Operational Policy

Policy title:	Information Security Risk Assessment Policy		
Policy number:	ODHS|OHA 090-006		
Original date:	03/11/2015	**Last update:**	11/02/2020
Approved:	Kris Kautz, OHA Deputy Director Don Erickson, ODHS Chief Administrative Officer		

Purpose

The Oregon Department of Human Services (ODHS) 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 ODHS|OHA information assets. Risk assessment supports the management of risk and the selection of cost-effective controls.

Description

This policy ensures that ODHS 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 ODHS 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. ODHS and OHA shall take appropriate measures to safeguard the confidentiality, integrity and availability of all protected information.

2. ODHS 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 digital media[1].
3. Digital media is any form of electronic media designed to store data in a digital format. This includes but is not limited to memory device in laptops, computers, and mobile devices; and any removable, transportable electronic media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card.
4. 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.
5. The ISPO shall assess agency information systems and the information processed, stored or transmitted 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.
6. Risk assessments shall include an evaluation of:
   a. Administrative security safeguards.
   b. Technical security and monitoring.
   c. Physical security safeguards.
   d. Compliance requirements.
7. Risk assessments shall be performed:
   a. As needed based on the statutory and regulatory requirements.
   b. When initiated by the Chief Information Risk Officer (CIRO).
   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.
8. 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. CIRO
   c. Privacy Compliance Officer
   d. Program section manager
   e. Chief Audit Officer
9. All ODHS and OHA workforce members shall cooperate with staff doing risk assessments.

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)
CJIS Security Policy 5.9

[1] Digital Media - Any form of electronic media designed to store data in a digital format. This includes but is not limited to memory device in laptops, computers, and mobile devices; and any removable, transportable electronic media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card. CJIS Security Policy, Version 5.9, 06/01/2020

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. 2
National Institute of Standards and Technology (NIST) 800-39
National Institute of Standards and Technology (NIST) 800-53 Rev. 5
Social Security Administration Information Exchange Security Requirements and Procedures
Statewide Information and Cyber Security Standards 2019
Center for Internet Security Top Twenty Critical Security Controls
ODHS|OHA 090-006-01 Information Security Risk Assessment Process
ODHS|OHA 090-006-02 Information Security Risk Assessment Process Map
ODHS|OHA 090-007 Information Technology Vulnerability Management Policy
ODHS|OHA 090-007-01 Continuous Vulnerability Assessment Process
ODHS|OHA 090-007-02 Continuous Vulnerability Assessment Process Map

Related policies
DAS 107-004-052 Information Security
DAS 107-004-120 Information Security Incident Response
ODHS|OHA 090-005 Information Security Incident Management
OHA 100-014 Report and Response to Privacy and Security Incidents

Contact
Information Security and Privacy Office (ISPO)
503-945-6812 (Security)
503-945-5780 (Privacy)
Email: ispo.inforisk@dhsoha.state.or.us

This policy shall be reviewed at least once every year to ensure relevancy.

Policy history
Version 1 DHS|OHA 090-006 established 03/11/2015
Version 2 DHS|OHA 090-006 reviewed annually 03/04/2016
Version 3 DHS|OHA 090-006 revised 11/7/2016
Version 4 ODHS|OHA 090-006 reviewed 11/02/2020

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

---