Operational Policy

Policy title:	Information Technology Vulnerability Management Policy		
Policy number:	ODHS|OHA 090-007		
Original date:	06/05/2017	**Last update:**	06/07/2021
Approved:	Kris Kautz, Deputy Director Oregon Health Authority Don Erickson, Chief Administrative Officer Oregon Department of Human Services		

Purpose

The Office of Information Services (OIS) is committed to implementing and maintaining a vulnerability management program for the Oregon Department of Human Services (ODHS) and the Oregon Health Authority (OHA) that protects information assets and systems, mitigates vulnerabilities, and reduces the risk of malicious activity. This policy pertains to third party software, operating systems, and any other systems not developed internally.

Description

This policy applies to all information systems and applications of ODHS|OHA. This policy outlines the implementation and maintenance of comprehensive, integrated information security techniques designed to proactively identify and report the exploitation of vulnerabilities through a collaborative, systematic, accountable, and documented process. Vulnerabilities may result in unauthorized access to a system or network, access to or theft of confidential data, resulting in regulatory, financial, or reputational impact.[1]

Applicability

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

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. Vulnerabilities are weaknesses in information technology (IT) systems, system security procedures, internal controls, or implementations that can be exploited or triggered by a threat source.

[1] National Institute of Standards and Technology (NIST) 800-30 Rev. 1

2. The Enterprise Information Services (EIS) Cyber Security Services (CSS) shall run automated vulnerability scans at least weekly on all ODHS|OHA information systems and applications. Systems that are not managed internally by the agency shall be required to prove ongoing vulnerability assessments are completed.
3. Vulnerability assessments of information systems and applications shall occur based on any of the following criteria:
   a. Best practices, or statutory and regulatory requirements.
   b. Significant or major changes are made to the environment including new infrastructure, applications, websites, upgrades, or modifications to infrastructure or applications, or other conditions that may impact the security of the system based on the information in each system.
   c. At the discretion of the EIS CSS and the agency Chief Information Risk Officer (CIRO).
4. Patch deployment shall be performed by authorized individuals in a timely manner.[2]
5. Where appropriate, OIS, ODHS|OHA programs, information system owners, EIS CSS, and EIS Data Center Services (DCS), shall ensure:
   a. All patches are evaluated for risk and impact to ODHS|OHA.
   b. The risk associated with deployment or exceptions from patching are approved and documented.
   c. Vulnerabilities remediated during the assessment are retested to verify patches and other corrections are effective in mitigating identified risks.
6. When vulnerabilities are identified and cannot be resolved, the information system owner shall be responsible for:
   a. Accepting the risk of allowing the vulnerability to persist in the system;
   b. Determining whether remediation is required, such as taking the information system offline; or
   c. Transferring or avoiding the risk.
7. An individual who requests not to receive a required patch for an ODHS|OHA issued device, whether mobile, desktop, laptop, or tablet, shall not use the device for ODHS|OHA business without an approved exception. Periodic review of the following shall occur:
   a. Whether the exception is still justified.
   b. Whether someone is ensuring that patches are still being manually applies to the extent possible.

References

Microsoft SecurityTech Center Security Bulletin Severity Rating System, GG309177
National Institute of Standards and Technology (NIST) 800-30 Rev. 1
NIST 800-40 Rev. 3
NIST 800-53 Rev. 5
NIST 800-61 Rev. 2
NIST 800-115
NIST 800-137
NIST Internal Report (IR) Common Vulnerability Scoring System (CVSS) Implementation Guidance 7946
ODHS|OHA 090-006-01 Information Security Risk Assessment Process
ODHS|OHA 090-006-02 Information Security Risk Assessment Process Map
ODHS|OHA 090-006-03 Continuous Vulnerability Management Process

[2] 2019 Statewide Information and Cyber Security Standards, Risk Assessment (RA)-5

ODHS|OHA 090-006-04 Continuous Vulnerability Management Process Map
45 CFR 164
Oregon Administrative Rules (OAR) 125-055-0100 to 125-055-0130
OAR 943-014-0400 to 943-014-0465
Oregon Revised Statute (ORS) 192.355
Criminal Justice Information Services (CJIS) Security Policy
Federal Information Processing Standards (FIPS) Publication (Pub) 199
Gartner, Improve IT Security With Vulnerability Management, G00127481
IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies
MARS-E Document Suite, Version 2.0, Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges
Social Security Administration Information Exchange Security Requirements and Procedures
Statewide Information and Cyber Security Standards 2019
Statewide Information Security Plan
Center for Internet Security (CIS) Controls

Related policies

DAS 107-004-052 Cyber and Information Security
DAS 107-004-120 Cyber and Information Security Incident Response
ODHS|OHA 070-015 Technology Change Management Policy
ODHS|OHA 090-005 Information Security Incident Management
ODHS|OHA 090-006 Information Security Risk Assessment Policy
OHA 100-014 Report and Response to Privacy and Security Incidents

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

Contact

Information Security and Privacy Office (ISPO)
Security 503-945-6812
Dhsinfo.security@state.or.us

Policy history

Version 1 DHS|OHA-090-007 established 06/05/2017
Version 2 revised 05/07/2018
Version 3 ODHS|OHA 090-007 revised 06/07/2021

Keywords

Confidentiality, Cyber Security Services, CSS, Data Center Services, DCS, Enterprise Information Services, EIS, information technology, integrity, patch, patch management, risk assessment, vulnerabilities, scan, security, vulnerability analysis

---

This document can be provided upon request in an alternate format for individuals with disabilities or in a language other than English for people with limited English skills. To request this document in another format or language, contact the Publications and Design Section at 503-378-3486, 7-1-1 for TTY, or email dhs-oha.publicationrequest@state.or.us.