Operational Policy

Policy title:	**Administrative, Technical and Physical Safeguards of Information Policy**		
Policy number:	ODHS|OHA 090-009		
Original date:	11/08/2004	**Last update:**	08/02/2021
Approved:	Kris Kautz, OHA Deputy Director, Don Erickson, ODHS CAO		

Purpose

The Oregon Department of Human Services (ODHS) and Oregon Health Authority (OHA) are committed to protecting the information assets and systems of the agencies. The purpose of this policy is to establish criteria for safeguarding protected information and to minimize the risk of unauthorized access, use, or disclosure.

Description

This policy describes the responsibility of ODHS|OHA staff to maintain the security of and manage risks for information assets and systems during day-to-day workplace practices. This includes ensuring awareness of information that may be disclosed in documents and conversations, the security of workplace surroundings, and the protection of information taken out of the worksite.

Applicability

This policy applies to all ODHS|OHA staff including employees, volunteers, and 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. Contractors and partners may face termination of the working relationship as well as federal sanctions.

Policy

1. ODHSIOHA shall take physical, technical, and administrative steps to protect information assets and systems from unauthorized access. An information asset is any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics that has value to the organization.
2. ODHS|OHA shall protect agency-owned physical and digital media including, but not limited to, the storage, accessibility, and transportation of protected information, personally identifiable information (PII), protected health information (PHI), federal tax information (FTI), Criminal Justice Information (CJI), or Social Security Administration (SSA) information.

3. ODHS|OHA shall monitor staff use of ODHS|OHA desktops, laptop computers, and mobile computing devices.
4. Information systems managed by agency, Enterprise Information Services (EIS), and hosted service providers, shall provide secure installations, configurations, distribution, and management for all agency-owned information assets.
5. On an annual basis, an inventory of information system components shall be developed, documented, and maintained by OIS that accurately reflects the current information system environment.
6. ODHS|OHA shall validate information system accounts on an annual basis for all ODHS|OHA systems accessing or storing CJI, FTI and SSA data, and document the validation process.
7. The ODHS|OHA Security Official shall be the Chief Information Risk Officer (CIRO) or, if that position is vacant, the ODHS|OHA Chief Information Officer (CIO) shall designate whom to fill the role. The CIRO shall:
    a. Provide guidance and oversight regarding the creation, receipt, maintenance, and transmission of electronic protected information.
    b. Develop and implement policies and processes to ensure the confidentiality, integrity, and availability of electronic protected information, and to protect against threats or hazards to the security or integrity of such information.
    c. Serve as the ODHS|OHA Security Official for concerns associated with the Health Insurance Portability and Accountability Act (HIPAA).
8. All ODHS|OHA staff shall ensure that information assets and systems are adequately shielded from unauthorized disclosure by the following:
    a. Ensuring that portable computers or other media including USB and other drives that store protected or confidential information have enabled encryption technology.
    b. Ensuring copies of documents containing protected information awaiting disposal or destruction are stored in physically secure spaces or containers.
9. ODHS|OHA staff shall screen lock agency-owned or approved personal electronic devices including computers, mobile communication devices, and other electronic devices if the devices are not in the area of the staff's immediate control.
10. ODHS|OHA staff shall not use publicly accessible computers to access, process, store, or transmit protected information.
11. When using protected information away from the ODHS|OHA work-site, staff shall comply with all work-site security requirements.
12. ODHS|OHA staff shall not:
    a. Introduce any computer code designed to self-replicate, damage or otherwise hinder the performance of agency information assets or systems.
    b. Connect non-agency owned devices such as USB drives or printers to any ODHS|OHA network, with the exception of the guest network, without prior written authorization from OIS.
13. Peripheral equipment such as printers, copiers, and fax machines shall be safeguarded from inadvertent or unauthorized access and will comply with the DAS 107-004-110 Acceptable Use of State Information Assets Policy.
14. If agency-owned computers or laptops are lost or stolen, the ODHS or OHA employee responsible for the device shall report the loss immediately to their supervisor, the OIS Service Desk, and local police department. (Refer to ODHS|OHA 090-009-03 Lost or Stolen Computer Process)
15. All emails containing confidential information shall be sent securely utilizing approved encryption standards within the email environment, except FTI which shall not be transmitted via email.
16. All protected information sent via fax shall be prepared accurately and sent securely only to authorized recipients, except FTI which shall not be transmitted via fax.

17. ODHS|OHA staff shall securely transport files and documents.
    a. ODHS|OHA staff removing agency resources from the worksite, including protected information, hard copy files, agency laptops, mobile communication devices, and other portable electronic devices, shall assure and assume responsibility for the security of the resource.
    b. ODHS|OHA staff authorized to remove protected information in hard copy from the worksite shall maintain physical custody and control of the documents or secure the documents in a locked environment.

References

Criminal Justice Information Services (CJIS) Policy
Federal Information Processing Standards (FIPS) Publication (Pub) 199
Federal Information Processing Standards (FIPS) Publication 200
IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies
MARS-E Document Suite, Version 2.0, Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges
National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 5
NIST SP 800-88
Social Security Administration Information Exchange Security Requirements and Procedures
Statewide Cyber Security Standards 2019
45 CFR 160 & 164
OAR 125-055-0100 to 125-055-0130
OAR 943-014-0400 to 943-014-0465
ODHS|OHA 090-009-03 Lost or Stolen Computer Process

Related policies

DAS 107-004-051 Controlling Portable and Removable Storage Devices
DAS 107-004-052 Cyber and Information Security
DAS 107-004-100 Transporting Information Assets
DAS 107-004-110 Acceptable Use of State Information Assets
DAS 107-004-120 Cyber and Information Security Incident Response
ODHS|OHA 060-045 Personal Use of Social Media
ODHS|OHA-070-014 Information Technology Asset Management Policy

Contact

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

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

Policy history

Version 1 DHS 090-009 established 11/08/2004
Replaced by joint policy and renamed

Version 1 DHS|OHA-090-009 established 03/11/2015
Version 2 DHS|OHA-090-009 revised 03/04/2016
Version 3 DHS|OHA-090-009 revised 02/05/2018
Version 4 ODHS|OHA revised 08/02/2021

Keywords
Administrative safeguard, authorization, access, disposal, email, federal tax information, FTI, individual, media, physical safeguard, privacy, protected information, protecting privacy, security, safeguarding, technical, technical safeguard, transport, unauthorized

---