Process

Title:	ODHS|OHA 090-002-09 Information System Audit and Monitoring Process
Related to:	Statewide Information and Cyber Security Standards
Effective date:	04/05/2021

Purpose

The Oregon Department of Human Services (ODHS) and the Oregon Health Authority (OHA) ensure auditable events[1] are recorded, reviewed, and monitored for information systems and applications.

The requirements contained herein comply with the Statewide Information and Cyber Security Standards developed by the Oregon Office of the State Chief Information Officer (OSCIO) and align with the Center for Internet Security's CIS Controls™. Agencies are responsible for complying with these standards to meet the requirements for information system and organizational operations within the State of Oregon.

Applicability

This process applies to all ODHS and OHA staff including employees, volunteers, trainees, 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.

Process Steps

1. Agency system owners[2] configure information systems to generate audit records for auditable events in accordance with those listed in the Statewide Information and Cyber Security Standards. Agency system owners are accountable for:
   a. Procurement, development, integration, modification, or operation and maintenance of an information system.
   b. Ensuring that system users and support personnel receive the requisite security training.
   c. Assisting in the identification, implementation, and assessment of information classification, security requirements, and the common security controls.

[1] Auditable events are listed in the Statewide Information and Cyber Security Standards 2019 AU-2, AU-3 and AU-12.
[2] Annual Agency Information Security Plan

2. Agency system owners, in conjunction with the Office of Information Services (OIS), review, update, and approve a list of auditable events at least annually or when a major change to the system occurs, and disseminates the list to applicable staff.
3. Automated mechanisms are employed to integrate audit review, analysis, and reporting to support organizational processes for investigation and response to suspicious activities. Information systems:
    a. Aggregate logs to a central log management system for analysis and review.
    b. Provide and support near real-time audit review, analysis, and reporting requirements and after the fact investigations of security incidents.
    c. Send malware detection events to anti-malware administration tools and centralized log servers for alerting and analysis.
    d. Ensure the audit reduction and report capability is tuned on a regular basis in order to better identify actionable events and decrease event noise.
    e. Do not alter the original content or time ordering of audit records.
    f. Use internal system clocks to generate time stamps for audit records.
4. Agency system owners review and analyze system audit records at least weekly across different repositories to gain agency-wide situational awareness including a review of the following:
    a. Indications of inappropriate or unusual activity related to potential unauthorized access.
    b. Other anomalies or abnormal events.
    c. Events of interest based on individual or a combination of items contained in the audit records.
5. Incidents discovered during audit record review and analysis are reported by agency system owners according to agency, state and federal requirements. (Refer to ODHS|OHA 090-005-01)
6. When there is an audit processing failure, an alert is generated to OIS and system administrators who:
    a. Take appropriate action to address the restoration of logging functionality immediately upon discovery; and
    b. Ensure that information systems receiving, processing, or storing regulated data comply with applicable laws and regulations, specific to the system.
7. Agency system owners are responsible for protecting audit information and audit tools from unauthorized access, modification, and deletion.
8. When transmitting information across agency boundaries, agencies use information systems and services of external organizations to coordinate the access and protection of audit information.
9. Agency system owners are responsible for ensuring sufficient audit record storage capacity including:
    a. Providing a warning to designated agency staff when allocated audit record storage volume reaches 80 percent utilization, or as specified by regulations specific to the system.
    b. Retaining audit records in accordance with state and federal rules and requirements to provide support for after-the-fact investigations of information technology security incidents.

References

45 CFR 160 & 164

Oregon Administrative Rule 166-300-0030

OAR 943-014-0400 to 943-014-0465

Center for Internet Security Top Twenty Critical Security Controls

MARS-E Document Suite, Version 2.0, Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges
Criminal Justice Information Systems Security Standards (CJIS)
Federal Information Processing Standards (FIPS) Publication (Pub) 199
Federal Information Processing Standards (FIPS) Publication (Pub) 200
IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies
National Institute of Standards and Technology (NIST) 800-53 Rev. 5
Social Security Administration Information Exchange Security Requirements and Procedures
5 U.S.C §552a(c) Accounting of Certain Disclosures
Statewide Information and Cyber Security Standards 2019
Annual Agency Information Security Plan
ODHS|OHA 090-002-08 Information System Audit and Monitoring Process Map
ODHS|OHA 090-005-01 Information Security Incident Reporting Process

Related policies
DAS 107-004-052 Information Security
DAS 107-004-050 Information Asset Classification Policy
ODHS|OHA 090-003 Access Control Policy
ODHS|OHA 090-004 Information Security and Privacy Awareness and Training Policy
ODHS|OHA 090-005 Information Security Incident Management Policy
ODHS|OHA 090-006 Information Security Risk Assessment Policy
ODHS|OHA 090-009 Physical, Administrative and Technical Safeguards Policy

Contact
Information Security and Privacy Office
Security 503-945-6812
Dhsinfo.security@dhsoha.state.or.us

Guidelines/Process history
Version 1 ODHS|OHA 090-002-07 Guidelines established 11/5/2018
Version 2 ODHS|OHA 090-002-07 Revised as process 04/05/2021

Keywords
Agency system owner, audits, audit record, events, logs, monitoring, security monitoring, storage

---