Guidelines

Title:	DHS|OHA 090-002-07 Information System Audit and Monitoring Guidelines
Related to:	Statewide Information Security Plan
Effective date:	11/5/2018

Purpose

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

Guidelines

1. Information system owners, in conjunction with the Office of Information Services (OIS), should review, update, and approve a list of auditable events within every 365 days, and disseminate the list of auditable events to applicable staff.
2. Information systems should record auditable events based on a risk assessment, mission or business needs, and/or applicable agency, state, and federal laws and requirements.
3. DHS|OHA should implement audit review, analysis, and reporting processes to ensure appropriate system use. These processes should include:
   a. Consistent use of automated mechanisms for indications of inappropriate or unusual activity.
   b. Analysis of vulnerability scanning information, information system performance data, and network monitoring information to identify inappropriate or unusual activity.
4. DHS|OHA should, at a minimum and where technically feasible, ensure audit logs are configured to include, but may not be limited to, the following auditable events:
   a. System shutdown and reboot
   b. Log onto and off system
   c. Change of password
   d. All system administrator commands, while logged on as system administrator
   e. Clearing of the audit log file
   f. Use of identification and authentication mechanisms
   g. Change of file or user permissions or privileges
   h. Date and time of the event
   i. Source and destination of the event
   j. Type of event

[1] "Auditable event" is an observable occurrence that is significant and relevant to the security of information systems and the environments in which those systems operate to meet specific and ongoing audit needs. *National Institute of Standards and Technology (NIST) 800-53 Rev. 4*

k. Outcome of the event

5. DHS|OHA should also ensure audit logs include the following additional auditable events:
   a. Verify that proper logging is enabled to audit administrator activities
   b. Server alerts and error messages
   c. Switching accounts or running privileged actions from another account, (e.g., Linux/Unix SU or Windows RunAs)
   d. Creation or modification of super-user groups
   e. Subset of security administrator commands, while logged on in the security administrator role
   f. Subset of system administrator commands, while logged on in the user role
   g. Startup and shutdown of audit functions
   h. Remote access outside of the corporate network communication channels (e.g., modems, dedicated VPN) and all dial-in access to the system
   i. Changes made to an application or database by a batch file
   j. Application-critical record changes
   k. Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility)
   l. System errors
   m. Application shutdown
   n. Application restart
   o. Application errors
   p. Security policy modifications
   q. Printing sensitive information
6. DHS|OHA should enable logging for perimeter devices, including firewalls and routers to include:
   a. User log-on and log-off (successful or unsuccessful)
   b. Log packet-screening denials originating from untrusted networks
   c. All system administration activities
   d. Packet-screening denials originating from trusted networks
   e. Account creation, modification, or deletion of packet filters
   f. System shutdown and reboot
   g. System errors
   h. Modification of proxy services
7. Information systems should generate alert notification for technical personnel review and assessment.
8. DHS|OHA should:
   a. Inspect administrator groups on demand but at least once every fourteen (14) days to ensure unauthorized administrator accounts have not been created.
   b. Review and analyze audit logs for inappropriate or unusual activity randomly but at least once every thirty (30) days or as required.
   c. Adjust the level of audit review, analysis, and reporting within the information system when there is a change in the threat environment including operations, asset, individuals, other organizations, or the Nation, based on law enforcement information, intelligence information, or other credible sources of information.
9. DHS|OHA should coordinate with the Office of Information Services (OIS) to:

a. Ensure audit logs storage capacity is available online for at least ninety (90) days.
b. Ensure audit logs are archived for ten (10) years to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

10. The information system should provide a warning when allocated audit record storage volume reaches maximum capacity.
11. Processes should be developed for sharing audit information with external organizations.
12. DHS|OHA should keep an accurate accounting of certain disclosures[2]:
    a. Keep an accurate accounting of the date, nature, and purpose of each disclosure of a record to any person/entity or other agency, and the name and address of the person/entity or agency to whom the disclosure is made.
    b. Retain the accounting for at least five (5) years or the life of the record, whichever is longer, after the disclosure for which the accounting is made,
    c. Make the accounting available to the individual named in the record at their request.
    d. Inform any person/entity or other agency about any correction or notation of dispute made by the agency of any record that has been disclosed to the person or agency if an accounting of the disclosure was made.

References

45 CFR 160 & 164
OAR 125-055-0100 to 125-055-0130
OAR 943-014-0400 to 943-014-0465
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. 4
Social Security Administration Information Exchange Security Requirements and Procedures
5 U.S.C §552a(c) Accounting of Certain Disclosures
Statewide Information Security Standards 2017
Statewide Information Security Plan 080118

Related policies

DAS 107-004-052 Information Security
DHS|OHA 010-014 Agency Compliance with Statewide Administrative Policy
DHS|OHA 090-003 Access Control Policy
DHS|OHA 090-004 Information Security and Privacy Awareness and Training Policy
DHS|OHA 090-005 Information Security Incident Management Policy

[2] "Disclosure" means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information. *45 Code of Federal Regulations Part 160*

DHS|OHA 090-006 Information Security Risk Assessment Policy
DHS|OHA 090-009 Physical, Administrative and Technical Safeguards Policy

Contact

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

Guidelines history

Version 1 DHS|OHA 090-002-07 established 11/5/2018

Keywords

Audits, audit record, events, logs, monitoring, security monitoring, storage

---