

<b>Policy Title:</b>	Privacy and Information Security Incident Management			
<b>Policy Number:</b>	DHS-090-005	<b>Version:</b>	2.0	<b>Effective Date:</b> Upon Approval

Signature on file in the office of: Jim Neely,

01/06/10

Chief Administrative Officer

Date Approved

## Overview

**Description:** This policy addresses privacy and information security incident management. An incident is a threat or event that compromises, damages, or causes a loss of confidential or protected information. Examples include unauthorized or accidental disclosure of information, failure to protect user identifications, theft of computer equipment containing confidential information or client files, unexplained changes to a systems file, viruses. A more complete list of privacy and information security incident examples can be found at the DHS Information Security Office Incident Management web page.

[http://oregon.gov/DHS/admin/infosec/incdnt\\_resp.shtml](http://oregon.gov/DHS/admin/infosec/incdnt_resp.shtml)

**Purpose/Rationale:** To outline general guidelines and requirements for reporting, analyzing, responding to, remediating, and documenting privacy and information security breaches, here after referred to as incidents.

**Applicability:** All individuals granted access to DHS information or systems are covered by this policy and shall comply with associated procedures and guidelines. These individuals include full and part-time employees, volunteers, contractors, temporary workers, those employed by others to perform DHS work, and others authorized to access DHS information, network and/or systems.

**Failure to Comply:** Failure to comply with this policy and any associated procedures and guidelines may result in disciplinary actions up to and including dismissal from state service for employees, volunteers or termination of contracts for consultants and other entities. Legal actions may also be taken for violations of applicable regulations and laws. The Office for Civil Rights, federal compliance agency for HIPAA privacy and security rules, may apply criminal penalties to individual employees who intentionally obtain or disclose protected health information without authorization.

## Policy

### 1. Incident Reporting

All privacy and information security incidents must be reported. Incident information must be submitted to the Information Security Office or to the Office of Information Services. Incidents can be reported via the following options:

**a. Information Security Office (ISO)**

A. Email incident summary to the Information Security Office at either of the following addresses:

[dhs.privacyhelp@state.or.us](mailto:dhs.privacyhelp@state.or.us) or [dhsinfo.security@state.or.us](mailto:dhsinfo.security@state.or.us)

B. DHS form #3001, DHS Privacy/Security Incident Reporting Guide, ([http://oregon.gov/DHS/admin/infosec/incdnt\\_resp.shtml](http://oregon.gov/DHS/admin/infosec/incdnt_resp.shtml)) may be used as a guide to submit incident information to the above noted email addresses.

C. Mail the incident summary, or completed form #3001, to 500 Summer St. NE, E24 Salem, OR 97301

D. Report by phone: 503-945-5780

E. Report by fax: 503-947-5396

**b. Wireless Communication Devices (loss or theft)**

A. See Policy DHS-020-006-02

[http://www.dhs.state.or.us/policy/admin/cp/020\\_006.pdf](http://www.dhs.state.or.us/policy/admin/cp/020_006.pdf)

**c. DHS Service Desk**

A. [dhs.servicedesk@state.or.us](mailto:dhs.servicedesk@state.or.us)

B. 503-945-5623

**2. Incident Reporting Action Steps**

**a. Workforce Members:**

A. Workforce members shall immediately report any privacy or information security incident to their manager/supervisor. If the manager/supervisor is not available, workforce members should proceed to steps (2b), A, B, & C of this policy and report the incident to their manager/supervisor in a timely manner.

B. If the manager/supervisor is potentially the cause of the incident, or the workforce member is concerned about possible retribution for reporting, the workforce member should proceed to steps (2b), A, B & C of this policy.

**b. Manager/Supervisor:**

The incident summary shall include the following:

(DHS form [DE3001](#) may be used as a guide to submit incident information).

**A. Reporting individual's:**

i. Name

ii. DHS Program Area

iii. Address, City

iv. Phone Number

## **B. Incident Information:**

- i. Date
- ii. Location
- iii. Type of information disclosed, e.g. Social Security numbers, individually identifiable client case information, protected health information

## **C. Description/Action:**

- i. Brief description of the incident, parties and/or information systems involved and any action taken
- ii. For incidents resulting from theft, whether or not a police report was made
- iii. For incidents resulting from a loss or theft of electronic devices, whether or not the reporting steps outlined in policy DHS-020-006-02 have been followed.

## **c. Information Security Office**

- A. ISO shall coordinate and facilitate immediate incident containment and risk assessment
- B. ISO shall apply Incident Severity Criteria and Privacy/Information Security Incident Notification Criteria to determine appropriate and required response
- C. ISO shall convene an Incident Response Team to include, as appropriate to the situation, ISO Incident Coordinator, reporting and other involved workforce members, Human Resources Generalist, Privacy Review Committee member representing the involved program area, Office of Information Services representative and Office of Contracts and Procurement.
- D. ISO shall ensure notification is provided to all individuals affected by a privacy or information security incident, when the incident meets a prescribed notification threshold as outlined in the Privacy/Information Security Incident Notification Criteria. Individual notification shall meet all state and federal timelines and methods. Public notification shall be made when the number of individuals impacted or other prescribed trigger circumstances are present, in accordance with the Privacy/Information Security Incident Notification Criteria.
- E. ISO shall report privacy and information security breaches within designated time frames to the appropriate state and federal compliance agencies, and in compliance with contractual obligations.

## **3. Incident Documentation and Process Improvement**

- a. ISO shall document privacy and information security incidents and maintain incident activity logs.
- b. ISO shall utilize information from incident activity logs to facilitate privacy and information security process improvements and periodic reports.
- c. ISO shall implement department-wide privacy and information security related awareness and education activities to reduce the risk of repeated incidents.

## Form(s) that apply:

- [DHS 3001](#): Privacy/Security Incident Reporting Process Guide

## Definition(s):

- Privacy and Information Security Glossary of Terms:  
[www.oregon.gov/DHS/admin/infosec/](http://www.oregon.gov/DHS/admin/infosec/)

## Reference(s):

- Federal HIPAA Security Rule <http://www.hhs.gov/ocr/>
- DHS Privacy Policies <http://www.dhs.state.or.us/policy/admin/privacylist.htm>
- DHS Security Policies <http://www.dhs.state.or.us/policy/admin/infosecuritylist.htm>
- Information Security Office Incident Response Program  
[http://oregon.gov/DHS/admin/infosec/incdnt\\_resp.shtml](http://oregon.gov/DHS/admin/infosec/incdnt_resp.shtml)

## Contact(s):

**Name:** Kyle Miller; **Phone:** (503-945-6812); **Email:** ([dhsinfo.security@state.or.us](mailto:dhsinfo.security@state.or.us))

## Policy History:

- **Version 2.0:**
  - 01/06/2010: This policy originated in 10/2004. It was created to inform DHS staff and management that privacy and information security incidents involving a threat or event that compromises, damages, or causes a loss of confidential or protected information, are reportable. The original policy provided guidance on a reporting process that was needed at that time to meet federal compliance requirements. State and federal regulations have changed and increased. They now require a greater level of notification and reporting activities regarding privacy and information security incidents. These new requirements are built into this revised policy.
- **Version 1.0:**
  - 10/01/2004 (Initial Release)