Operational Policy

Policy title:	Configuration Management Policy		
Policy number:	ODHS|OHA 070-002		
Original date:	02/07/2022	**Last update:**	02/07/2022
Approved:	Kris Kautz, OHA Deputy Director Don Erickson, ODHS Chief Administrative Officer		

Purpose

The purpose of this policy is to establish, implement, and actively manage configuration management controls that safeguard the confidentiality, integrity, and availability of information systems.

Description

This policy outlines the requirements for effective configuration management for hardware, software, and applicable documentation that may impact ODHS|OHA's network performance, operations, and security.

Applicability

This policy applies to all ODHS|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. ODHS|OHA shall establish configuration management practices for authorized operating systems and software in compliance with state and federal requirements for items within the agency's scope of control.
   a. Configuration management is a collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.[1]
   b. Configuration management includes establishing, implementing, and actively managing the security configuration of all configuration items, including endpoints such as mobile devices,

[1] National Institute for Standards and Technology (NIST) Special Publication (SP) 800-128

laptops, servers, and workstations, in order to prevent attackers from exploiting vulnerable services and settings.

2. ODHS|OHA shall maintain documented security configuration standards as set by the Enterprise Information Services (EIS) Cyber Security Services (CSS).
   a. A baseline configuration is a set of specifications for a system, or configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for current and future builds, releases, and changes. [2]
   b. A configuration item is an identifiable part of a system such as hardware, software, firmware, documentation, or a combination thereof, that is a discrete target of configuration control processes.[3]
3. ODHS|OHA shall review the configuration standards at least annually according to the EIS Statewide Cyber Security Standards.
4. ODHS|OHA staff performing an approved and authorized change to a configuration item shall be responsible for following both the Office of Information Services (OIS) Configuration Management Process and the OIS Change Management Process to maintain the integrity and accuracy of the configuration management system.
5. Exceptions to baseline security shall be obtained through completion of the MSC 3489 Risk Exception Request Form.

References

National Institute of Standards and Technology (NIST) Special Publications (SP) 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations

NIST SP 800-128 Guide for Security-Focused Configuration Management of Information Systems

Criminal Justice Information Systems Security Policy (CJIS)

Internal Revenue Service (IRS) Publication 1075, Tax information Security Guidelines for Federal, State and Local Agencies

OIS Configuration Management Process

OIS Approved Configuration Management Database

Center for Internet Security Top Twenty Critical Security Controls

Statewide Information and Cyber Security Standards 2019

Statewide Information Security Plan

OIS Change Management Process

Forms

MSC 3489 Risk Exception Request Form

Related policies

DAS 107-004-052 Cyber and Information Security

Contact

Office of Information Services

Service Desk: 503-945-5623

[2] NIST SP 800-128

[3] NIST SP 800-128

OIS.servicedesk@dhsoha.state.or.us

Policy history

Version 1 ODHS|OHA 070-002 established 02/07/2022

Keywords

Baseline configuration, configuration item, configuration management, configuration management data set, information, technology

---