Policy No. 580-055

INFORMATION SERVICES

580-055-0000

Executive Summary

(1) OUS has a responsibility to protect its Information Assets, business processes, and follow appropriate laws and regulation relating to information security.

(2) OUS will meet its obligations by each member institution implementing an ongoing information security program.

(3) Each Institution's President (or designee) will have overall responsibility for institution's program.

(4) Each Institution will assign Chief Information Security Officer (CISO) duties to a qualified person.

(5) Each Institution's CISO or equivalent will be responsible for the security program and for ensuring that institutional policies, procedures, and standards are developed, implemented, and maintained

(6) Each Institution will create Information Systems Policies that cover at a minimum: Classification Standards that at least identify Essential and Highly Sensitive data, processes, and systems; security baselines commensurate with classification; and labeling and handling standards for Highly Sensitive data, processes, and systems.

(7) Each Institution will create Personal Information and User Policies that cover at a minimum: Securing Personally Identifiable Information; Acceptable Use of Computing Resources; employee polices for security-sensitive personnel; and account management policies.

(8) Each Institution will create Security Operations policies that cover at a minimum: a notification and escalation plan for breaches of personally identifiable information, a risk assessment program; and an incident response plan.

(9) Each Institution will create Network and Telecommunications Policies that at a minimum ensure that Highly Sensitive Information Assets are in a secured zone on the network and are not transmitted outside of secured zones in clear text.

(10) Each Institution will establish physical security standards that protect Essential or Highly Sensitive Information Assets that are critical to the functioning of the institution and ensure that disposal procedures remove or render sensitive data irretrievable from hard drives, compact disks, external memory, PDAs, etc.

(11) Each Institution will establish a Disaster Recovery Plan for Essential Information Assets.

(12) Each Institution will develop awareness and training programs for all Information Asset users regarding Information Security.

(13) OUS Internal Audit will conduct periodic Information Security Policy Audits.

Hist.: OSSHE 4-2007, f. & cert. ef. 7-23-07

580-055-0010

Purpose

(1) The Oregon University System and its member institutions, collectively referred hereinafter as OUS, have a responsibly to protect information entrusted to them, ensure the effective operation of business critical processes, and must abide by the security policies established by the State Board of Higher Education as well as laws and regulation at the federal, state, and local level relating to information security. OUS must meet a standard of due care regarding the protection of institutional information assets as well as those belonging to OUS students, faculty members, customers, and research partners.

(2) OUS "Information Assets" include information and systems that are owned by OUS, information that OUS is obligated to keep secure by applicable law or by contract, and information exempt from disclosure under public records laws. OUS Information Assets are found in written, spoken, electronic, printed, magnetic, optical, and other mediums.

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

Hist.: OSSHE 4-2007, f. & cert. ef. 7-23-07

580-055-0020

Goals

OUS member institutions will develop and implement ongoing information security programs, and assign clear and appropriate roles and responsibilities to the administration, IT personnel, and institutional community members. The basic objectives are to achieve and maintain:

(1) TRUST -- Ensure that institutions establish a baseline of security that will serve as a basis for the ongoing trust of OUS' information systems, engender confidence between OUS and its students, faculty members, customers, research partners, and the citizens of the State of Oregon.

(2) INTEGRITY -- Establish the concepts of due care, best practice, and security baselines as the basis for protecting the Information Assets of OUS in a manner commensurate with their sensitivity, value, and criticality to ensure they meet expectations of form, fit, and function.

(3) ACCOUNTABILITY -- Maintain the accountability of information users, preserve management options if there is asset misuse or abuse, ensure security of OUS's physical assets, and provide for business continuity.

Hist.: OSSHE 4-2007, f. & cert. ef. 7-23-07

580-055-0030

Authority and Scope

(1) This policy applies to the Oregon University System as organized and empowered by ORS chapters 351 and 352 and is specifically authorized under ORS 351.087. This policy is applicable to all OUS member institutions as well as all employees, students, contractors, consultants, agents, and vendors working on their behalf. It is applicable to all OUS Information Assets, regardless of form or media. It applies to information gathering, protection, use, processing, storage, communications, and transit.

(2) OUS Member Institution policies, procedures, standards, and work instructions are required to comply with this policy.

Hist.: OSSHE 4-2007, f. & cert. ef. 7-23-07

580-055-0040

Roles and Responsibilities

(1) The OUS Chancellor shall have overall oversight responsibility for the provisions of this policy.

(2) The OUS Chief Information Security Officer (CISO) shall have responsibility to develop, implement, maintain, and monitor compliance with this policy.

(3) Each member institution's President shall have overall oversight responsibility for institutional provisions set forth in this policy.

(4) Each member institution's Chief Information Officer (CIO), or equivalent, shall be responsible for ensuring that institutional policies are developed in accordance with this policy.

(5) Each member institution shall designate a CISO or equivalent. The institutions' CISO shall be responsible for the member institution's security program and for ensuring that institutional policies, procedures, and standards are developed, implemented, and maintained.

(6) All university community members have a responsibility to help ensure security of the Institution's Information Assets.

Hist.: OSSHE 4-2007, f. & cert. ef. 7-23-07

580-055-0050

Institutional Policy Requirements

(1) Security Management:

(a) Each member institution shall establish an ongoing information security program and assign clear and appropriate roles and responsibilities to their Administration, CIOs (or equivalent), CISO (or equivalent), and all local University community members. The President of each member institution (or their designee) will be responsible for establishing the program and ensuring that it is effective.

(b) Each member institution should create clear and consistent policy in accordance with their information security program, that outline general information security operations including such things as risk assessment procedures, incident response responsibilities, security testing, and day to day security compliance. The specifics of those policy requirements are outlined in the following sections.

(2) Information Systems Security:

(a) 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. OUS Member institutions should establish policy, procedures, security controls, and standards that 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 or those generally incorporated into the COBIT framework, are established and maintained.

(b) At a minimum each member institution shall establish:

(A) Information system classification standards. These standards shall ensure that Essential and/or Highly Sensitive data, applications, and infrastructure systems are identified and standards for handling them are developed. Member institutions may deem it appropriate to establish multiple levels of sensitivity or criticality.

(B) Security baselines for information systems. Security baselines are minimum set of operational guidelines that affect the relative security of an Information Asset. Baselines shall be appropriate to the level of sensitivity and criticality of the systems and ensure that the due care and best practice principles are met.

(3) User and Personal Information Security:

(a) Everyone interacting with information assets has a responsibility to ensure the security of those assets. Each member institution must create policies that articulate the rights, responsibilities, and roles of anyone interacting with Information Assets. Policies must take into account federal, state, and local laws, as well as other institutional policies. For example, FERPA requirements will require attention when dealing with student records and HIPPA requirements will require attention when dealing with health information. Policies should be made readily available to all interested parties.

(b) At a minimum, each member institution shall establish:

(A) Personal Information Policies. Member institutions are required to specifically define procedures for dealing with personally identifiable information. Information, such as social security numbers, credit card numbers, and driver's license information, is naturally sensitive and appropriate steps should be taken to protect the privacy of this type of information.

(B) Acceptable Use Policies. Member institutions are required to develop policies that define the parameters of acceptable use for all users of information resources within the organization. These policies must ensure that the use of Information Assets is consistent with standard security practices, ensures that those resources operate effectively, and that appropriate laws relating to Information Assets are followed. For example, these policies may include user resource use limitation, definitions of inappropriate behavior, copyright restrictions, commercial use restrictions, and confidentiality requirements. These polices should also include definitions of enforcement mechanisms in case of violation. Member institutions shall make it clear that prior notification is not a requirement for applicability of the policy and they shall clearly state that there should be no expectation of privacy while using institutional resources.

(C) Security Sensitive Personnel Policies. 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 055.055 and be subject to the appropriate employment policies of the institution.

(D) Account management Polices. Member institutions are required to develop policies that ensure appropriate management of user accounts. These polices shall: establish and maintain accountability, timely notification of access changes and terminations, timely response to these notifications; and periodic reconciliation of accounts to active users, privileges, and separation of duty requirements. This includes students, employees, contractors, vendors.

(4) Security Operations:

(a) OUS member institutions have a responsibility to 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 that comply with appropriate laws and regulations. In particular, member institutions should provide anti-virus software, a system to distribute current anti-virus definitions, and a security patch management system for commonly used operating systems.

(b) At a minimum each member institution shall establish:

(A) An incident response plan. This plan shall include a threat containment strategy, an intrusion detection system, 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 the member institution's administration, OUS' 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.

(5) Network and Telecommunications Security:

(a) OUS member institutions have a responsibility to ensure secure management of their local networks. Member institutions should have the ability to control who connects to their networks, the ability to create secure zones with restricted access on their networks, and be able to ensure the effective operation of their networks.

(b) At a minimum each member institution shall establish:

(A) Secured Zones for Essential and Highly Sensitive Information Assets. These zones shall be created by employing standard network technology to restrict access at the network level to authorized personnel only.

(B) Policies that prohibit transmission of unencrypted Highly Sensitive data outside of secured zones.

(6) Physical and Environmental Security:

(a) Each member Institution should establish procedures for the physical protection of its Information Assets. Protection of physical equipment or of software and data residing on storage media, from theft, loss, damage, or improper use should be addressed. Particular attention must be paid where access to or function of Essential or Highly Sensitive Information Assets is concerned; however, member institutions should also consider physical security for computers and other local Information Assets housed in departmental work areas or under departmental control, such as laptop computers, PDAs, etc. Member institutions should adopt policies that only allow Highly Sensitive data to be permanently retained on portable equipment if protective measures, such as encryption, are implemented that safeguard the confidentiality and integrity of the data in the event of theft or loss of the portable equipment.

(b) At a minimum, member Institutions shall develop policies and procedures to:

(A) Protect physical areas containing Information Assets that represent Essential or Highly Sensitive information systems that are critical to the functioning of the institution.

(B) Ensure that disposal procedures remove or render sensitive data irretrievable from hard drives, compact disks, external memory, PDAs etc.

(c) In addition, physical inventories of equipment should be completed and maintained in accordance with section 55.100 of the OUS Fiscal Policy Manual.

(7) Disaster Recovery:

(a) As part of ongoing business continuity planning, member institutions are responsible for preparing, periodically updating, and regularly testing a campus Disaster Recovery Plan. This plan should address recovering from a disaster that renders Essential Information Assets unavailable for an unacceptable period of time. Such a Disaster Recovery Plan should establish the frequency of testing member institution disaster recovery procedures. Member institutions should ensure that any local operations procedures are coordinated with overall institutional disaster preparedness plans.

(8) Awareness, Education, and Training:

(a) Member institutions 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 carried out on a regular basis and they should be periodically reevaluated in order to assess their effectiveness.

(b) 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 that may apply to them. Contact information for central IT Security personnel, as well as department 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.

(c) Educational or training materials should be made 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.

Hist.: OSSHE 4-2007, f. & cert. ef. 7-23-07

580-055-0060

Policy Review Process

The OUS CISO will review this policy annually to ensure that it complies with applicable law and Board Policies. Should this policy be revised, the CIOs (or equivalent) of each member institution will be notified to ensure local policies are reviewed and revised as appropriate.

Hist.: OSSHE 4-2007, f. & cert. ef. 7-23-07

580-055-0070

Audit

The OUS internal audit office has the authority to conduct periodic information security policy audits using the COBIT framework or suitable substitute to ensure compliance and notify each member institution of any noted deficiencies.

Hist.: OSSHE 4-2007, f. & cert. ef. 7-23-07

580-055-0080

Glossary

(1) Anti-Virus -- Programs that identify malicious code installed on computers without the owner/operator's knowledge or consent.

(2) Applications -- Computer programs that collect, process, or otherwise manipulate data.

(3) Best Practice -- Generally accepted industry practices that have been broadly adopted and considered standard.

(4) Built-in Firewall -- Functions within the local operating system of a computer that limit what other machines on the network can connect to it.

(5) Business Continuity -- The ability for business processes and functions to continue and for an organization to continue to function despite emergencies, major disruptions, etc.

(6) CIO -- Chief Information Officer. The executive level position in an organization that is generally in charge of the Information Technology division and is responsible for the overall IT operations of an organization.

(7) CISO -- Chief Information Security Officer. Generally, the CISO function is one of being responsible for the Information Security Program.

(8) Data -- Information stored electronically, or in print.

(9) Due Care -- The conduct that a reasonable man or woman will exercise in a particular situation in looking out for the safety of others. If one uses due care, then an injured party cannot prove negligence. This is one of those nebulous standards by that negligence is tested. Each juror has to determine what a "reasonable" man or woman would do.

(10) Essential Information Assets -- Those Information Assets that are critical to the function of the member institution and without which the normal business functions of the member institution cannot occur.

(11) FERPA -- Family Educational Rights Privacy Act. This federal act protects student records, other than directory information, as private information available only to those with an educational need to know.

(12) HIPPA -- Health Information Protection and Privacy Act. This federal act protects health records as private information.

(13) Highly Sensitive Information Assets -- Those Information Assets that OUS is obligated by law or contract to protect or that represent obviously confidential data that, if released, would represent some actual legal liability to the member institution.

(14) Incident Response -- The planned reaction to a breach of security that includes identifying the breach, closing it, and mitigating its effect.

(15) Information Assets -- Information and systems that are owned by OUS, information that OUS is obligated to keep secure by applicable law or by contract, and information exempt from disclosure under public records laws. OUS Information Assets are found in written, spoken, electronic, printed, magnetic, optical, and other mediums.

(16) Information Systems -- A collection of computers and processes that interact with each other to manipulate, transmit, and store data.

(17) Infrastructure Systems -- Computers and network devices and the operating systems that run them.

(18) Institutional Community Members -- faculty, staff, students, vendors, visitors, affiliates, courtesy faculty, etc. In short, all persons who have a relationship with the Institution and therefore may interact with Information Assets of the Institution.

(19) Intrusion Detection System -- A program or series of programs that watch network traffic and other activities to identify intrusion attempts and compromised machines.

(20) Risk Assessment -- In the context of information security, risk assessment is the determination of both the importance of all Information Assets and their likelihood of being accessed by an unauthorized person or of their function being intentionally impaired by someone.

(21) Security Baseline -- A minimum set of operational guidelines that affect the relative security of an Information Asset. These guidelines would typically cover such things as firewall settings and network access controls, local permissions, password change policy, operating system patch management, anti-virus policy, and physical access controls.

(22) Security Breach -- Theft or unauthorized acquisition of Information Assets by a person that harms or poses an actual threat to the security, confidentiality, or integrity of those assets.

(23) Security Controls -- Procedures to follow that help establish and maintain Authentication, Authorization, and Access to Information Assets. These controls include such things as verifying identity, giving access to Information Assets based on job function or duties, network appliances that restrict connections coming from the Internet or unsecured zones, etc.

(24) Threat Containment -- Reactive measure to ensure that a security breach is contained to affected systems and that those systems are not able to be used to launch successful intrusion attempts to other systems.

(25) Operating System -- The series of programs loaded on a computer that operates it. Common operating systems include Windows, MacOS, and Unix.

(26) OUS Member Institutions -- The Chancellor's Office, Eastern Oregon University, Oregon Institute of Technology, Oregon State University, Portland State University, Southern Oregon University, University of Oregon, and Western Oregon University.

(27) Password Management -- The practice of creating and maintaining passwords on a system that are not easily guessed, programmatically determined, or otherwise obtained by unauthorized persons. This generally means requiring a base level of complexity in the password, and that it is changed on a regular basis.

(28) Personally Identifiable Information -- A combination of name and one or more other data elements that could uniquely identify an individual for the purpose of providing restricted access. This term may be formally defined shortly in anti "ID Theft" legislation. Common data elements used in combination with name are: Social Security number, driver's license numbers, date of birth, account number (such as credit or debit card number), account passwords (including pass phrases such as mother's maiden name), identification number issued by a foreign nation, passport number, biometric data, etc.

Hist.: OSSHE 4-2007, f. & cert. ef. 7-23-07