Operational Policy

Policy title:	Information System Maintenance Policy		
Policy number:	ODHS|OHA 090-012		
Original date:	06/06/2022	**Last update:**	06/06/2022
Approved:	Kris Kautz, Deputy Director OHA Don Erickson, Chief Administrative Officer ODHS		

Purpose

The Oregon Department of Human Services (ODHS) and the Oregon Health Authority (OHA) are responsible for the establishment and implementation of information system controls that safeguard the confidentiality, integrity, and availability of information systems. This policy addresses security concerns by managing risks from information asset maintenance and repairs through the establishment of an effective information system maintenance program.

Description

This policy outlines the requirements for maintenance of information systems and information system components of ODHS and OHA.

Applicability

This policy applies to all ODHS|OHA staff and those partners and contractors using ODHS|OHA approved maintenance tools.

As keepers of the public trust, all agency employees have a responsibility to comply with state and agency policies, administrative rules, and state and federal laws. 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. Information system maintenance refers to the processes needed to sustain a product, system, or service, keeping it relevant and valuable throughout its life cycle.
2. This policy shall apply to all information systems and information system components that are managed by, or managed for, ODHS and OHA including:
   a. Mainframes, servers, and other devices that provide centralized computing capabilities.
   b. Devices that provide centralized storage capabilities.
   c. Desktops, laptops, and other devices that provide distributed computing capabilities. This includes multiple computer systems working on a single problem.
   d. Mobile communication devices.

e. Routers, switches, and other devices that provide network capabilities.
f. Firewalls, intrusion detection and prevention (IDP) sensors, and other devices that provide dedicated security capabilities.

3. ODHS|OHA programs with information technology (IT) systems in the agency's infrastructure shall adhere to applicable requirements for maintaining those systems.
4. The Office of Information Services (OIS), through the Chief Information Officer (CIO) or designees, shall authorize, approve, control, and monitor maintenance and diagnostic activities performed on or offsite on ODHS and OHA information systems.
5. The information system owner or designee shall approve the removal of information systems or information system components for off premises maintenance, repair, or replacement.
6. Only authorized staff shall schedule, perform, document, and review records of maintenance and repairs on information system components in accordance with manufacturer, vendor, or partner specifications and organizational requirements. Authorized staff shall:
   a. Send notification of the date, time, and description of the planned maintenance activity to ODHS|OHA information system owners in accordance with the ODHS|OHA 070-015 Information Technology Change Management Policy.
   b. Coordinate and follow maintenance activities inside of designated change management windows as required by ODHS|OHA 070-015 and the OIS Change Management Process.
   c. Monitor vendor and partner changes that have potential to impact the ODHS|OHA information systems environment.
   d. Coordinate with OIS Information Technology Asset Management (ITAM) to complete activities necessary for repair, dependent upon the warranty coverage of the device.
7. Only authorized staff or technicians accompanied by authorized staff, shall have access to agency information systems.
8. Associated media containing protected data shall be handled in accordance with applicable state and federal requirements. Associated media includes those components not directly associated with information processing or data and information retention such as scanners, copiers, and printers.
9. Remote access for vendor maintenance shall be approved, monitored, and documented through the following:
   a. Utilize remote maintenance, diagnostic tools, and encryption consistent with organizational policy and documented in the security plan for the system.
   b. Employ strong authentication in the establishment of remote sessions.
   c. Track remote sessions through current ticketing systems for record keeping purposes.
   d. Terminate session and network connections when nonlocal maintenance is completed.
10. Maintenance tools shall be documented as part of the IT standards or approved IT standard exceptions.
    a. The use of maintenance tools shall be restricted to authorized staff.
    b. Maintenance tools shall have current patches and updates installed.
11. Maintenance logs shall be maintained for mission and business critical systems, and such logs shall be maintained in accordance with record retention requirements.

References

Center for Internet Security Top Twenty Critical Security Controls

Minimum Acceptable Risk Safeguards for Exchanges (MARS-E) Volume 1: Harmonized Security and Privacy Framework Version 2.2

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

NIST SP 800-82 Rev. 2 Guide to Industrial Control Systems (ICS) Security

Oregon Administrative Rules (OARs) 166-300-0030(1) Information and Records Management Records

Statewide Information and Cyber Security Standards 2019

OIS Change Management Process

OIS IT Standards and Approved Products List

Related policies

DAS 107-004-110 Acceptable Use of State Information Assets

ODHS|OHA 070-015 Information Technology Change Management Policy

ODHS|OHA 090-009 Administrative, Technical and Physical Safeguards of Information Policy

This policy shall be reviewed at least once every year to ensure relevance.

Contact

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

History

Version 1 ODHS|OHA 090-012 established 06/06/2022

Keywords

Equipment, information system maintenance, local maintenance, maintenance, nonlocal maintenance, remote maintenance

---