# Operational Policy

| | | | |
|---|---|---|---|
| **Policy title:** | Information Technology Risk Management Policy | | |
| **Policy number:** | ODHS\|OHA 090-016 | | |
| **Original date:** | 06/06/2022 | **Last update:** | 06/06/2022 |
| **Approved:** | Kris Kautz, OHA Deputy Director<br>Don Erickson, ODHS Chief Administrative Officer | | |

## Purpose

The Oregon Department of Human Services (ODHS) and the 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 this policy is to ensure and foster the practice of risk-based decision-making processes for ODHS and OHA information assets and systems.

## Description

This policy establishes the framework for the agency's information technology risk management program which includes risk assessment, risk response, and risk monitoring.

## Applicability

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

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 best possible measures to safeguard the confidentiality, integrity, and availability of all protected information.
2. ODHS and OHA, through the Information Security and Privacy Office (ISPO), shall develop and implement an ODHS|OHA Information Technology Risk Management Plan. The plan shall:
   a. Define roles and responsibilities for information security risk management within ODHS|OHA.
   b. Establish an information security risk governance body.

c. Establish and implement a risk management framework.[1]
d. Ensure that information security risk findings are included in the strategic decision-making processes for information assets and systems.
e. Develop and maintain processes to identify, assess, and continually monitor information security risk.
f. Implement a risk triage process for the determination of the appropriate level of mitigation for each information security risk.
g. Establish and maintain an ODHS|OHA Information Security Risk Register to track risk owners, and prioritize and monitor risks.

3. The ODHS|OHA risk owners with outstanding items on the ODHS|OHA Information Security Risk Register shall provide updates at least quarterly to the Risk Management Team.
4. The Risk Management Team shall review and update the ODHS|OHA Information Technology Risk Management Plan every two years or when significant changes occur in the business environment.

**References**

45 CFR 160 General Administrative Requirements

45 CFR 164 Security and Privacy

Criminal Justice Information Services (CJIS) Security Policy

Internal Revenue Service (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

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 Rev. 1 Guide for Conducting Risk Assessments

NIST SP 800-37 Rev. 2, Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach

NIST SP 800-39, Managing Information Security Risk

NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations

NIST White Paper: Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 16, 2018

NIST Interagency Report 8170 Approaches for Federal Agencies to Use the Cybersecurity Framework

Social Security Administration (SSA) Electronic Information Exchange Partner Technical System Security Requirements

2019 Statewide Information and Cyber Security Standards

ODHS|OHA Agency Information Security Plan

ODHS|OHA 090-006-01 Information Security Risk Assessment Process

ODHS|OHA 090-006-02 Information Security Risk Assessment Process Map

[1] National Institute of Standards and Technology (NIST) Special Publications (SP) 800-37 Rev. 2

ODHS|OHA Information Technology Risk Management Plan

**Forms referenced**
MSC 3489 Risk Exception Request Form

**Related Policies**
ODHS|OHA 090-006 Information Security Risk Assessment Policy

**Contact**
Information Security and Privacy Office (ISPO)
Phone: 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 relevance.

**Policy history**
Version 1 OHDS|OHA 090-016 established 06/06/2022

**Keywords**
Risk, risk assessment, risk management, risk management plan, risk register

---