

Operational Policy

Policy title:	Information Security and Privacy Awareness and Training Policy		
Policy number:	ODHS OHA 090-004		
Original date:	05/17/2004	Last update:	10/04/2021
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 committed to protecting the agency’s information assets and systems. The purpose of this policy is to establish and sustain an appropriate level of protection for information and technology resources through security and privacy awareness training.

Description

This policy describes the responsibilities of ODHS|OHA to ensure staff are aware and trained in information security and privacy policies and practices. It also describes the responsibility of staff to know, understand, and comply with agency, state and federal laws, and other requirements.

Applicability

This policy applies to all ODHS|OHA staff including employees, volunteers, trainees, interns, partners, and contractors.

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. ODHS|OHA staff shall guard against improper use or disclosure of protected information through awareness and training, and regularly reviewing policies.
2. ODHS|OHA shall follow the training curriculum provided by the Department of Administrative Services (DAS) for ongoing information security and privacy awareness and training program for authorized users of the agencies information assets and systems.
 - a. This training shall cover, among other things, the policies and procedures related to the protection of Protected Health Information (as defined in 45 CFR 160.103)
 - b. Providers and contractors shall follow the training curriculum provided by their agency.
3. The information security and privacy awareness and training program shall include the following:
 - a. Scheduled and unscheduled awareness assessments.
 - b. Updates and reminders.
 - c. Insider threat awareness training including:

- A. How to recognize potential indicators of insider threat; and
 - B. How to respond to suspected insider threat incidents.
- d. Additional training related to protecting agency information assets and systems.
4. Records related to information security and privacy training shall be maintained and tracked by ODHS|OHA in accordance with record retention requirements, with retention for a minimum of five years.
 5. All staff shall be aware of their responsibilities for the security and privacy of information assets and systems under agency, state and federal law and requirements.
 - a. The importance of information security and privacy and the role of staff in protecting the information in ODHS|OHA systems shall be discussed during new employee orientation.
 - b. Staff shall complete information security and privacy training within 30 days of beginning employment and refresher training on an annual basis.
 - c. ODHS|OHA managers shall ensure that all members of the agency's staff are aware of and have access to current versions of information security and privacy policies, processes, guidelines, and best practices.
 - d. ODHS|OHA managers and information system owners are responsible for ensuring staff who have access to protected information are informed of their responsibilities related to communication and storage of information regardless of format: hard copy, electronic, or audio.
 6. ODHS|OHA staff shall acknowledge they have been informed and are aware of ODHS|OHA information security and privacy policies and their role in protecting ODHS|OHA information assets and systems by signing form MSC 2400.
 7. Any user of ODHS|OHA information assets or systems who knowingly and willfully violates agency, state, or federal law and requirements for improper use or disclosure of agency held information, including personally identifiable information and protected health information, are potentially subject to criminal investigation and prosecution, civil litigation, or civil monetary penalties.
 8. All ODHS|OHA contracts shall contain language concerning awareness of information security and privacy policies and require adherence to ODHS|OHA information security and privacy policies, processes, and guidelines.
 9. Contractors, partners, business associates and other authorized users shall acknowledge their responsibilities for protecting information assets and systems through the terms of their contracts, memoranda of understanding, or other required documentation.
 10. Neither ODHS nor OHA entities or any ODHS|OHA employee shall intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against any individual for opposing, reporting, or testifying to an unlawful action or security incident.

References

[45 CFR 160 General Administrative Requirements](#)

[45 CFR 164 Security and Privacy](#)

[OAR 125-055-0100 to 125-055-0130 HIPAA Privacy and Security Rule Implementation; HITECH Act Implementation](#)

[OAR 166-300-0040\(11\) Personnel Records](#)

[OAR 407-014-0300 to 407-014-0320 Privacy and Confidentiality](#)

[OAR 943-014-0300 to 943-014-0465 Privacy and Confidentiality](#)

[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 \(Pub\) 200](#)
[Internal Revenue Service Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies](#)
[National Institute of Standards and Technology \(NIST\) Special Publication \(SP\) 800-16](#)
[National Institute of Standards and Technology \(NIST\) Special Publication \(SP\) 800-53 Rev. 5](#)
[Social Security Administration Information Exchange Security Requirements and Procedures](#)
[Statewide Information and Cyber Security Standards 2019](#)
[Statewide Information Security Plan](#)
[Center for Internet Security Top Twenty Critical Security Controls](#)

Forms referenced

[MSC 2400 ODHS|OHA Policy and Procedure Summary](#)

Related policies

[DAS 107-004-052 Information Security](#)

[DAS 107-004-053 Employee Security](#)

[OHA 100-012 Enforcement, Sanctions, and Penalties for Violations of Individual Privacy](#)

Contact

Information Security and Privacy Office (ISPO)

Phone: 503-945-6812 (Security)

503-945-5780 (Privacy)

dhsinfo.security@dhsoha.state.or.us

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

Policy history

Version 1 DHS090-004 established 05/17/2004

Replaced by joint policy

Version 1 DHS|OHA 090-004 established 3/11/15

Version 1 DHS|OHA 090-004 reviewed annually 03/04/16

Version 2 DHS|OHA 090-004 revised 12/20/2017

Version 2 DHS|OHA 090-004 reviewed annually 04/01/2019

Version 2 ODHS|OHA 090-004 reviewed annually 11/02/2020

Version 2 ODHS|OHA 090-004 reviewed annually 10/04/2021

Keywords

Annual, awareness, assets, authorized users, contracts, HIPAA, information assets, refresher, security, systems, training

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.