Oregon Dept of Human Services

& Oregon Health Authority

Information Security Incident Response Plan

Bryant Lister, Director of Information Security & Privacy Office

September 17, 2021

TABLE OF CONTENTS

Introduction

The purpose of an information security incident response program is to ensure the effective response and handling of security incidents that affect the availability, integrity, or confidentiality of agency information assets. In addition, an incident response program will ensure information security events, incidents and vulnerabilities associated with information assets and information systems, are communicated in a manner enabling timely corrective action.

ORS 276A.300 requires agencies to develop the capacity to respond to incidents that involve the security of information. Agencies must implement forensic techniques and controls, and consider lessons learned. The statute also requires reporting incidents and plans to the Enterprise Information Services (EIS) Cyber Security Services (CSS). The Oregon Consumer Information Protection Act (ORS 646A.600, et seq.) requires agencies to take specific actions in cases where compromise of Personal Information and Protected Health Information (PHI) has occurred. This plan addresses these requirements.

The Oregon Department of Human Services (ODHS) and Oregon Health Authority (OHA) have developed this Information Security Incident Response Plan to implement their incident-response processes and procedures effectively, and to ensure that ODHS and OHA workforce understand them.

- The intent of this document is to describe the process of responding to an incident and educate employees on their role during an incident.
  - Immediate detection and analysis allow determination of scope, threat entry point, and level of comprise.
- Respond to support containment, eradication, and recovery
  - Containment - aims to stop the threat entry point
  - Eradication - aims to remove the threat
  - Recovery - aims to get agency systems operational

An incident response plan brings together and organizes the appropriate resources for dealing with any event that harms or threatens the security of information assets. Such an event may be a malicious code attack, an unauthorized access to information or systems, the unauthorized use of services, a denial-of-service attack, or a hoax. The goal is to facilitate quick and efficient response to incidents, and to limit their impact while protecting the state’s information assets. The plan defines roles and responsibilities, documents the steps necessary for effectively and efficiently managing an information security incident, and defines channels of communication. The plan also prescribes the education needed to achieve these objectives.

Authority

Statewide information security policies:

Policy Number	Policy Title	Effective Date
107-004-050	Information Asset Classification	1/31/2008
107-004-051	Controlling Portable and Removable Storage Devices	7/30/2007
107-004-052	Cyber and Information Security	11/16/2020
107-004-053	Employee Security	7/30/2007
107-004-100	Transporting Information Assets	1/31/2008
107-004-110	Acceptable Use of State Information Assets	01/01/2010
107-004-120	Cyber and Information Security Incident Response	11/16/2020
107-004-140	Privileged Access to Information Systems	07/10/2013
107-004-150	Cloud and Hosted Systems Policy	05/01/2019

ODHS|OHA information security policies:

Policy Number	Policy Title	Effective Date
ODHS|OHA 090-003	Access Control Policy	08/02/2021
ODHS|OHA 090-004	Information Security and Privacy Awareness and Training Policy	11/2/2020
ODHS|OHA 090-005	Information Security Incident Management Policy	03/01/2021
ODHS|OHA 090-006	Information Security Risk Assessment Policy	11/2/2020
ODHS|OHA 090-007	Information Technology Vulnerability Management Policy	06/07/2021
ODHS|OHA 090-009	Administrative, Technical and Physical Safeguards of Information Policy	07/12/2021

Terms and Definitions

Asset: Anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards).

Control: Means of managing risk including policies, procedures, guidelines, practices, or organizational structures, which can be of administrative, technical, physical, management, or legal nature.

Event: An observable occurrence in an information system that happened at some point in time.

Evidence Preservation: Balancing the need to restore operations against the need to preserve evidence is a critical part of incident response. Gathering evidence and preserving it are essential for proper identification of an incident, and for business recovery. Follow-up activities, such as personnel actions or criminal prosecution, also rely on gathering and preserving evidence.

Incident: A single or a series of unwanted or unexpected information security events (see definition of "information security event") that may result in harm or pose a significant threat of harm to information assets and require non-routine preventative or corrective action.

Incident Classification: According to the Information Asset Classification Policy (DAS 107-004-050) the following factors are considered when evaluating incidents: Criticality of systems that are (or could be) made unavailable, value of the information compromised (if any), number of people or functions impacted business considerations, public relations, enterprise impact, and multi-agency scope.

- Level 1 Information – Information that is published, readily available, or retrievable by simple means (including internet search.) Examples include press releases, public-access web pages and advertisements.
- Level 2 Information – Sensitive but unprotected information where the impact of release should be considered before disclosure. Examples include state issued identification numbers, audit reports, names, and addresses. This information is often regulated by internal policies.
- Level 3 Information – Sensitive and/or legally protected information where unauthorized release or disclosure may require notification. Examples include Social Security numbers, Protected Health Information, and network diagrams. This information is regulated by state and/or federal law.
- Level 4 Information – Highly sensitive and/or legally protected information intended for use by named individuals only. Examples include classified information and Criminal Justice Information (CJIS.)

Incident Identification: The process of analyzing an event and determining if that event is normal or if it is an incident. An incident is an adverse event and it usually implies either harm, or the attempt to harm the ODHS|OHA. Events occur routinely and will be examined for impact. Those showing either harm or intent to harm may be escalated to an incident.

Incident Response Plan: Written document that states the approach to addressing and managing incidents and their effects on information systems.

Incident Response Policy: Written document that defines organizational structure for incident response, defines roles and responsibilities, and lists the requirements for responding to and reporting incidents.

Incident Response Processes: Written document(s) of the series of steps taken when responding to incidents.

Incident Response Program: Combination of incident response policy, plan, and processes.

Incident Log: A record of the events related to an incident within an organization's affected systems and networks.

Information: Any communication or representation of knowledge in any medium or form. Examples include, but are not limited to:

- Documents, reports, statistics, files, and records, compiled or stored in digital or physical form
- E-mails or messaging system conversations and their attachments
- Audio and video files
- Images, graphics, pictures, and photographs
- Programs, software, and macros

Information Security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.

Information Security Event: An observable, measurable occurrence with respect to an information asset that is a deviation from normal operations.

Personal Information as defined by the Oregon Consumer Information Protection Act (Oregon Revised Statute 646A.602):

(12)(a) "Personal information" means:

(A) A consumer's first name or first initial and last name in combination with any one or more of the following data elements, if encryption, redaction or other methods have not rendered the data elements unusable or if the data elements are encrypted and the encryption key has been acquired:

(i) A consumer’s Social Security number;

(ii) A consumer’s driver license number or state identification card number issued by the Department of Transportation;

(iii) A consumer’s passport number or other identification number issued by the United States;

(iv) A consumer’s financial account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to a consumer’s financial account, or any other information or combination of information that a person reasonably knows or should know would permit access to the consumer’s financial account;

(v) Data from automatic measurements of a consumer’s physical characteristics, such as an image of a fingerprint, retina or iris, that are used to authenticate the consumer’s identity in the course of a financial transaction or other transaction;

(vi) A consumer’s health insurance policy number or health insurance subscriber identification number in combination with any other unique identifier that a health insurer uses to identify the consumer; or

(vii) Any information about a consumer’s medical history or mental or physical condition or about a health care professional’s medical diagnosis or treatment of the consumer.

(B) A user name or other means of identifying a consumer for the purpose of permitting access to the consumer’s account, together with any other method necessary to authenticate the user name or means of identification.

(C) Any of the data elements or any combination of the data elements described in subparagraph (A) or (B) of this paragraph without the consumer’s user name, or the consumer’s first name or first initial and last name, if:

(i) Encryption, redaction or other methods have not rendered the data element or combination of data elements unusable; and

(ii) The data element or combination of data elements would enable a person to commit identity theft against a consumer.

(b) “Personal information” does not include information in a federal, state or local government record, other than a Social Security number, that is lawfully made available to the public.

Protected Information: Information, which is protected by law, rule, regulation, or contract. This can be Protected Health Information as defined by HIPAA, Personal Information as defined by the Oregon Consumer Information Protection Act, Social Security Numbers, Federal Tax Information and Criminal Justice Information. See Level 1-4 Information above.

Threat: A potential cause of an unwanted incident, which may result in harm to a system or the agency.

Roles and Responsibilities

Agency Chief Information Officer (CIO)

Responsible for providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; developing, maintaining, and facilitating the implementation. The CIO is responsible for overall effectiveness of the incident response program. Acts as Incident Commander or delegates Incident Commander role as needed. The CIO is responsible for providing consultation and direction on incidents to support compliance with local, state, and federal laws.

Agency Chief Information Risk Officer

Responsible for providing guidance and oversight regarding the creation, receipt, maintenance, and transmission of electronic protected information. Develops and implements 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. Serves as the ODHS|OHA Security Official for concerns associated with the Health Insurance Portability and Accountability Act (HIPAA).

Agency Director

Responsible for information security in the agency, for reducing risk exposure, and for ensuring the agency's activities do not introduce undue risk to the enterprise. The director also is responsible for ensuring compliance with state enterprise security policies, standards, and security initiatives, and with state and federal regulations. Agency directors are also responsible for representing the agency business owner, and for providing business continuity response and leadership in the event a security incident jeopardizes the on-going business operations of the agency.

Agency Point of Contact

Responsible for establishing agency reporting method and communicating incidents with EIS CSS Security Operations Center (SOC). Provides a point of contact for communications between EIS CSS SOC and agency responders during an incident.

Cyber Security Services (CSS)

The Enterprise Information Services (EIS) CSS manages the state's response to incidents including those involving an actual or suspected breach under the Oregon Consumer Information Protection Act (ORS 646A.600 et seq). Depending upon the incident scope and impact, and agency capabilities, EIS CSS may either directly manage the incident or coordinate with the affected agency on the incident response. The EIS CSS's role may change during the incident.

Incident Commander

The Incident Commander has overall responsibility for managing the incident by establishing objectives, planning strategies, and implementing tactics. The Incident Commander is the only position that is always staffed in an Incident Command System (ICS) application. On small incidents and events, one person, the Incident Commander, may accomplish all management functions. The Incident Commander is responsible for all ICS management functions until they delegate those functions. Depending on the scope and severity of the incident, the Incident Commander may be representative of EIS CSS or the agency.

Incident Command System (ICS)

A standardized incident management approach that allows for the integration of facilities, equipment, personnel, procedures, and communications within a common organizational structure; enables a coordinated response among different agencies and entities; and establishes common processes for planning and managing resources.

Incident Response Lead See Incident Commander

Information Owner Responsible for creating initial information classification, approving decisions regarding controls and access privileges, performing periodic reclassification, and ensuring regular reviews for value and updates to manage changes to risk.

Legal Counsel Responsible for providing legal guidance in all stages of incident response activities.

Local Agency Security Officer (LASO

The primary Information Security contact between an ODHS or OHA unit or program using criminal justice information, and the Oregon State Police (OSP) through which the unit or program interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to Criminal Justice Information Security, disseminates Information Security alerts and other material to their constituents, maintains Information Security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps OSP informed as to any Criminal Justice Information Security needs and problems.

ODHS|OHA Communications Office

Responsible for coordinated release of information about incidents to the public, under the direction of the Incident Commander. In the event of a public release and depending upon the scope of the incident, the agency Communications Office will work together with EIS and the Governor's Public Information Office to provide a unified message to the public.

Office of Emergency Management

Responsible for maintaining the state Emergency Operations Plan and managing the Emergency Coordination Center (ECC) facility. Maintains a state-wide common operating picture and coordinates emergency response and recovery activities across local, tribal, state, and federal governments and the private sector. In incidents classified as Levels 3 or 4, may be called upon to facilitate coordination of response efforts.

ODHS|OHA Communications Office

Responsible for coordinated release of information about incidents to the public, under the direction of the Incident Commander. In the event of a public release and depending upon the scope of the incident, the agency Communication's Office will work together with EIS and the Governor's Public Information Office to provide a unified message to the public.

Security Incident Response Team (SIRT)

Team of responders, composed of both EIS CSS SOC and Agency personnel, to an information security incident. Although the makeup of the team may vary depending upon incident scope and severity, it will contain the following common elements regardless of size: an incident command structure, a communications component and information security technical advisors.

State Chief Information Security Officer (CISO)

Responsible for statewide information security and integration of incident response strategies and serves as the spokesperson for communications (as necessary) and signature authority and engagement of third-party incident and breach services.

User	Responsible for complying with the provisions of policies, processes, and practices.

Program

ODHS and OHA face a wide variety of security incidents and threats both internally and externally, that may impact both agencies' ability to support business operations and could result in significant loss to confidential information of Oregonians. This incident response plan is governed through collaboration with key stakeholders throughout ODHS, OHA and the Department of Administrative Services (DAS). Refer to Appendix A for the technology governance structure.

The Incident Response Program is composed of this plan in conjunction with policies and processes. The following documents should be reviewed for a complete understanding of the program:

1. *Information Security Incident Management Policy*, ODHS|OHA 090-005, located in Appendix B.

2. *Information Security Incident Reporting Process*, ODHS|OHA 090-005-01, located in Appendix B.

3. *Information Security Incident Reporting Process Map*, ODHS|OHA 090-005-02, located in Appendix B.

4. *Report and Response to Privacy and Security Incidents*, OHA 100-014, located in Appendix B.

Information security incidents will be communicated in a manner allowing timely corrective action to be taken. This plan shows how ODHS|OHA will handle responses to an incident, incident communication, incident response plan testing, training for incident responders, and information security awareness training

The Information Security Incident Response Policy, plan, and processes will be reviewed annually, or as significant organizational or regulatory changes occur, to ensure their continuing adequacy and effectiveness. Each will have an owner who has approved management responsibility for its development, review, and evaluation. Reviews will include assessing opportunities for improvement and approach to managing information security incident response in regard to integrating lessons learned, changes to ODHS|OHA environment, new threats and risks, business circumstances, legal and policy implications, and technical environment.

Identification

Events reports to the Information Security And Privacy Office will go through the process of identification. Identification of an incident is the process of analyzing an event and determining if that event is normal or if it is an incident. An incident is an adverse event and it usually implies either harm, or the attempt to harm the

ODHS|OHA. Events occur routinely and will be examined for impact. The events are reported to the Information Security and Privacy office for investigation. Those showing either harm or intent to harm may be escalated to an incident.

The incident commander will enlist a security professional from the agency or from EIS CSS to analyze the event and then determine if a security incident has occurred.

Incident Classification

Once an event is determined to be an incident, several methods exist for classifying incidents.

The incident commander or their delegate will be responsible for working with all appropriate stakeholders in determining incident classification and whether to report the incident within the approved ticketing system.

The following factors are considered by a security professional when evaluating incidents:

- Criticality of systems that are (or could be) made unavailable
- Value of the information compromised (if any)
  - Data classification
  - Data type
- Number of people or functions impacted
- Business considerations
- Public relations
- Enterprise impact
- Multi-agency scope

Triage

The objective of the triage process is to gather information, assess the nature of an incident andbegin making decisions about how to respond to it. It is critical to ensure when an incident is discovered and assessed the situation does not become more severe.

The Incident Commander, and if applicable, the Incident Response Team including the security analyst and other technical teams will be responsible for the following:

- The initial investigation and discovery.
- Monitoring, triage and investigation of logs, reports and system event alerts including threat intelligence software within the agency.
- Document detailed information throughout the incident response process.
- Reports to Incident Commander or delegate on the incident and confirming the level of compromise and/or breach of information.

- Important questions to consider:
    - What type of incident has occurred?
    - Who is involved?
    - What is the scope?
    - What is the urgency?
    - What is the impact thus far?

Evidence Preservation

Carefully balancing the need to restore operations against the need to preserve evidence is a critical part of incident response. Gathering evidence and preserving it are essential for proper identification of an incident, and for business recovery. Follow-up activities, such as personnel actions or criminal prosecution, also rely on gathering and preserving evidence.

Incident response teams, that include security analyst and other technical teams will be responsible for the following:

- Providing expertise on incident response and forensics, threats, and vulnerability reporting.
- Collecting and managing evidence as directed by the Incident Response Commander or delegate.

The Incident Response Team will work with stakeholders to collect, categorize, and securely store evidence applicable to the incident.

Forensics

In information security incidents involving computers or mobile devices, when necessary agency forensic resources, will technically analyze computing devices to identify the cause of an incident, its scope, or to analyze and preserve evidence.

Agency forensic resources will practice the following general forensic guidelines:

- Document observations and actions taken
- Make forensically-sound images of systems and retain them in a secure place
- Establish and document chain of custody for evidence
- Assist in preserving the chain of custody for evidence collected during the incident as directed
- Provide basic forensic training to incident response staff, especially in preservation ofevidence

Incident Commander and Incident Response Team would determine if it is necessary for a third-party vendor to be procured to do the analysis.

Threat/Vulnerability Eradication

After an incident, efforts will focus on identifying, removing, and repairing the vulnerability that led to the incident and restore the system to normal operations, which could include rebuilding systems. To do this, the vulnerability(s) needs to be clearly identified so the incident isn't repeated. The goal is to prepare for the resumption of normal operations with confidence that the initial problem has been fixed.

Incident Commander or delegate identifies program and plan improvements and works in collaboration with appropriate stakeholders to support further agency or operational changes. The system owner follows the lessons learned from the incident regarding vulnerabilities to the system and takes the necessary steps to remediate the vulnerabilities.

Confirm that Threat/Vulnerability has been Eliminated

After the cause of an incident has been removed or eradicated and data or related information is restored, it is critical to confirm all threats and vulnerabilities have been successfully mitigated and that new threats or vulnerabilities have not been introduced.

The system owner works with security professionals who conduct a vulnerability assessment of the system to ensure that vulnerabilities have been eliminated.

Resumption of Operations

Resuming operations is a business decision, but it is important to conduct the preceding steps toensure it is safe to do so.

Business executives decide if they are ready to return to operations and give direction to staff.

Post-Incident Activities

An after-action analysis will be performed for all incidents. The analysis may consist of one or more meetings and/or reports. The purpose of the analysis is to give participants an opportunityto share and document details about the incident and to facilitate lessons learned. The meetings should be held within one week of the Incident Commander closing the incident.

The Incident Commander conducts the lessons learned with relevant stakeholders, gathering facts about the incident response and mitigation to develop plans for improvement.

Awareness and Education

ODHS|OHA shall ensure that incident response is addressed in awareness and education programs. The programs shall address what to do in the event of a security incident such as a data breach, insider threat, malware attack or network intrusion.

The Incident Response Plan will be reviewed annually, which may include a tabletop exercise or other assessments, and training provided at least annually. The exercise and training will provide and support the following:

- Ongoing assessment of the incident response plan
- Agency needs (e.g. tools, resources, etc.)
- Evaluation of the overall effectiveness of the incident response plan

Periodic training will be provided to support organizational readiness and changes within the organization.

The agency education and awareness coordinator reviews lessons learned and determines if additional artifacts, trainings, and materials are necessary to address identified gaps.

Communications

Because of the sensitive and confidential nature of information and communication surrounding an incident, all communication must be through secure methods utilizing encryption and/or obfuscation where appropriate.

The Incident Commander or delegate collaborates with appropriate stakeholders to provide guidance into communications for internal and external parties. The Incident Commander or delegate will provide appropriate stakeholders periodic updates and reports on the status of the incident and remediation efforts.

Depending on the severity and scope of the incident, the Incident Commander or delegate should consult with the Department of Justice (DOJ) for counsel and support.

Playbooks need to include a Responsible Accountable Consulted Informed (RACI) Matrix for communications depending on type of incident.

When appropriate, external communications need to be handled by ODHS or OHA Communications Departments.

Assume that all communications regarding an incident should be sent securely unless otherwise indicated by the Incident Commander. Approved communications will be managed by ISPO with the current, approved, and acceptable methods for securing communication.

As delegated by the Incident Commander and with approval from agency executive leadership communications will be handled by the agencies’ Media Press Office which handles all media relations and inquiries.

Compliance

ODHS|OHA is responsible for implementing and ensuring compliance with all applicable laws, rules, policies, and regulations.

ODHS and OHA CIO in collaboration with the CIRO and other stakeholders is responsible for supporting the overall oversight and compliance function for both ODHS and OHA.

45 CFR 160 General Administrative Requirements

45 CFR 164 Security and Privacy

ORS 276A.300 Information Security

OAR 407-014-0000 through 0320 Privacy and Confidentiality

OAR 943-014-0000 to 943-014-0465 Privacy and Confidentiality

DAS 107-004-120 Cyber and Information Security Incident Reponses Policy

Center for Internet Security Top Twenty Critical Security Controls

Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy

Internal Revenue Service 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

Statewide Information and Cyber Security Standards 2019

ODHS|OHA 090-005 Information Security Incident Management Policy

ODHS|OHA 090-005-01 Information Security Incident Reporting Process

Centers for Medicare and Medicaid Services (CMS)

If an "incident" or "breach" occurs, as defined by the Interconnection Security Agreement between CMS and the Oregon Health Authority One System, notification will be made to HIX.incidents@cms.hhs.gov within one hour of discovery.

If a suspected security incident warrants a disconnection of the system-to-system connection to CMS, OHA will contact the CMS IT Service Desk at 410.786.2580 and/or via email at CMS_IT_Service_Desk@cms.hhs.gov.
If a suspected security incident implicates Medicaid and/or CHIP data, notification will be made to the CMS IT Service desk at 410.786.2580 as well as to the appropriate Special Agent-in-Charge, TIGTA and IRS Office of Safeguards within 24 hours of discovery of the incident.

Criminal Justice Information

If an incident is determined to impact Criminal Justice Information (CJI), the Local Agency Security Officer (LASO) will report the incident information to the state CJIS Information Security Officer (CJIS ISO). The LASO uses the OSP IT Security Incident Response Form when reporting incidents to the Oregon State Police and the Federal Bureau of Investigations (FBI) CJIS Division. The FBI Security Incident Response Form provided in Appendix F of the CJIS Security Policy will also be accepted.

Federal Tax Information

If a suspected security incident involves Federal Tax Information (FTI), notification will be made to the IRS Office of Safeguards via email to safeguardreports@irs.gov and via telephone to the Treasury Inspector General for Tax Administration (TIGTA) at 800.589.3718.

Upon discovering a possible improper inspection or disclosure of FTI, ISPO contacts the TIGTA Field Division Office special agent-in-charge immediately, but no later than 24 hours after identification of a possible issue involving FTI. Concurrent to notifying TIGTA, the ISPO will notify the IRS Office of Safeguards via email.

The agency notifies a taxpayer in writing if the agency proposes an administrative determination as to disciplinary or adverse action against an employee arising from the employee's unauthorized inspection or disclosure of the taxpayer's return or return information. The written notice includes the date of the unauthorized inspection or disclosure of return information and the rights of the taxpayer under Internal Revenue Code (IRC) §7431. The agency cooperates with TIGTA and Office of Safeguards investigators, providing data and access as needed to determine the facts and circumstances of the incident.

Oregon Consumer Information Protection Act (OCIPA)

If an incident is determined to be a breach of security as defined in OCIPA, notification to all impacted individuals will be completed within 45 days of discovery of the incident. If the cost of notification exceeds $250,000 or the affected class of consumers exceeds 350,000, or if there is insufficient contact information to notify consumers, substitute notice will be made pursuant to current Oregon law. Notification may be delayed if a law enforcement agency determines that such notification will impede a criminal investigation.

If the security breach affects more than 1,000 consumers, ODHS or OHA will report the breach to all consumer reporting agencies that compile and maintain reports on consumers on a nationwide basis the content of the notice given to affected consumers without unreasonable delay.

If, after an appropriate investigation or, after consultation with relevant federal, state, or local law enforcement agencies, it is determined that the consumer(s) whose personal information was subject to the breach of security are unlikely to suffer harm, notification is not required. Such determination will be documented and maintained for at least five years.

Social Security Administration Information

If an incident is determined to impact Social Security Administration (SSA) Information, ISPO will notify the SSA Regional Office or the SSA Systems Security Contact as identified in the SSA Information Exchange Agreement (IEA) within one hour of notification of the suspected or actual loss of SSA-provided information. ISPO will provide updates to SSA as appropriate. SSA makes a determination about whether the risk presented by the breach or security incident requires the notification to the impacted individuals.

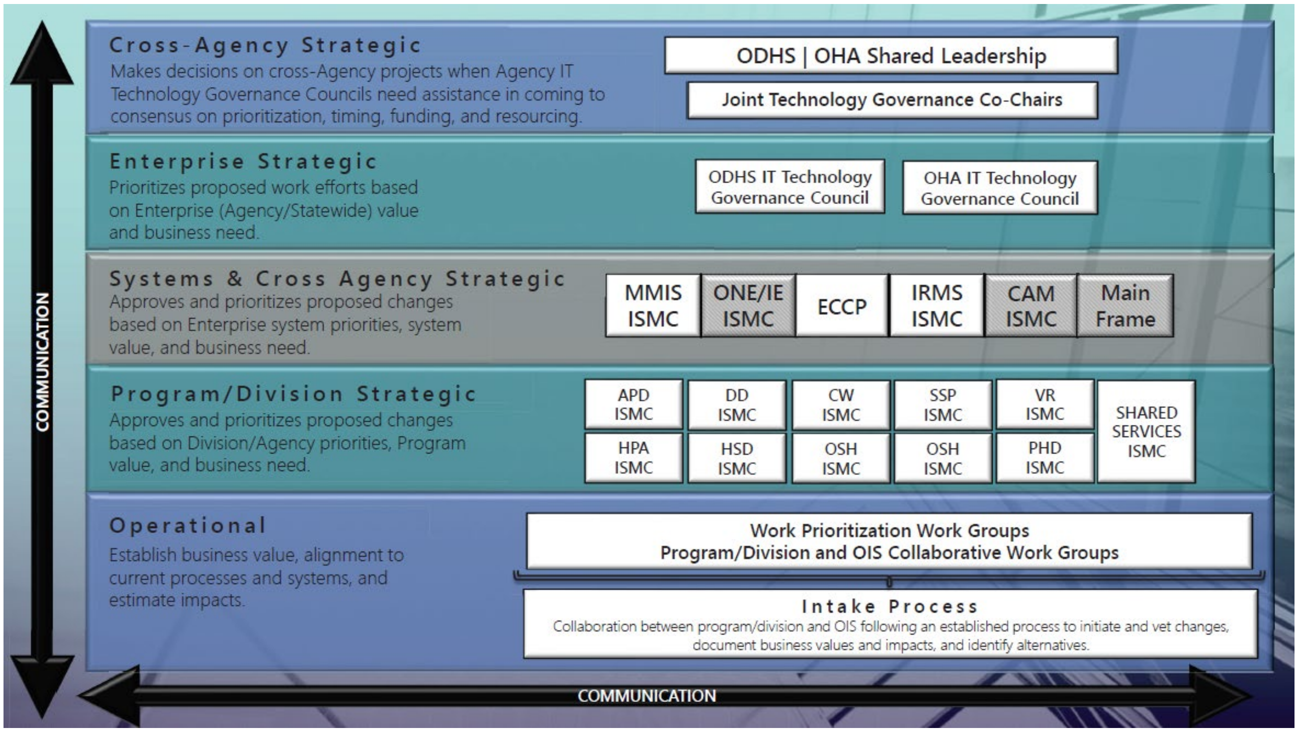
Implementation

ISPO is committed to assist ODHS|OHA in formulating and implementing appropriate incident response strategies.
This plan was developed to achieve this goal by giving direction and support for agency staff involved in incident response.

ISPO will:

- Respond to information security incidents.
- Serve as core staff within the Incident Command Structure for incidents.
- Coordinate with trained technical staff with the capability to forensically gather and analyze evidence while observing necessary evidence-preservation practices.
- Test the incident response plan and verify incident response team’s ability to execute.
- Maintain a comprehensive list of key contacts that is regularly updated with status information.
- Provide or recommend basic incident response training covering incident identification and an overview of an incident response plan.
- Make recommendations for specific training or courses.
- Provide education or guidelines on the accurate and timely identification and escalation of incidents.

APPENDIX A: TECHNOLOGY GOVERNANCE STRUCTURE



Cross-Agency Strategic

Makes decisions on cross-Agency projects when Agency IT Technology Governance Councils need assistance in coming to consensus on prioritization, timing, funding, and resourcing.

ODHS | OHA Shared Leadership

Joint Technology Governance Co-Chairs

Enterprise Strategic

Prioritizes proposed work efforts based on Enterprise (Agency/Statewide) value and business need.

ODHS IT Technology Governance Council

OHA IT Technology Governance Council

Systems & Cross Agency Strategic

Approves and prioritizes proposed changes based on Enterprise system priorities, system value, and business need.

MMIS ISMC | ONE/IE ISMC | ECCP | IRMS ISMC | CAM ISMC | Main Frame

Program/Division Strategic

Approves and prioritizes proposed changes based on Division/Agency priorities, Program value, and business need.

APD ISMC | DD ISMC | CW ISMC | SSP ISMC | VR ISMC | SHARED SERVICES ISMC

HPA ISMC | HSD ISMC | OSH ISMC | OSH ISMC | PHD ISMC

Operational

Establish business value, alignment to current processes and systems, and estimate impacts.

Work Prioritization Work Groups
Program/Division and OIS Collaborative Work Groups

Intake Process

Collaboration between program/division and OIS following an established process to initiate and vet changes, document business values and impacts, and identify alternatives.

APPENDIX B: INCIDENT RESPONSE POLICIES AND PROCESSES

1. Cyber and Information Security Incident Response Policy, DAS 107-004-120

2. Information Security Incident Management Policy, ODHS|OHA 090-005

3. Information Security Incident Reporting Process, ODHS|OHA 090-005-01

4. Information Security Incident Reporting Process Map, ODHS|OHA 090-005-02

5. Report and Response to Privacy and Security Incidents, OHA 100-014

APPENDIX C: NOTIFICATIONS

- Center for Medicare and Medicaid Services (CMS) Office of Communications: 202-690-6145
- CJIS Information Security Officer-Frank Miles: 503-507-7851
- Credit Monitoring Bureaus
  - Equifax: 1-800-525-6285
  - Experian: 1-888-397-3742
  - TransUnion: 1-800-680-7289
- OHA Communications: 503-945-6691: OHA-Communications@dhsoha.state.or.us
- ODHS Communications: 503-945-6331: DHS-Comm@dhsoha.state.or.us
- ODHS|OHA Chief Information Officer-Debbie Estabrook: 503-947-2591
- ODHS|OHA Chief Information Risk Officer-Bryant Lister: 503-602-8746
- ODHS Agency Director-Fariborz Pakseresht: 503-945-7001
- ODHS Chief Administrative Officer-Don Erickson: 503-884-8774
- OHA Agency Director-Pat Allen: 503-945-6777
- OHA Deputy Director-Kris Kautz: 503-383-5147
- Department of Administrative Services (DAS) Enterprise information Services (EIS) Cyber Security Services (CSS) Hotline: 503-378-5930
- DAS EIS CSS Security Operations Center (SOC)-Mark E. Johnston: 503-947-0488
- DAS EIS CSS Chief Information Security Officer-Gary Johnson: 503-373-0210
- State CIO-Terrance Wood: 503-373-7751
- DAS Director’s Office-Katy Coba: 503-378-3104
- DAS Office Communication Director-Andrea Chiapella: 971-345-1333
- Federal Bureau of Investigations: 503-460-2371
- Internal Revenue Services (IRS) Treasury Inspector General for Tax Administration (TIGTA) Field Division Office: 801-620-7734; Hotline Number: 800-589-3718
- Oregon Department of Justice (DOJ)-Ellen Flint: 503-947-4342
- Oregon State Police: 503-378-3720 (Ask for Criminal Lieutenant)
- OSP Northern Command Center: 503-375-3555
- Social Security Administration (SSA): 877-697-4889
- SSA Assistant District Management-Dawn Stone: 866-931-9171

Approval

By: ____

Debbie Estabrook, Chief Information Officer Date

By: ____

ODHS Agency Director or Designee Date

By: ____

OHA Agency Director or Designee Date