SHARED SERVICES
Office of Information Services
Information Security and Privacy Office

Operational Policy

Policy title:	Information Technology Vulnerability Management Policy		
Policy number:	DHS|OHA-090-007		
Original date:	06/05/2017	**Last update:**	Rev. 05/07/2018
Approved:	Don Erickson, DHS Deputy Administrative Officer, Kris Kautz, OHA Deputy Director		

Purpose

The Office of Information Services (OIS) is committed to implementing and maintaining a vulnerability management program for the Department of Human Services (DHS) and the Oregon Health Authority (OHA) that protects information assets and systems, mitigates vulnerabilities, and reduces the risk of malicious activity.

Description

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

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

Policy

1. Vulnerability assessments of information systems and applications shall occur based on any of the following criteria:
   a. As needed based on best practices, or statutory and regulatory requirements.
   b. When new public facing websites are created.
   c. When significant or major changes are made to the environment including new infrastructure or applications, 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.
   d. At the discretion of the Chief Information Risk Officer (CIRO).
2. The Chief Information Officer (CIO) has delegated the CIRO as the primary approver for vulnerability assessments.
3. Whenever a vulnerability assessment is performed, a vulnerability score shall be calculated using the NIST National Vulnerability Database Common Vulnerability Scoring System Support criteria:
   a. Critical (9-10): A vulnerability whose exploitation could allow code execution without user interaction. These scenarios include self-propagating malware (e.g. network worms), or unavoidable common use scenarios where code execution occurs without warnings or prompts. This could mean browsing to a web page or opening email.
   b. High (7-8.9): A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of user data, or of the integrity or availability of processing resources. These scenarios include common use scenarios where an individual is compromised with warnings or prompts regardless of the prompt's origin, quality, or usability. Sequences of user actions that do not generate prompts or warnings are also covered.
   c. Medium (4-6.9): Impact of the vulnerability is mitigated to a significant degree by factors such as authentication requirements or applicability only to non-default configurations.
   d. Low (0.1-3.9): Impact of the vulnerability is comprehensively mitigated by the characteristics of the affected component.23

4 When a vulnerability is identified, the information system owner shall:
   a. Take appropriate action such as patching or updating the information system; or
   b. Implement compensating security controls to address identified risks.

5. The Information Security and Privacy Office (ISPO) shall collaborate with OIS, appropriate DHS|OHA programs, information system owners, and Enterprise Technology Services (ETS), as required, to ensure:
   a. Deployment of patches and other vulnerability remediation practices are completed in a timely manner.
   b. All patches are evaluated for risk and impact to DHS|OHA, and approved before they are installed on production systems in accordance with DHS|OHA-070-015.
   c. The risk associated with exceptions from patching shall be approved and documented.
   d. Patch deployment is performed by authorized individuals.
   e. Vulnerabilities remediated during the assessment are retested to verify the corrections.
6. DHS|OHA issued mobile devices, desktops, laptops, and tablets which have not received required patches through OIS, shall not be used for DHS|OHA business.
7. Vulnerabilities identified in software that cannot be patched because it is no longer supported or maintained by the vendor shall:

   a. Be remediated with documented controls.
   b. Removed from production; or
   c. Have the risks associated with exceptions from patching approved and documented.
8. DHS|OHA shall follow all agency, state, and federal laws and requirements to include all applicable Oregon Department of Administrative Services statewide policies.

References

Microsoft SecurityTech Center Security Bulletin Severity Rating System, GG309177
National Institute of Standards and Technology (NIST) 800-30 Rev. 1
NIST 800-37 Rev. 1
NIST 800-39
NIST 800-40 Rev. 3
NIST 800-53 Rev. 4
NIST 800-61 Rev. 2
NIST 800-115
NIST 800-128
NIST 800-137
NIST National Vulnerability Database (NVD) Common Vulnerability Scoring System (CVSS) Support v3.0 Specification (v1.7)
NIST Internal Report (IR) Common Vulnerability Scoring System (CVSS) Implementation Guidance 7946
DHS|OHA-090-006-01 Information Security Risk Assessment Process
DHS|OHA-090-006-02 Information Security Risk Assessment Process Map
DHS|OHA-090-006-03 Vulnerability Assessment Process
DHS|OHA-090-006-04 Vulnerability Assessment Process Map
45 CFR 164
OAR 125-055-0100 to 125-055-0130
OAR 943-014-0400 to 943-014-0465
Criminal Justice Information Systems Security Standards (CJIS)
Federal Information Processing Standards (FIPS) Publication (Pub) 199
Federal Information Processing Standards (FIPS) Publication (Pub) 200
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
2017 Statewide Security Standards

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-070-015 Technology Change Management Policy
DHS|OHA-090-005 Information Security Incident Management
DHS|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 relevancy.

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

Keywords

Confidentiality, information technology, integrity, patch, patch management, risk assessment, vulnerabilities, scanning, 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.