Operational Policy

Policy title:	Information Security Incident Management Policy		
Policy number:	ODHS|OHA 090-005		
Original date:	10/01/2004	**Last update:**	05/02/2022
Approved:	Kris Kautz, OHA Deputy Director Don Erickson, ODHS Deputy Director		

Purpose

The Oregon Department of Human Services (ODHS) and the Oregon Health Authority (OHA) are committed to reporting, analyzing, remediating, and documenting any information security incident that compromises ODHS|OHA information and systems.

Description

This policy describes the responsibility of ODHS|OHA staff to report known or suspected information security incidents. This includes, but is not limited, to incidents involving personally identifiable information (PII), protected health information (PHI), federal tax information (FTI), or Criminal Justice Information Services (CJIS) information.

Applicability

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

Policy

1. ODHS|OHA staff have a duty to immediately report known or suspected information security incidents and can do so without fear of retaliation. An information security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
2. Upon discovery of an information security incident, ODHS|OHA staff must immediately report the incident to management and the Information Security and Privacy Office (ISPO). This includes incidents relating to:
   a. Violations of ODHS|OHA policies and processes.
   b. Unauthorized access to ODHS|OHA data, information assets, or systems.
   c. Unauthorized disclosure of protected data.
3. ODHS|OHA staff shall notify ISPO of the information security incident by email, phone, or submission of the MSC 3001 form.

4. When a complaint or incident is received, ISPO shall:
   a. Work with the program or individual to investigate the incident.
   b. Document and report investigation results.
   c. Report incidents to required state and federal agencies, as required by ODHS|OHA 090-005-01.

References

45 CFR 160 General Administrative Requirements
45 CFR 164 Security and Privacy
Oregon Revised Statutes (ORS) 276A.300 Information Security
ORS 646A.600 Oregon Consumer Information Protection Act
ODHS|OHA 090-005-01 Information Security Incident Reporting Process
ODHS|OHA 090-005-02 Information Security Incident Reporting Process Workflow
ODHS|OHA 070-001-02 Lost or Stolen Mobile Communication Device
Criminal Justice Information Systems Security Standards (CJIS)
Federal Information Processing Standards (FIPS) Publication (Pub) 200
IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies
Minimum Acceptable Risk Safeguards for Exchanges (MARS-E) Document Suite Volume II: Administering Entity System Security and Privacy Plan Version 2.2
National Institute of Standards and Technology (NIST) 800-53 Rev. 5
Social Security Administration Information Exchange Security Requirements and Procedures
Statewide Information and Cyber Security Standards 2019
Center for Internet Security Top Twenty Critical Security Controls
ODHS|OHA Agency Information Security Plan
ODHS|OHA Information Security Incident Response Plan
ODHS|OHA Information Technology Risk Management Program

Forms referenced

MSC 3001 ODHS|OHA Privacy/Security Incident Report

Related policies

DAS 107-004-052 Cyber and Information Security Policy
DAS 107-004-120 Cyber and Information Security Incident Response
OHA 100-014 Report and Response to Privacy and Security Incidents

Contact

Information Security and Privacy Office (ISPO)
Phone: 503-945-6812; dhsinfo.security@dhsoha.state.or.us

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

Policy history

Version 1 DHS 090-005 established 10/01/2004
Replaced by joint policy
Version 1 DHS|OHA 090-005 established 03/11/2015
Version 2 DHS|OHA 090-005 reviewed annually 03/04/16

Version 3 DHS|OHA 090-005 revised 11/13/2017
Version 3 DHS|OHA 090-005 reviewed annually 04/01/2019
Version 3 ODHS|OHA 090-005 reviewed annually 03/01/2021
Version 3 ODHS|OHA 090-005 reviewed annually 05/02/2022

Keywords
Incident, incident management, report, response, security incident

---