Operational Policy

Policy title:	Information Technology Vulnerability Management Policy		
Policy number:	ODHS|OHA 090-007		
Original date:	06/05/2017	**Last update:**	06/05/2023
Approved:	Kris Kautz, Deputy Director OHA Seth Lyon, COO ODHS		

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 all software and systems including third party applications. operating systems, and any other systems not developed internally.

Description

This policy applies to all information systems and applications of ODHS and 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

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

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, software, system security procedures, internal controls, or implementations that can be exploited or triggered by a threat source.
2. To address security vulnerabilities, the Office of Information Services (OIS) shall run automated vulnerability scans of assets using a security content automation protocol compliant vulnerability scanning tool on all ODHS and OHA information systems and applications according to the Statewide Cyber Security Standards.
    a. For systems that are not managed internally by the agency, the external vendors shall be required to prove ongoing vulnerability scans are completed.
    b. Systems that are managed internally by the agency shall establish and maintain a secure application development process.
3. Vulnerability scans of information systems and applications shall occur based on any of the following criteria:
    a. Best practices, or statutory and regulatory requirements.
    b. When significant or major changes are made to the environment including new infrastructure, applications, websites, upgrades, 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 Enterprise Information Services (EIS) Cyber Security Services (CSS) and the agency Chief Information Risk Officer (CIRO).
4. A risk-based remediation strategy shall be established, maintained, documented, and reviewed at least monthly by the Information Security and Privacy Office (ISPO).
5. OIS shall remediate software and operating system vulnerabilities through automated patch management at least monthly.
6. Where appropriate, OIS, ODHS and 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 and OHA.
    b. Remediated vulnerabilities are retested to verify patches and other mitigations were effective.
7. ODHS and OHA issued mobile devices, desktops, laptops, and tablets that have not received required patches through OIS shall be evaluated by ISPO in coordination with OIS Customer Service and Support (CSS), and as appropriate, other agency programs.
8. When vulnerabilities are identified and cannot be resolved, the MSC 3489 Risk Exception Request Form shall be completed.

a. The risk owner, such as the information system owner, program director, or higher, shall describe the vulnerability, its potential impact, and the justification for risk acceptance on the MSC 3489.
b. The risk owner signs and submits the form to ispo.inforisk@odhsoha.oregon.gov.
c. The ISPO Risk Management Team assesses the risk and collaborates with the risk owner to ensure the risk and any compensating controls have been evaluated.
d. The Chief Information Risk Officer (CIRO) shall review, and if approved, sign the form.

9. After the MSC 3489 has been approved, the risk owner shall:
   a. Collaborate with ISPO Risk Management Team to add the vulnerabilities to the risk register.
   b. Collaborate with ISPO to determine the next steps for the remediation plan.
   c. Implement compensating controls to mitigate risk.
10. ISPO shall review the following at least every ninety days:
   a. The unmitigated vulnerabilities in the risk register.
   b. The exception and risk determination are still justified.

References

Microsoft SecurityTech Center Security Bulletin Severity Rating System, GG309177
National Institute of Standards and Technology (NIST) 800-30 Rev. 1 Guide for Conducting Risk Assessments
NIST SP 800-40 Rev. 4 Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology
NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations
NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide
NIST SP 800-115 Technical Guide to Information Security Testing and Assessment
NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
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
ODHS|OHA 090-006-04 Continuous Vulnerability Management Process Map
45 CFR 164 Security and Privacy
Oregon Administrative Rules (OAR) 125-055-0100 to 125-055-0130 State Purchasing
OAR 943-014-0400 to 943-014-0465 Privacy and Confidentiality
Oregon Revised Statute (ORS) 192.355 Public Records Exempt from Disclosure

Criminal Justice Information Services (CJIS) Security Policy
Federal Information Processing Standards (FIPS) Publication (Pub) 199 Standards for Security Categorization of Federal Information and Information Systems
Gartner, Improve IT Security with Vulnerability Management, G00127481
IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies
Minimum Acceptable Risk Safeguards for Exchanges (MARS-E) Document Suite Volume I Harmonized Security and Privacy Framework Version 2.2
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

Forms

MSC 3489 Risk Exception Request Form

Related policies

DAS 107-004-052 Cyber and Information Security
DAS 107-004-120 Cyber and Information Security Incident Response
ODHS|OHA 070-015 Information 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

Office of Information Services
Service Desk: 503-945-5623
OIS.ServiceDesk@odhsoha.oregon.gov

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
Version 4 ODHS|OHA 090-007 revised 06/05/2023

Keywords

Information technology, patch, patch management, risk, risk management, risk register, scan, security, vulnerability, vulnerabilities

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.