Operational Policy

Policy title:	Information Security Risk Assessment Policy		
Policy number:	DHS|OHA-090-006		
Original date:	03/11/2015	**Last update:**	11/07/2016
Approved:	Mark Fairbanks, CFO OHA Dr. Reginald Richardson, Deputy Director, DHS		

Purpose

The Department of Human Services (DHS) and Oregon Health Authority (OHA) are committed to ensuring the confidentiality, integrity, and availability of information assets and systems by protecting those assets and systems from unauthorized access, modification, destruction, or disclosure and ensuring their physical security. The purpose of an information security risk assessment (ISRA) is to identify and assess the threats and vulnerabilities that pose a risk to DHS|OHA information assets. Risk assessment supports the management of risk and the selection of cost-effective controls.

Description

This policy ensures that DHS and OHA information assets and systems are assessed for potential risks and vulnerabilities so the agencies can maintain the confidentiality, integrity, and availability of all protected information.

Applicability

This policy applies to all DHS and OHA staff including employees, volunteers, trainees, and interns as well as contractors, partners and business associates.

As keepers of the public trust, all agency employees have a responsibility to comply with state and agency policies, administrative rule, and state and federal law. The agency takes this responsibility seriously and failure to fulfill this responsibility is not treated lightly. Employees who fail to comply with state or agency policy, administrative rule, or state and federal law may face progressive discipline, up to and including dismissal from state service.

Policy

1. DHS and OHA shall take appropriate measures to safeguard the confidentiality, integrity and availability of all protected information.
2. DHS and OHA shall develop, implement and maintain a risk assessment program that identifies potential threats and vulnerabilities to information assets and systems to include all forms of electronic media. Electronic media includes but is not limited to, hard drives, floppy disks, CDs, DVDs, other storage devices, transmission media, and portable media.

3. The Information Security and Privacy Office (ISPO) will use the results from risk assessments to advise the agency on appropriate measures to safeguard against identified risks, in accordance with federal and state statute and rule program requirements.
4. The ISPO shall assess agency information systems and the information it processes, stores or transmits for the likelihood and magnitude of harm resulting from unauthorized use, disclosure, disruption, modification, or destruction of the system or information, as required by law based on the information in each system.
5. Risk assessments shall include an evaluation of:
   a. Administrative security measures.
   b. Technical security and monitoring.
   c. Physical security measures.
6. Risk assessments shall be performed:
   a. As needed based on the statutory and regulatory requirements.
   b. When initiated by the Chief Information Security Officer (CISO).
   c. When there are significant changes to the information system, the environment of operation, or other conditions that may impact the security of the system based on the information in each system.
7. ISPO shall communicate the results of risk assessments to management personnel for inclusion in the agencies' risk evaluation and management plans including the:
   a. Chief information Officer
   b. Chief Information Security Officer
   c. Privacy Compliance Officer
   d. Program section manager
   e. Chief Audit Officer
8. All DHS and OHA workforce members shall cooperate with staff doing risk assessments.
9. DHS and OHA follow all federal and state statutes and rules and all applicable Oregon Department of Administrative Services statewide policies.

References

45 CFR 160 & 164
OAR 125-055-0100 to 125-055-0130
OAR 943-014-0400 to 943-014-0465 MARS-E Document Suite, Version 2.0, Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges
Criminal Justice Information Systems Security Standards (CJIS)
Federal Information Processing Standards (FIPS) Publication (Pub) 199
Federal Information Processing Standards (FIPS) Publication (Pub) 200
IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies
National Institute of Standards and Technology (NIST) 800-30 Rev. 1
National Institute of Standards and Technology (NIST) 800-37 Rev. 1
National Institute of Standards and Technology (NIST) 800-53 Rev. 4
Social Security Administration Information Exchange Security Requirements and Procedures
DHS|OHA-090-006-03 Vulnerability Assessment Process
DHS|OHA-090-006-04 Vulnerability Assessment Process Map

Forms referenced

Related policies

DAS 107-004-052 Information Security
DAS 107-004-120 Information Security Incident Response

DHS|OHA-010-014 Agency Compliance with Statewide Administrative Policy
DHS|OHA-090-001 General Security Policy
DHS|OHA-090-005 Security Incident Management
OHA-100-014 Report and Response to Privacy and Security Incidents

Related Processes

DHS|OHA-090-006-01 Risk Assessment Process
DHS|OHA-090-006-02 Risk Assessment Process Map

Contact

Information Security and Privacy Office (ISPO)
Phone: 503-945-6812 (Security)
503-945-5780 (Privacy)
Fax: 503-947-5396
ispo.inforisk@dhsoha.state.or.us

Policy history

Version 1 DHS|OHA-090-006 established 03/11/15
Version 2 DHS|OHA-090-006 reviewed annually 03/04/16
Version 3 DHS|OHA-090-006 revised 11/7/16

Keywords

Confidentiality, electronic protected health information, ePHI, integrity, ISRA, information security risk assessment, personally identifiable information, PHI, PII, protected health information, physical security assessment, risk assessment, vulnerabilities, scanning, security, vulnerability analysis

---