior to use.
- 4.12.8 All web inputs including sensitive/critical or personally identifiable information must use a secure connection (e.g. SSL certificates).
- 4.12.9 No new production 3rd party systems that handle, process, store, or transmit sensitive or confidential information or that permit 3rd party access to production systems may be introduced to PSU networks without an OIT contract and security review.
- 4.12.10 PSU systems that handle, process, store, or transmit FERPA data must meet FERPA requirements.
  - 4.12.10.1 PSU systems that handle, process, store, or transmit HIPAA data are exempt from the HIPAA privacy rule as long as they meet FERPA requirements. The HIPAA security rule should be used as a guideline to

---

<sup>1</sup> [http://www.issa.org/gaisp/\\_pdfs/v30.pdf](http://www.issa.org/gaisp/_pdfs/v30.pdf)  
or see also code of practice for information security management at  
<http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html>

<sup>2</sup> [www.isaca.org/cobit/](http://www.isaca.org/cobit/)

meet due care requirements since FERPA has no security requirements related to health related information.

- 4.12.11 All organizations which accept credit card transactions must use the PSU Business Affairs specified solution(s).
- 4.12.12 Any systems which work with PSU credit card systems must ensure that they do not violate the PCI standard or expose sensitive credit card information.
- 4.12.13 Any information asset manager or individual which qualifies as a "covered entity" for with Fair and Accurate Credit Transactions Act (FACTA) must perform regular risk assessments to determine if they have "covered accounts" for the benefit of PSU or it's employees and students.
  - 4.12.13.1 Information asset managers or individuals which qualify as a covered entity and which have covered accounts must implement a written Identity Theft Prevention Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account, or any existing covered account
  - 4.12.13.2 The program must be appropriate to the size and complexity of the information asset manager organization's size and complexity and the nature and scope of its activities.
  - 4.12.13.3 The program must include reasonable policies and procedures to:
    - 4.12.13.3.1 Identify relevant red flags and incorporate them into the program
    - 4.12.13.3.2 Detect red flags that are part of the program
    - 4.12.13.3.3 Respond appropriately to any red flags that are detected
    - 4.12.13.3.4 Ensure the program is updated periodically to address changing risks
    - 4.12.13.3.5 Incorporate appropriate FACTA Red Flag Guidelines into the program
  - 4.12.13.4 Senior management must oversee development, implementation and administration of the program, training of appropriate staff, and service provider arrangements.
    - 4.12.13.4.1 Ensure service providers' activities are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.
  - 4.12.13.5 The Identity Theft Prevention program must meet FACTA Suspicious Activity Reports requirements.
- 4.12.14 Credit card information shall not be accepted, forwarded, or stored on PSU systems or networks.
- 4.12.15 Social Security Numbers, Drivers' License numbers, other Government IDs (except the PSU ID) and Passport numbers shall not be used as an identifier on PSU systems or networks.
- 4.12.16 All contracts for software, IT hardware, or services must be reviewed by OIT to ensure network and security requirements and conditions, as stated in this security policy, are met.

#### 4.13 Security Operations

- 4.13.1 Organizations managing PSU information assets will either:

4.13.1.1 Create clear and consistent implementation policies in accordance with this information security policy.

4.13.1.2 **OR** agree to comply with the OIT Information Security Policy.

4.13.2 Organizations managing PSU information assets will construct operational standards and policies that ensure due care is taken to secure Information Assets. These operational standards and policies should include reasonable and appropriate proactive and reactive measures to protect Information Assets from unauthorized access, disruption of normal operations, and which comply with appropriate laws and regulation. In particular, organizations managing PSU information assets should provide anti-virus software, a system to distribute current anti-virus definitions, and a security patch management system for commonly used operating systems.

4.13.3 At a minimum each organization managing information assets shall establish:

- a) An incident response plan. This plan shall include a threat containment strategy, a description of the intrusion detection system or approach, and a mechanism for tracking and reporting security breaches.
- b) A notification and escalation plan for security breaches involving personally identifiable information. This plan shall include clearly defined criteria used to determine that personally identifiable information has been exposed and has been, or it is reasonably believed to have been, obtained by an unauthorized person. This plan shall also include clear escalation and notification steps when such an event occurs and the means by which PSU's administration, OUS's administration, appropriate law enforcement agencies, and the people that could be identified by the information in question, are notified of the breach.
- c) An ongoing risk assessment program. This program should regularly identify and track all Essential and/or Highly Sensitive Information Assets, and verify that the appropriate security baseline is in place and being followed with respect to those Information Assets.

4.13.4 Periodic Assessments

4.13.4.1 On a periodic basis, OIT will review PSU security practices for vulnerabilities. This review should include:

4.13.4.2 Review of changes to network infrastructure

4.13.4.3 Quarterly automated external vulnerability testing of PSU systems

4.13.4.4 Password integrity/strength checking

4.13.4.5 On an annual basis, PSU will conduct a penetration test using an external resource for selected highly sensitive or critical systems.

4.13.4.6 Results and remediation efforts will be tracked and trended by the designated approval authority for each system.

4.14 *Security Awareness, Training, and Education*

4.14.1 Organizations which manage information assets are required to develop methods for increasing the level of awareness of information security issues among their constituents. Awareness and training programs may be carried out using a number of different approaches, including document distribution, software distribution, web publishing, and internal or external training sessions. These programs should be

conducted for all new employees and on an annual basis They should be periodically reevaluated in order to assess their effectiveness.

4.14.2 At a minimum, users should be made aware of their roles and responsibilities within the organization as they relate to the security of Information Systems. Users should also be informed of all policies and procedures, which may apply to them. Contact information for OIT Security personnel, as well as organization IT personnel, should be made available. Users should be informed of whom to contact, and appropriate measures to take in the event of a security incident. Policies and procedures should be made readily available in accessible locations Organizations will require and collect acknowledgement of training from users.

4.14.3 All employees should receive appropriate security awareness training as part of the orientation process. This training will cover areas such as:

- Information security policies, standards and procedures
- Accountability for protection of IT assets
- Procedures for reporting the loss and damage of IT assets and security mechanisms
- Practical implications of federal and state law such as privacy concerns and consequences of illegal activity
- The use or reproduction of copyrighted material
- The proper use of SSN, credit card numbers, and other personally identifiable information (PII).
- Virus prevention, detection, and removal
- Internet risks and best practices
- Availability and proper use of Virtual Private Networks
- Password policies and procedures
- Procedures for handling inappropriate requests for information (social engineering attacks)
- The PSU Acceptable Use Policy
- Sanctions for violation of policy

4.14.4 The CISO and OIT should make educational or training materials available in order to educate users on standard security practices. Training on basic computer security concepts should be provided. These concepts include the following: operating system patching, built-in firewalls, anti-virus software, password management, and browser and e-mail security. Additional training should be offered in areas that are of particular concern to the institution.

#### 4.15 *Disaster Recovery/Business Continuity*

4.15.1 As part of ongoing business continuity planning, OIT is responsible for preparing, periodically updating, and regularly testing a campus Disaster Recovery Plan.

- 4.15.2 This plan should address recovering from a disaster that renders Essential Information Assets unavailable for an unacceptable period of time.
  - 4.15.3 The Disaster Recovery Plan should establish the frequency of testing PSU disaster recovery procedures.
  - 4.15.4 The Disaster Recovery plan should ensure that federal, state, local law, regulation and PSU policy is enforced during any response to a disaster.
  - 4.15.5 Information asset managers should ensure that any operations procedures related to essential information assets are coordinated with overall PSU disaster preparedness and business continuity plans.
- 4.16 *Law and regulatory compliance*
- 4.16.1 Policies must take into account federal, state and local laws, other institutional policies and the principle of due care.
  - 4.16.2 To ensure the proper functioning of the University network and compliance with law and regulations, staff of organizations that manage IT assets will monitor network and computer activity and statistics. Anomalies will be reported and investigated as appropriate.
  - 4.16.3 Any websites operated by or for PSU that ask for personally identifiable information must develop and make available a privacy statement that details the website's data collection practices. The privacy statement will meet US privacy law requirements and the Preferences for Privacy Practices (P3P) standard. A copy of the privacy statement should be forwarded to the PSU General Counsel's office for review and approval prior to posting.
  - 4.16.4 Any research projects that involve personally identifiable information or that include requirements for the protection of the research data are required to develop a security plan for approval by the PSU CISO.
  - 4.16.5 All organizations which manage information assets are subject to audits by OUS or security assessments by PSU OIT.

## 5.0 Exceptions

The CIO, via written communication from department chairs, Deans or other university executives, will accept requests for exemptions. Requests must detail the specific exception being requested, the organizational benefit and any measures that will be applied to manage the additional risk. An exception is not considered granted until written approval is received from the CIO.

## 6.0 Enforcement

In general, individuals in a position of trust (sensitive or critical personnel), in a supervisory, or management position will be held to a higher standard of conduct and enforcement.

To ensure consistent enforcement of policy, the CISO will work with the CIO, HR, FADM, the Provost's office, and General Counsel to develop an enforcement standard.

### 6.1 Organizations

Organizations which manage IT assets that fail to comply with this policy may be subject to a number of actions based on the severity or frequency of the violations. Steps which may be taken include but are not limited to actions to protect the university or the Internet community from damage, (isolating or shutting down disruptive or dangerous systems), requiring systems to be moved to a protected data center, and loss of the privilege to operate independently of OIT. In

addition, HR may exercise additional disciplinary measures for associated faculty and staff. Faculty and staff associated with some violations may also be subject to civil liabilities or criminal prosecution.

#### 6.2 *Faculty/Staff*

Sanctions for faculty or staff violations of this policy or the AUP include but are not limited to temporary or permanent loss of PSU information asset access privileges, fines, leave without pay, restitution of damages, termination, civil or criminal prosecution.

#### 6.3 *Students*

Sanctions for student violations of this policy and the AUP include but are not limited to temporary or permanent loss of PSU information asset access privileges, fines, suspension, or expulsion, civil, or criminal prosecution.

#### 6.4 *Non-PSU*

Contractors, vendors, temporary employees, visitors, and other non-PSU individuals who violate this policy may lose the privilege of having access to PSU information assets. Some violations of this policy may also subject the individual to civil suit or criminal prosecution.

### 7.0 Related Policies/Procedures

PSU Acceptable Use Policy – <http://www.oit.pdx.edu/aup/>

### 8.0 Policy Update Requirements

Technological advances and changes in the business requirements will necessitate periodic revisions to policies and standards. The Chief Information Security Officer is responsible for routine maintenance of these items to keep them current. Deficiencies within this Information Security Policy should be immediately communicated to the PSU Chief Information Security Officer. Major policy changes will require the approval of the CIO. Responsibility for maintenance of the PSU Information Security Policy resides with the CIO. This policy will be reviewed no less than annually.

## Appendix A – Definitions

**Accountable Authority** – The major stakeholder for an information asset. The accountable authority controls access and makes decisions about the use, disposition, and protection of an information asset. The Accountable Authority makes the accreditation decision to put a system into production and accept residual risk. The Accountable Authority ensures that all major stakeholders are known and that their needs have been considered during decision making.

**Data Owner** – an individual with administrative responsibility for campus organizational units (e.g. deans, department chairs, directors, or managers) or individuals having functional ownership of data. This individual should represent the primary stakeholder of this information. The data owner creates the data, directs its use and protection, and ensures that users of the data use the data in compliance with law and regulation.

**Process Owner** - an individual with administrative responsibility for campus organizational units (e.g. deans, department chairs, directors, or managers) or individuals having functional ownership of a process, procedure, or program. This individual should represent the primary stakeholder of this information. The process owner creates the process, directs its use and protection, and ensures that users of the process use the it in compliance with law and regulation.

**Data Provider** – an individual or group who designs, manages, and/or operates electronic information resources, e.g. project managers, system designers, application programmers, or system administrators.

**Data Custodian** – an individual, designated by the data owner, who is empowered to make technical decisions regarding the disposition of a particular data set (e.g. a departmental administrator). The Data custodian is responsible for protecting the university and the custodial information assets in a manner that meets applicable law, regulation and due care.

**Data Set** – a functional grouping of related data. This would include databases or database tables, file systems and directories.

**Designated Accountable Authority** - For all information assets there needs to be a single individual that is accountable (controls access, makes decisions about, etc.) In most cases that accountable authority is not ambiguous. However, in cases where there are several major stakeholder for a particular information asset, the accountable authority must be designated by a management representative sufficiently high enough to encompass all stakeholders.

**Information Asset** - includes information, networks, and systems that are owned by PSU, information that PSU is obligated to keep secure by applicable law or by contract, and information exempt from disclosure under public records laws. PSU Information Assets are written, spoken, electronic, printed, magnetic, optical and other mediums.

**Odin Account Manager (OAM)** – OAM is the PSU system for managing the primary enterprise user accounts.

**Personally Identifiable Information (PII)** – The Oregon Identity Theft Prevention Act defines personal information as a name associated with a Social Security number, Passport number (or other United States issued identification number), Oregon drivers license number or Oregon identification card, financial (e.g. bank account), credit or debit card number along with a security or access code or password that would allow someone access to a consumer's financial account. Further it requires that the SSN be protected even if it is not accompanied with a name. Other laws (such as HIPAA, FERPA, etc.) identify different sets of information as

Personally Identifiable or as requiring specific protections. Owners, providers, custodians, and users of information must ensure that this information is protected in accordance with relevant law.

**PSU Sponsor** - A PSU Sponsor is an employee or staff of PSU with an active PSU Account who agrees to be responsible for the behavior of one or more sponsored account holders. Sponsors must ensure that sponsored account holders comply with PSU Acceptable Use Policy.

**Server** – Any system that provides services may be considered a server regardless of the type of platform (e.g. workstation, Unix server, Windows server, Mac desktop). Even PDA or cell phones may be considered a server if they offer services for other users. For purposes of this policy, a system is considered a server if it offers departmental or enterprise services. In addition a system which could impact the integrity, availability, or confidentiality of PSU information assets is considered a server so that security controls can be levied against it to mitigate the potential harm.

**Sponsored Account** – PSU maintains a private network. Individuals who are not students, faculty or staff that wish use PSU information assets must have a PSU Sponsor.

**Technology Administrators Group (TAG)**– An organization chaired by OIT that meets to discuss Information Technology topics and coordinate IT activity that affects multiple organizations. Members of the TAG are appointed by their organizations and serve as their organization’s Point of Contact for IT and Information Security issues. The group serves as a venue for discussion of PSU-wide policy and issues related to IT and Information Security.

**University community members** – Students, faculty, staff, vendors, contractors, guests. Any and all users of PSU information assets, PSU resources or attendees of events held at PSU.

**Users** - individuals who access and use PSU information assets

**Secure Transport** – A method of transferring information that ensures both confidentiality (e.g. encryption) and authenticity (strong authentication). Common examples include the Secure Shell (SSH) protocol and Transport Layer Security (TLS/SSL).

**Security Sensitive Personnel** – Employees that are likely have or need access to essential or highly sensitive data and processes shall be designated as Security Sensitive Personnel. Per OAR 580-023-0005 these employees serve in critical or security-sensitive capacities and are subject to the appropriate employment policies (e.g. background checks) of the institution.

## **Sensitive and Confidential Information**

**Attorney-Client privileged** – Communications between a client and an attorney are privileged communications and must not be shared with law enforcement or opposing counsel. This type of information asset must be protected according to guidelines in the DOJ Corporate Prosecution Guidelines.

**Unclassified** – Information which may be seen by anyone. Only default security measures apply or security measures taken by the possessor or owner.

**Public** - May be seen by anyone, but requires protection against unauthorized modification. This would include information such as class schedules or material appropriate for publishing on a publicly accessible website.

**Essential** – Information Assets that are critical to the function of PSU and without which

normal business functions of PSU cannot occur. These information assets would be a subset of PSU or department production information assets.

**Sensitive** - Only authorized individuals may see or modify this information. Requires customized access control procedures. Improper disclosure may result in harm to the organization or to individuals. This would include most personal information such as addresses and phone numbers.

**Highly Sensitive** - Information Assets that are owned by PSU, information that PSU is obligated to keep secure by applicable law or by contract, and information exempt from disclosure under public records laws. PSU Information assets are found in written, spoken, electronic, printed, magnetic, optical and other mediums. This would include information such as but not limited to access credentials (passwords), Social Security Numbers, student financial information, video surveillance, audit trail logs for Sensitive, Essential or above systems, and credit card information.

**Audit Trail logs** - Audit trail logs should be considered at least as sensitive as the data whos activity it records. Audit trails containing access control and authentication data should be considered the highest classification of any data on a system.

DRAFT

## Appendix B – Relevant legislation, regulation, and industry standard

OUS Information Security Policy (OAR 580-055-0000)

OUS Criminal Background Checks Policy (OAR 580-023-0005)

Other divisions of OAR 580 related to student records, faculty records, requirements related to the protection of information assets.

Digital Millennium Copyright Act (DMCA)

Family Educational Rights and Privacy Act (FERPA)

Health Insurance Portability and Accountability Act (HIPAA)

Payment Card Industry-Data Security Standard (PCI –DSS)

Personally Identifiable Information (PII) related to the Oregon ID Theft Protection Act and others

e-Discovery related to the 2006 US Supreme Court amendment to the Federal Rules of Civil Procedure and Oregon Department of Justice guidance regarding e-Discovery.

Fair and Accurate Credit Transactions (FACT) Act of 2003, particularly the Red Flag rules