Guidelines

Title:	DHS|OHA-090-003-03 Information System Maintenance Guidelines
Related to:	DHS|OHA-090-003 Access Control Policy
Effective date:	10/24/16

Purpose

The Department of Human Services (DHS) and the Oregon Health Authority (OHA) are committed to having information system security controls in place for maintenance, diagnostic, and repair activities. DHS and OHA authorized staff including contractors and partners who conduct maintenance, diagnostic, and repair activities, whether performed local (onsite) or non-local (offsite or remote) maintenance, are required to follow these guidelines.

Guidelines

1. The Office of Information Services (OIS), through the Chief Information Officer (CIO) or designee, authorizes maintenance and diagnostic activities (local and non-local) performed on DHS and OHA information systems in compliance with the documented security plan for the information system and DHS and OHA policies and processes.
2. OIS is responsible for approving, controlling, and monitoring as appropriate, maintenance and diagnostic activities performed by authorized staff including contractors and partners.
3. Authorized staff shall follow these requirements for maintenance:
   a. Schedule, perform, document, and review records of maintenance and repairs on information system components in accordance with the manufacturer or vendor specifications and DHS and OHA policies and processes.
   b. Approve and monitor all maintenance activities performed, whether the equipment is serviced onsite or removed to another location.
   c. Perform maintenance inside of designated change management windows as required by DHS|OHA-070-015 and DHS|OHA-070-015-01.
   d. Send notification of date and time of planned maintenance to DHS and OHA system administrators, database administrators and application administrators in accordance with DHS|OHA-070-015-01.
   e. Obtain approval from the CIO or designee for removal of the information system or system components from the facility if necessary for off-site maintenance or repair.
   f. Inspect and sanitize equipment to remove all sensitive information from associated media prior to removal from facility for off-site maintenance or repair.
   g. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.
   h. Document any security related repairs and modifications to the physical components of the buildings.

4. In addition to the maintenance requirements, non-local maintenance and diagnostic activities performed by authorized staff should include:
    a. Implementing a level of security at least as high as that implemented on the system being serviced including cryptographic mechanisms to protect the integrity and confidentiality of remote maintenance and diagnostic communications.
    b. Using strong identification and authentication techniques such as multi-factor authentication in compliance with the requirements of the specified system.
    c. Utilizing encryption for secure communication in compliance with the requirements of the specified system.
    d. Utilizing privileged access management process for those authorized to conduct the remote maintenance and diagnostic activities as required.
    e. Verifying remote maintenance was disconnected including all sessions and network connections.
    f. When hardware must be taken off-site for maintenance or repair, inspecting and sanitizing the components for potentially malicious software and unauthorized implants before removal from the facility, and before reconnecting the component to the information system.
    h. If password-based authentication is used, changing the passwords following each maintenance session as required by the security protocols of the specified system.
5. For completed maintenance activities, audit logs shall be:
    a. Closely monitored and documented as required by the security protocols of the specified system.
    b. Archived following the record retention rules and schedules, and the security protocols of the specified system.

References

45 CFR 160 & 164
MARS-E Document Suite, Version 2.0, Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges
Criminal Justice Information Systems (CJIS) Security Policy
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
DAS 107-08-PRC330 Enterprise Technology Services Internal Process, Information System Maintenance
DHS|OHA-070-015-01 Technology Change Management Process
DHS|OHA-090-003-02 Privileged Access and Management Process

Forms referenced

Related policies

DAS 107-08-240 DAS Enterprise Technology Services Internal Policy, Information System Maintenance Policy

DAS 107-004-052 Information Security

DHS|OHA-070-015 Technology Change Management

DHS|OHA-090-001 General Security

DHS|OHA-090-002 Information System Audit and Monitoring Policy
DHS|OHA-090-003 Access Control
DHS|OHA-090-005 Security Incident Management
DHS|OHA-090-006 Risk Assessment

Contact
Information Security and Privacy Office
Security: 503-945-6812
Fax: 503-947-5396
Dhsinfo.security@state.or.us

History
Version 2 DHS|OHA 10/24/16
Version 1 DHS|OHA established 10/30/15

Keywords

Audit logs, authentication, communications, cryptographic, diagnostic, encryption, maintenance, non-local, password, privileged access, remote, sanitize

---

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.