Operational Policy

<table>
<thead>
<tr>
<th>Policy title:</th>
<th>Information Security Incident Management Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy number:</td>
<td>DHS</td>
</tr>
<tr>
<td>Original date:</td>
<td>10/01/2004</td>
</tr>
<tr>
<td>Last update:</td>
<td>04/01/2019</td>
</tr>
<tr>
<td>Approved:</td>
<td>Kris Kautz, OHA Deputy Director</td>
</tr>
<tr>
<td></td>
<td>Don Erickson, DHS Chief Administrative Officer</td>
</tr>
</tbody>
</table>

Purpose

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

Description

This policy describes the responsibility of DHS|OHA staff to report known or suspected information security incidents and presents an overview of the responsibilities of DHS|OHA related to investigating and reporting these incidents.

Applicability

This policy applies to all DHS|OHA staff including employees, volunteers, trainees, interns, 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. DHS|OHA staff have a duty to report known or suspected information security incidents and can do so without fear of retaliation.
2. Upon discovery of an information security incident, DHS|OHA staff shall immediately report the incident to management and the Information Security and Privacy Office (ISPO) relating to:
   a. The violation of DHS|OHA policies and processes.
   b. Impermissible access to DHS|OHA information assets or systems.
3. DHS|OHA staff shall notify ISPO of the information security incident by email, phone, or submission of the MSC 3001 form.
4. When ISPO receives an information security incident report, ISPO shall:
   a. Perform an initial assessment
   b. Investigate, document, and report on the incident as appropriate.
   c. Report incidents to required state and federal agencies as required by DHS|OHA-090-005-01.

References
45 CFR 160 & 164
OAR 125-055-0100 to 125-055-0130
OAR 943-014-0400 to 943-014-0465
DHS|OHA-090-005-01 Information Security Incident Reporting Process
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
National Institute of Standards and Technology (NIST) 800-53 Rev. 4
National Institute of Standards and Technology (NIST) 800-115
Social Security Administration Information Exchange Security Requirements and Procedures
2017 Statewide Information Security Standards
Statewide Information Security Plan
Center for Internet Security Top Twenty Critical Security Controls

Forms referenced
MSC 3001 DHS|OHA Privacy/Security Incident Report

Related policies
DAS 107-004-052 Information Security
DAS 107-004-120 Information Security Incident Response
DHS|OHA 010-014 Agency Compliance with Statewide Administrative Policy
DHS|OHA 090-005-01 Information Security Incident Reporting Process
OHA 100-013 OHA Business Associate Relationships
OHA 100-014 Report and Response to Privacy and Security Incidents

Contact
Information Security and Privacy Office (ISPO)
Phone: 503-945-6812
dhsinfo.security@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