Oregon Dept of Human Services

& Oregon Health Authority

Information Security Incident Response Plan

Kristine Cornett, Chief Information Risk Officer

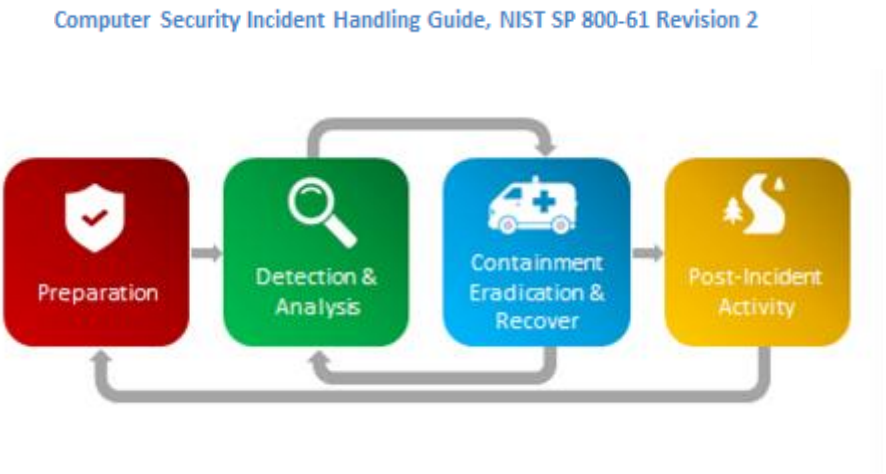
December 2024

TABLE OF CONTENTS

PURPOSE

PURPOSE

The purpose of this Information Security Incident Response Plan (the "IRP" or "Plan") is to provide a framework for responding to an information security incident that might involve the loss of sensitive data or the disruption of information technology services. It follows the framework established by the National Institute of Standards and Technology ("NIST") that divides the incident response life cycle into four major phases, as represented in the following graphic:



Authority

The Oregon Revised Statute (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 information security 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 personally identifiable information (PII) and protected health information (PHI) has occurred. This plan addresses these requirements. (Refer to Authority and Compliance in Appendix A). The Privacy Office has a response plan relative to privacy incidents. However, Privacy must be notified upon discovery of an information security incident to assess whether PHI or PII data has been potentially viewed or exfiltrated, providing regulatory support as required.

Compliance

The Oregon Department of Human Services (ODHS) and Oregon Health Authority (OHA) are responsible for implementing and ensuring compliance with all applicable laws, rules, policies, and regulations.

The ODHS and OHA Chief Information Officer (CIO) in collaboration with the Chief Information Risk Officer (CIRO) and applicable participants are responsible for

supporting the overall oversight and compliance function for both ODHS and OHA. (Refer to Authority and Compliance in Appendix A).

Program

ODHS and OHA face the potential of a wide variety of information security incidents and threats, both internally and externally, that may impact both agencies' ability to support business operations.

The Office of Information Services (OIS) Information Security Incident Response Program, in support of ODHS and OHA, is composed of this plan in conjunction with policies and processes. (Refer to Authority and Compliance in Appendix A)

The information security incident response plan is governed through collaboration with key partners throughout ODHS and OHA and the Department of Administrative Services (DAS). (Refer to Technology Governance Structure in Appendix B).

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

The DAS 107-004-052 Cyber and Information Security Incident Policy requires that the IRP will be reviewed annually, or as significant organizational or regulatory changes occur, to ensure its 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 regarding integrating lessons learned, changes to ODHS and OHA environment, new threats and risks, business circumstances, legal and policy implications, and technical environment.

Implementation

The Information Security and Privacy Office (ISPO) is committed to assisting ODHS and OHA in formulating and implementing incident response strategies. This plan was developed to achieve that goal by giving direction and support for agency staff involved in information security incident response activities.

ISPO will:

- Respond to information security incidents and report inappropriate disclosure of data including protected health information (PHI), personally identifiable information (PII), Social Security Administrative (SSA) data, Criminal Justice Information (CJI), and Federal Tax Information (FTI) to the Privacy Compliance Officer.
- Serve as coordinators within the Information Security Incident Command Structure as the Agency Incident Commander.

- Ensure the Privacy Team is involved if compromised systems contain PHI or PII.
- Coordinate with trained technical staff with the capability to forensically gather and analyze evidence while observing necessary evidence-preservation practices.
- Test the IRP and verify information security incident response team's ability to execute.
- Maintain a comprehensive list of key contacts that is updated at least annually with status information.
- Educate on basic IRP principles, the accurate and timely identification and escalation of information security incidents, and any updates for the agency through Awareness and Education.
- Make recommendations for specific information security incident response training or courses.
- Discern steps that should be considered to prevent further data leakage and communicate with key players when necessary.
- Report to EIS CSS Security Operations Center (SOC) all security incidents within 24 hours.

Information Security Incident Severity and Classification

Information security incident severity determination answers the question "what is the overall impact of the information security incident on the State of Oregon?" Accordingly, incident severity ratings drive incident routing, escalation, escalation urgency, and composition of the Incident Response Team (IRT) to respond appropriately to information security incidents. Incident severity may change during response activities based on factors such as scope change, increased publicity, or other escalation factors.

Escalation

Different levels of information security incident(s) require different types of resources, communication strategies and levels of authority to respond. Information security incidents and response circumstances may change, often quickly, requiring smooth escalation of response efforts.

Escalation is generally prompted by the following types of events:

- Publicity: Public or media interest in an information security incident may increase the sensitivity, urgency, and resource requirements.
- Scope Change: The scope of the information security incident may increase.
- Responsibility or Authority Change: Responsibility or authority to respond may be transferred.
- Resource Constraints: The capacity or capabilities of current responders may be exceeded.
- Political Sensitivity: Potential political damage may require a higher-level response.

- Perceived or Actual Mismanagement: Initial response may be (deemed) inadequate, requiring a higher-level response.

An escalation requires transfer of authority and information security incident command to a responder appropriate for the new level of response, including possible transition to a new information security incident command structure. Additionally, it may require opening communications with other parties, bringing new resources online and coordination with current response activities and personnel.

(Refer to the Statewide IR Plan – Information Security Incident Severity and Classification, Escalation and Escalation Communications & Chart (Escalation Severity Levels and Prompts) in Appendix C).

Communications
Communications are critical and an important component of information security incident response that must be handled with due care. The Information Security Incident Commander or delegate will collaborate with appropriate staff to provide guidance regarding communications for internal and external parties. (Refer to the Statewide IR Plan in Appendix C).

Objectives
The objectives of the information security incident response plan are to facilitate quick and efficient response to information security incidents, limiting their impact and protecting State information assets. The information security incident response plan defines roles and responsibilities, documents the steps necessary for effectively managing an information security incident, describes incident severity levels and how escalation occurs, pre-defines communications channels, and prescribes necessary education to achieve these objectives.

The objectives of the plan are to:

- Identify the (ODHS and OHA) response team and their responsibilities.
- Provide a systematic and efficient means of response and recovery in a manner and timeframe that meets agency policies, and contractual and regulatory requirements. Refer to ODHSOHA 090-005 Information Security Incident Management Policy, ODHSOHA 090-005-01 Information Security Incident Reporting Process, and ODHSOHA 100-014 Report and Response to Privacy Incidents
- Minimize disruption to business operations and loss or theft of information assets.
- Minimize any negative impact to ODHS and OHA financial health and reputational harm.
- Minimize negative impact to third parties, including partners, service providers and contractors, and employees.

- Minimize any negative impact to Oregonian's and the communities served by ODHS and OHA.

Scope
The IRP is intended as an overarching structure for responding to information security incidents. The plan applies to:

- Business, partner(s), and employee information supported or managed by ODHS and OHA in electronic or non-electronic form.
- Third party infrastructure (i.e., partners, contractors, and service providers) that rely on ODHS and OHA to access data, or for other business operations.

Activation Criteria
The IRP may be activated for any incident involving the security of information and/or privacy incidents that result in a breach of information. (Refer to Incident Escalation Severity Levels and Prompts in Appendix C).

Terms and Definitions
(Refer to information security incident response-related terms and definitions in Appendix D).

Roles and Responsibilities

Roles	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 information security incident response program. Acts as Information Security Incident Commander or delegates Information Security Incident Commander role as needed. The CIO is responsible for providing consultation and direction on information security incidents to support compliance with local, state, and federal laws.
Agency Chief Information Risk Officer (CIRO)	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 and 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 also are responsible for representing the agency business owner, and for providing business continuity response and leadership in the event an information security incident jeopardizes the on-going business operations of the agency.
Agency Point of Contact	Responsible for establishing agency reporting method and communicating information security incidents with EIS CSS

Roles	Responsibilities
	Security Operations Center (SOC). Provides a point of contact for communications between EIS CSS SOC and agency responders during an information security incident.
Cyber Security Services (CSS)	The Enterprise Information Services (EIS) CSS manages the state's response to information security incidents including those involving an actual or suspected breach under the Oregon Consumer Information Protection Act (ORS 646A.600 et seq). Depending upon the information security incident scope and impact, and agency capabilities, EIS CSS may either directly manage the information security incident or coordinate with the affected agency on the information security incident response. The EIS CSS's role may change during the information security incident.
Information Security Incident Commander	The Information Security Incident Commander has overall responsibility for managing the information security incident by establishing objectives, planning strategies, and implementing tactics. The Information Security Incident Commander is the only position that is always staffed in an Information Security Incident Command System (ICS) application. On small information security incidents and events, one person, the Information Security Incident Commander, may accomplish all management functions. The Information Security Incident Commander is responsible for all ICS management functions until they delegate those functions. Depending on the scope and severity of the information security incident, the Information Security Incident Commander may be a representative of EIS CSS or the agency.
Information Security Incident Command System (ICS)	A standardized information security 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.
Information Security Incident Response Lead	See Information Security Incident Commander

Roles	Responsibilities
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 information security 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 (CJI), and the Oregon State Police (OSP) through which the unit or program interfaces with the FBI Criminal Justice Information Services (CJIS) Division. The LASO actively represents their agency in all matters pertaining to CJIS, 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 CJIS needs and problems.
ODHS and OHA Communications Offices	Responsible for coordinated release of information about information security incidents to the public, under the direction of the Information Security Incident Commander. In the event of a public release and depending upon the scope of the information security 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 (OEM)	Responsible for maintaining the state Emergency Operations Plan. 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 information security incidents with a Severity Level High or Critical, OEM may be called upon to facilitate coordination of response efforts.
Privacy	Provides guidance and oversight regarding the creation,

Roles	Responsibilities
Compliance Officer	maintenance, use, transmission, and destruction of PHI and PII. Participates in the review and the response to privacy related inquiries and information security incidents. Serves as the ODHS and OHA Privacy Official for privacy concerns associated with HIPAA.
Information Security Incident Response Team (IRT)	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 information security incident scope and severity, it will contain the following common elements regardless of size: an information security 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 information security 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.

1.0 PREPARATION

PREPARATION
Preparation is the most important step in the information security incident life cycle – the cycle begins and ends with preparation. This IRP is intended to be flexible and scalable as is the organization of the information security incident response team. This section is designed to depict the information security incident management structure that will be utilized for an information security incident.

1. Information Security Incident Command System (ICS)

ODHS and OHA support, in coordination with EIS-CSS and EIS-SOC, a standardized approach to the command, control, and coordination of emergency response. Data security incidents are managed by utilizing key concepts of ICS. Although first responders may be general IT staff, ICS provides a flexible management framework that changes with information security incident scope, severity, and resource needs.

A. Key Concepts of ICS

- Unity of command (each response individual reports to only one supervisor).
- Common terminology (avoid acronyms and other specialty language/terms).
- Management by objective (clear objectives spelled out for the response team; specific strategies and tactics for how to accomplish objectives).
- Flexible and modular organization (flex the management and response structure to the size and severity of the information security incident.

B. Stand-up of ICS

- The lead IT individual (the person leading the initial investigation into an information security event/incident will stand up ICS at the onset of an event investigation and is now the designated Information Security Incident Commander (IC).

- The agency incident commander will mobilize and manage the IRT tasked with addressing the event or potential information security incident.

2. Information Security Incident Commander

A. Designation of an IC

- An Information Security Incident Commander will be designated and will stand-up the ICS for an information security incident response. This individual is typically the lead IT technical expert who is actively involved in managing the technical response effort. In a severity Level Medium IT event, (as defined by EIS) however, the IC designation may be passed to an IT Manager while the CIO or a Senior IT Manager assumes a high-level information security incident management role within the ICS.

B. Transfer of IC Designation

- An individual must actively be able to perform all required IC duties before assuming the role of IC.
- If an individual is unavailable to perform the role of IC, a suitable replacement must be designated.
- IC's may request a higher-level manager assume IC responsibility for an information security incident and higher-level managers may assume IC responsibility at their discretion and at any time.

3. Information Security Incident Commander Responsibilities

The IC has primary responsibility for managing and coordinating the ICS Team activities and has the following responsibilities:

- Primary contact for information security events or incidents reported.
- Convenes the IRT Team, as necessary.
- Coordinates, establishes, and manages the ICS & IRT, including establishing an onsite or virtual room that can be used as a centralized meeting place and information repository.
- Oversees communication during the information security incident response process in situations that do not involve public affairs.
- Coordinates information security incident briefings with the ICS members to review the nature of the information security incident and develop the response strategy.
- Conducts regular incident response updates.
- Develops an action plan that documents the nature of the information security incident and the goals and strategies of the ICS in responding to the information security incident.

- Obtains appropriate approval of the recommended action plan and other key decisions throughout the information security incident response process.
- Continuously monitors and assesses the information security incident status and the severity level (e.g., level of technology disruption and implications for sensitive information), and appropriate ICS strategic and tactical objectives.
- Oversees execution of the recommendations and tracks progress.
- Ensures tactics are in place for meeting applicable regulatory and contractual deadlines and obligations.
- Coordinates "lessons learned" after action review with ICS Team.
- Ensures each ICS & IRT member is aware of his or her general responsibilities.

4. Incident Response Team (IRT)

The IRT may be activated at any time and at the appropriate level necessary to address an event or potential information security incident. This team's first effort during an information security incident is to take control of the situation and prevent or minimize damage to ODHS and OHA and its partners. It is the team's responsibility to:

- Implement and monitor an information security event or incident identification and escalation procedure.
- Manage the information security incident response process for a specific information security event or incident.
- Defend against attacks and prevent further damage from occurring when an information security event or incident occurs.
- Recover systems, data, and operations.
- Implement improvements that prevent attacks from reoccurring.
- Support the IC, based on information security event or incident level and characteristics.
- Review information security incident reports after an event or incident has been remediated and gather lessons learned for future responses.
- Participate in training and tabletop exercises so team members are trained to execute the plan.
- Review the plan on an annual basis and update as needed.

5. ISPO

ISPO staff provide the following services: Privacy and information security incident management, breach notification support, risk management oversight, Information Exchange (Third-Party Access), eDiscovery and litigation, awareness, and education (privacy and security), vulnerability management, audit and security support services, cyber risk and information security incident response support, and policy and process development for privacy, security, and information technology.

ISPO provides a focal point of authority, information sharing, and coordination of the overall information security incident response. The ICS will be activated whenever an information security incident has been declared by the Chief Information Risk Officer or delegate. ISPO will handle third party security vendor breaches or compromise that affects the agency resources.

6. ICS Representatives

The ICS is comprised of ODHS and OHA representatives from a variety of departments and programs including but not limited to Executive Team members, affected business/operational areas, Communications, and Legal. (Refer to Appendices E and H outlining ICS representatives that may be activated as part of a response). Also, see Figure 1 below.

The actual staffing of the ICS will be determined by the nature and severity of the information security incident. Consultation with the Department of Justice (DOJ) is dependent on the level of the security event and the data potentially compromised.

7. Third Party Security Vendors, Legal Assistance, External Resources

Due to the complicated nature of an information security incident response and the many legal, financial, and business-related implications, ODHS and OHA may work with the EIS CSS if assistance of vendors and external firms are required to help with response efforts. These external resources may include outside legal counsel, forensics investigators, credit monitoring/identity restoration services, and public relations firms.

8. Information Security Incident Escalation

There are several levels of escalation with regards to the magnitude of the information security incident and the reporting requirements. The personnel needed to manage the response will vary with each level. The IC will utilize their own discretion when escalating information security incidents to the next higher-level entity.

(Refer to the Statewide Information Security Incident Response Plan that outlines the escalation process in Appendix C)

9. Information Security Incident Communication & Reporting

Reports of an information security event or potential incidents can come from many sources. Once identified, all information security incidents should be handled by opening a dedicated collaboration channel.

10. Testing the Plan

On an annual basis, a simulated information security incident, commonly known as a tabletop exercise, will be run to exercise the information security ICS & IRT, the information security incident ISPO staff, and this plan. These exercises will improve

the performance of all responsible parties and will help identify issues with related policies, processes, and communication. The Chief Information Risk Officer will be responsible for determining when a simulated information security incident must be planned, the type and severity of the information security incident to be tested and facilitating the event.

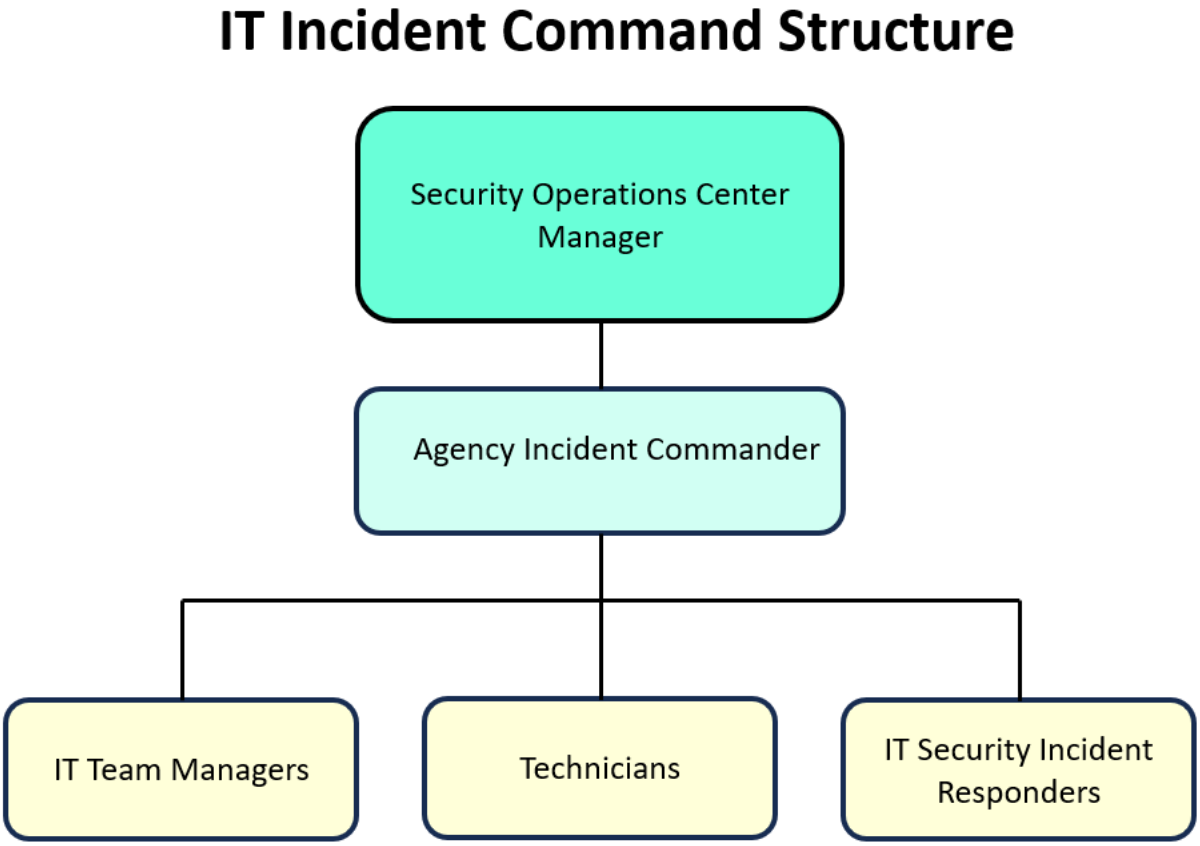


Figure 1

Figure 1 depicts all entities that may become part of the ICS structure when responding to and resolving an information security incident. Refer to Appendix E for specific individuals assigned to each position and their associated contact information.

2.0 DETECTION AND ANALYSIS

1. Identification and Escalation of an Information Security Incident

Reports of potential privacy or data security concerns can come from many sources. Identification typically begins after a user, system operator, employee, partner, vendor, or third party has noticed unusual or suspicious behavior in a system, network, or other business process. Employees, partners, vendors, business associates or authorities may all report a potential information security incident in a variety of entry points throughout the organization. ODHS and OHA conducts training to educate and encourage immediate reporting of an information security incident to the ISPO.

Staff must immediately report an information security incident to the Service Desk, their Manager/Supervisor and ISPO by any communications means necessary, i.e., phone, email, messaging services, etc. If there is a suspected data compromise (i.e., CJI, FTI, PII, PHI, or SSA data), staff shall submit an online notification using the Online Privacy Incident Reporting Form.

The IC will conduct an initial review of the details of a newly reported event and establish the Information Security IRT as necessary. The IC will be responsible for, directly or through delegation, the collection of documents and evidence, as well as documenting the chronology of the investigation and resolution.

The identification phase involves a determination of whether an information security incident has occurred, and if so, the nature and severity of the information security incident. This also includes informing and soliciting help from people who can assist in investigating, escalating, and scoping the information security incident (i.e., establishing the ICS Team).

2. Triage

This is the phase where events are triaged and could become information security incidents. If an event becomes an information security incident, the situation is assessed in this phase to determine the proper course of action for the follow-on Information Security Incident Response phases. The workflow for Phase Two is

depicted in Figure 2.1. The information security incident can be moved to Phase Three once step 2.2 (Assess the Situation) has been completed.

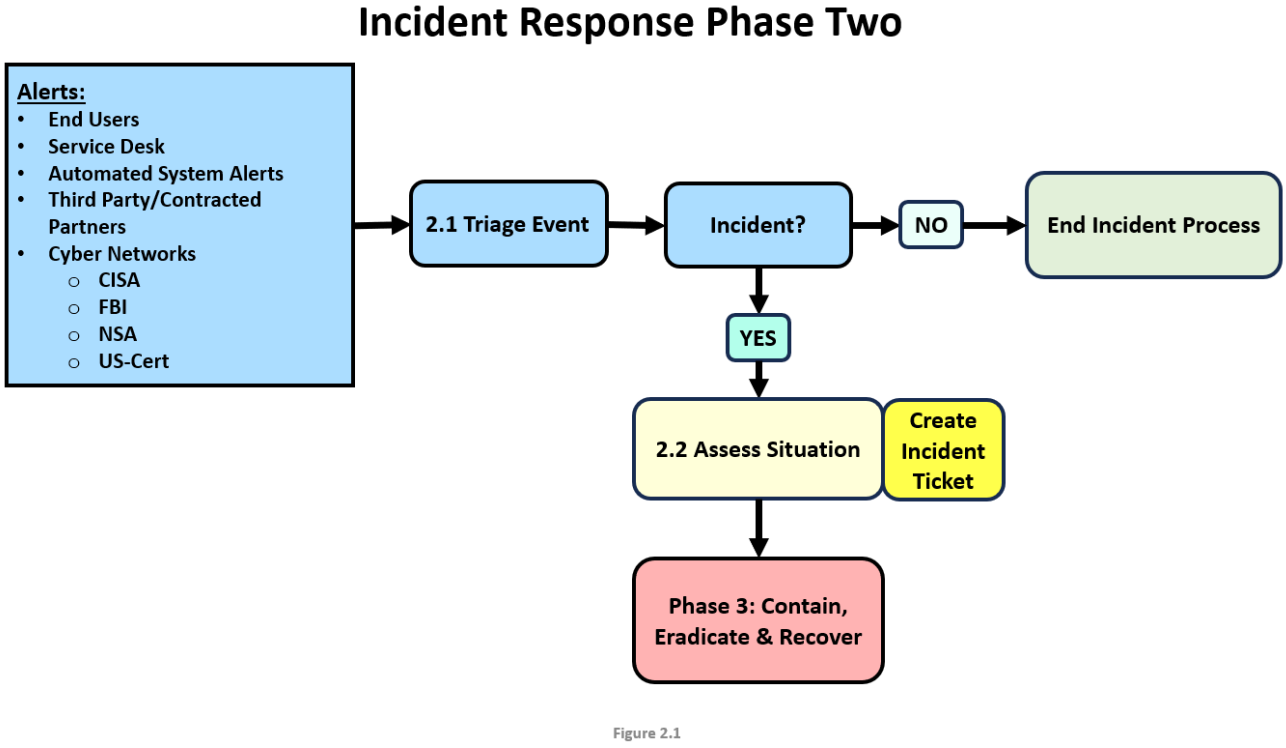


Figure 2.1: Information Security Incident Response Phase Two (Detect/Analysis)

3. Containment

The workflow for Phase Three is depicted in Figure 3.1. The information security incident can be moved to Phase Four once steps 3.2 (Implement Asset Continuity Procedures) and 3.3 (Gather/Preserve Information Security Incident Data) have both been completed.

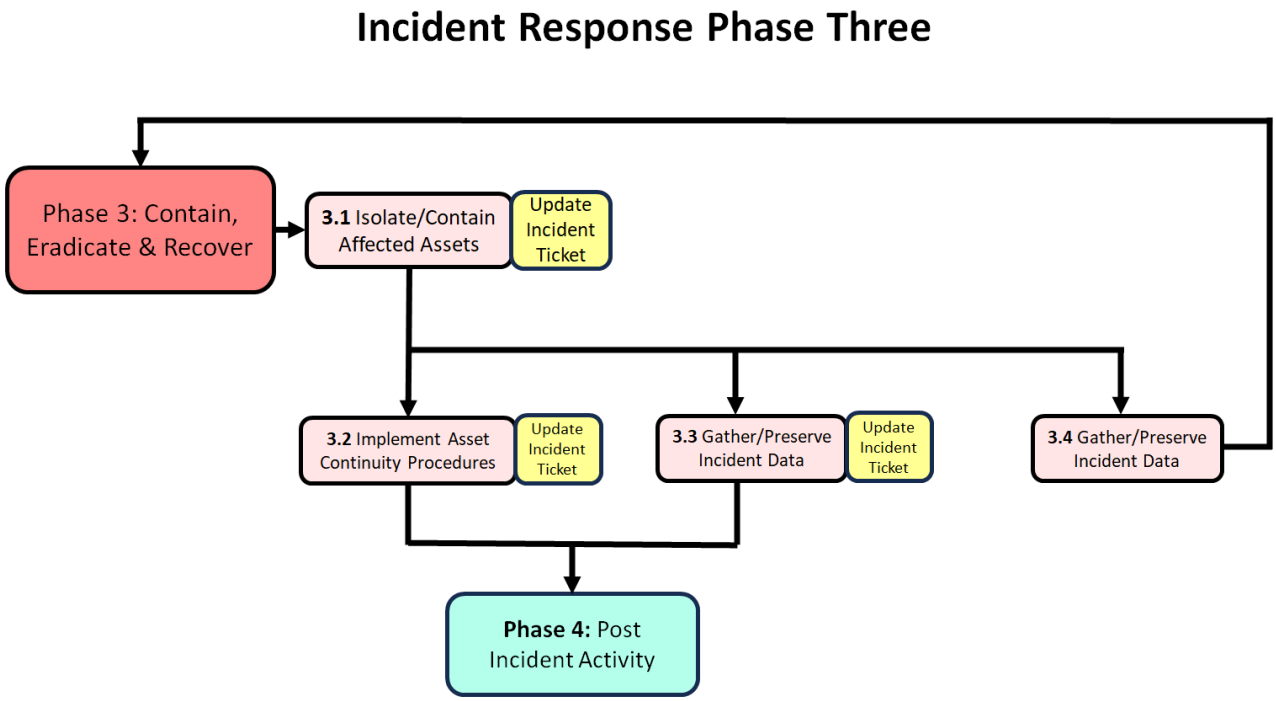


Figure 3.1: Information Security Incident Response Phase Three (Contain/Eradicate/Recover)

During the detection and analysis phase, the Team can begin to implement containment as needed to isolate the issues, preserve evidence, and protect affected systems. (Refer to Regulatory Information Security Incident Response Supplemental Information in Appendix F). A few key actions to consider are:

- Physically Secure Area. Restrict physical access to the area where the information security incident or compromised system(s) is/are located if possible and applicable.
- Documentation & Communication. Clearly communicate and document all information regarding the information security incident.
- Identify Data at Risk. If Sensitive Information is at risk, the investigation should focus on obtaining details that will assist DOJ in the assessment of risk and regulatory obligations.

4. Confidentiality & Legal Privilege

Confidentiality

All information regarding information security incidents must be treated as confidential. Do not discuss, share, forward or otherwise disseminate information

related to the information security incident to any person not directly involved in the investigation.
Furthermore, information obtained during the investigation should not be shared in any way with any person who is implicated in the information security incident. This is true even if the person implicated is the person to whom the employee reports.

There may not be an information security incident commander at the time the information security incident is witnessed. If the information security incident involves a person to whom the direct supervisor of the employee-witness reports (either direct supervisor or in their chain of command), then staff should notify the Chief Information Risk Officer and/or Chief Information Officer and/or Human Resources. The IC can designate the use of alternative communication methods at any time during an information security incident if there is concern the primary communication methods are compromised.

Legal Privilege
ODHS and OHA will follow DOJ direction to support documentation and investigation work product requirements when appropriate.

5. Coordination with External Parties

Coordinate with external parties (Refer to ICS Team Members in Appendix E) as part of the response, as needed, but only after proper approval has been secured by the IC. The team may consider additional third parties depending on the type of incident, such as internet service providers (ISPs), software or hardware vendors, or special interest groups, such as specialist security or professional associations.

The Regulatory Information Incident Response Supplemental Information in Appendix F includes guidance on contacting third parties with a potential notification requirement, such as:

- Impacted parties (i.e., partners, employees, or third-party vendors).

Only authorized individuals will be involved in external communications, such as communications to the media or partners, and they will issue only approved messaging. **No external public communications are permitted without the prior consent of the IC in coordination with ODHS or OHA Communications.** All information is shared on a need-to-know basis with only the necessary people engaged and informed as information leakage can damage the effectiveness of response.

6. Handling of Systems Involved in the Information Security Incident

If the information security incident stems from a compromise of security of electronic records, computer systems, computer networks, or the physical environment wherein Assets exist, the Information Security ICS Team members will refer to and follow guidelines in the Agency Information Security Incident Response Playbook.

7. Documentation

From the very beginning of a suspected information security incident, all ICS Team members should take notes of each step in their process and involvement. It is best if the notes are chronological, with the time of each entry indicated. The notes should be as factual as possible; care should be taken to avoid speculation, as speculation can confuse the evaluation of the information security incident. The IC or his/her delegate will be responsible for collecting and summarizing all Team members' notes.

8. Collect and Preserve Information

For most information security incidents, evidence collection and forensics is the responsibility of CSS SOC, with agency personnel supporting collection as appropriate. The general Enterprise goal of evidence collection and forensics is to facilitate rapid containment and recovery. Information security incidents that have criminal implications will be coordinated with law enforcement and with support from assigned staff from the Department of Justice (DOJ).

3.0 CONTAINMENT, ERADICATION & RECOVERY

CONTAINMENT, ERADICATION AND RECOVERY

This Section describes the overall goals and responsibility for information security incident containment, eradication, and recovery. The ICS Team should refer to and follow guidelines in the Agency IR Playbook.

1. Containment

The IC is responsible for directing the development of a containment recommendation for review and approval by the ICS Team members and/or the EIS CSS Security Operations Center (SOC) as appropriate.

2. Eradication

The goal of the eradication phase is to eliminate or mitigate the factors that resulted in a compromise of system security. If the source of the compromise is not eradicated, it will likely be magnified, resulting in a much larger compromise. The ICS team should perform a vulnerability analysis, improve system defense, remove the cause of the information security incident, and address other viruses, malicious codes, network intrusions and encryption attacks.

3. Remediation

Technical remediation involves providing whatever technical support is necessary to update software, repair hardware, or otherwise move the system toward recovery. Legal remediation involves assessing the impact on affected consumers, identifying legal notification obligations, and determining whether offering credit monitoring or identity theft restoration services would be appropriate.

4. Recovery

The recovery phase returns the system(s) to full operational status.

4.0 POST-INCIDENT ACTIVITY

POST INFORMATION SECURITY INCIDENT ACTIVITY

This section provides the ICS Team with lessons learned evaluation of the effectiveness and efficiency for information security incidents and a framework for the post information security incident response. After recovery, ISPO and EIS CSS will conduct a "lessons learned" exercise for all Team members after distributing a detailed post information security incident report. The distribution of the post information security incident report will depend on the scope of the information security incident: if it's a very large, multi-agency information security incident, CSS will be responsible for the After-Action Report, with each agency responsible for implementing agency-specific protection measures. If it's a single agency information security incident, responsibility will be shared between CSS and the agency.

The IC and ICS Team will plan and facilitate the exercise, addressing the following questions:

- What happened exactly? At what times?
- How well did staff and management deal with the information security incident? Were documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps taken that might have inhibited recovery?
- What would staff, or management do differently the next time a similar information security incident occurs?
- What corrective actions can prevent a future similar information security incident?
- What additional tools or resources are needed to detect, analyze, and mitigate future information security incidents?
- What can be done in both the short-and long-term to increase the ODHS and OHA security posture?

Using the information from the lessons-learned exercise, the IC will draft a follow-up report, in coordination with the ICS Team, to identify gaps and highlighting opportunities of how the information gathered can better protect ODHS and OHA

in the future. All Teams will review the report to support corrective action and changes to respective playbooks. Feedback from all interested teams will be gathered and documented as part of the final lessons learned report.

The IC will submit the final report to the CIRO for review and approval. In instances where the CIRO is the IC, the report will be submitted to the CIO for review and approval. Upon approval, an individual designated by the IC will provide an executive summary of the information security incident and final recommendations to management. Relevant information may include information security incident response education and training, or operational staff training needs, infrastructure tools and resources needed (total costs and impacts of the information security incident), a cost estimate for recommended changes, a high-level schedule, and the impact of implementing or not implementing the recommended actions.

Changes should be considered at three levels:

- Information Security Incident: Improve defenses specific to preventing the actions that led to the most recent information security incident.
- Process: Improve the people, process, and technology elements of the plan based on the most recent response with a goal of reducing the risk of further information security incidents.
- Program: Improve elements of the overall security program based on the most recent information security incident and response.

The IC and key Team members shall prepare a mitigation plan and/or remediation plan. The steps taken for corrective action will be documented by the IC and included in the information security incident documentation. The CIRO will be updated on a regular basis regarding the progress on implementing the mitigation plan and/or remediation plan.

Awareness & Education

It is vital to implement a continuous education and awareness program to help empower the workforce to adopt good security habits at work, home, and while mobile. The goal of the program is to change human behavior and reduce information risk, thereby increasing the overall security posture of ODHS and OHA.

Awareness and education programs will include information security incident response and cover what to do in the event of an information security incident such as a data breach, insider threat, malware attack, or network intrusion.

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

- Ongoing assessment of the IRP

- Agency needs (e.g., tools, resources, etc.)
- Evaluation of the overall effectiveness of the IRP

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

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

APENDIX A:
Authority & Compliance

Compliance

ODHS and OHA are 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 interested parties is responsible for supporting the overall oversight and compliance function for both ODHS and OHA.

ORS 276A.300 requires agencies to develop the capacity to respond to information security incidents that involve the security of information. Agencies must implement forensic techniques and controls, and consider lessons learned. The statute also requires reporting information security incidents and plans to the EIS 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.

Regulatory Requirements

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
Center for Internet 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
Acceptable Risk Controls for Affordable Care Act for Medicaid Partner Entities
Statewide Information Technology (IT) Control Standards

Statewide Technology and Security Policies:

107-004-050 Information Asset Classification
107-004-051 Controlling Portable and Removable Storage Devices
107-004-052 Cyber and Information Security
107-004-053 Employee Security
107-004-100 Transporting Information Assets
107-004-110 Acceptable Use of State Information Assets
107-004-120 Cyber and Information Security Incident Response
107-004-140 Privileged Access to Information Systems
107-004-150 Cloud and Hosted Systems Policy

ODHS and OHA Information Security Policies and Incident Reporting Processes:

ODHSOHA 090-003 Access Control Policy
ODHSOHA 090-004 Information Security and Privacy Awareness and Training Policy
ODHSOHA 090-005 Information Security Incident Management Policy
ODHSOHA 090-005-01 Information Security Incident Reporting Process
ODHSOHA 090-006 Information Security Risk Assessment Policy
ODHSOHA 090-007 Information Technology Vulnerability Management Policy
ODHSOHA 090-009 Administrative, Technical and Physical Safeguards of Information Policy
ODHSOHA 090-011 Media Protection and Disposal Policy
ODHSOHA 090-012 Information System Maintenance Policy
ODHSOHA 090-013 Administrative Privileges Policy
ODHSOHA 090-014 Password Policy
ODHSOHA 090-015 Email Security Policy
ODHSOHA 090-016 Information Technology Risk Management Policy
ODHSOHA 100-014 Report and Response to Privacy Incidents

APPENDIX B:
Technology Governance Structure

APPENDIX C:
Escalation Steps and Definitions

Statewide Information Security Incident Response Plan

The Statewide plan includes:

Information Security Incident Severity and Classification
Information Security Incident severity determination answers the question "*What is the overall impact of the information security incident on the State of Oregon?*" Accordingly, incident severity ratings drive incident routing, escalation, escalation urgency, and composition of the IRT to respond appropriately to incidents. Incident severity may change in response to factors such as scope change, increased publicity, or other escalation factor.

Escalation and Escalation Communications
Different level information security incidents require different types of resources, communication strategies and levels of authority to respond. Information security incidents and response circumstances may change, often quickly, requiring smooth escalation of response efforts. Below is the Escalation Based Severity Levels and Prompts graph.

Communications
Maintaining communications security is critical while responding to information security incidents. Every effort must be taken to preserve the confidentiality of incidents; for that reason, all communications shall be on a need-to-know basis.

Follow the Data Breach Reporting Protocol in the Executive Branch Agency Breach Response Protocol.

ESCALATION AND ESCALATION BASED COMMUNICATIONS

ESCALATION PROMPTS

- Publicity
- Scope
- Responsibility/authority
- Lack of resources
- Political sensitivity
- Mismanagement (perceived or actual)

Escalation Level	Involved Parties	Communications*
SEVERITY LEVEL: INFORMATIONAL **Example Prompts:** Initial detection, routine, triage	Agency IT Staff	**Agency Notifies** Internal Staff (as applicable)
SEVERITY LEVEL: LOW **Example Prompts** Agency determines that it meets definition of information security incident	Agency IT Staff CSS SOC (advisory as applicable) DCS Staff (as applicable) No/Little Management Involvement	**Agency Notifies** CSS
SEVERITY LEVEL: MEDIUM **Example Prompts** Significant impact to 1 agency Potential or actual media coverage	Agency CIO Agency PIO CSS SOC State CISO Agency Management (as applicable)	**Agency/CSS Notifies** DOJ (as applicable) **CSS Notifies** State CISO LFO
SEVERITY LEVEL: HIGH **Example Prompts** Multi-Agency, wide-spread impact Significant impact to multiple agencies Statewide press coverage Potential for serious impact to state (e.g. reputation, regulatory)	Agency Executive Management (as applicable) Agency CISO/CIO(s) (multiple agencies) Agency/State/Governor's PIO CSS SOC State CISO State CIO DCS Administrator (as applicable) DOJ	**CSS Notifies** Governor's Office State CIO (if not already involved) (Optional) OEM/OERS at 1.800.452.0311 **CSS & Agency** Law enforcement (consult DOJ)

Escalation Level	Involved Parties	Communications*
SEVERITY LEVEL: CRITICAL **Example Prompts:** Scope beyond just State Agencies (public/private) High impact to citizens National press interest Serious statewide or multi- state impact	**EOC ACTIVATED** Governor Representative State CISO State CIO (as applicable) DCS Administrator (as applicable) Agency Director (as applicable) Agency/State/Governor's PIO (as applicable) DAS Director TAG – OEM Governor RPC (as applicable) EO 08-20 Governor GRC (as applicable) EO 08-20 DOJ	**CSS Notifies** (if not already involved) MS-ISAC Fusion Center OEM/OERS *Communications should be assumed to be additive, whereby lower levels also includes the notifications of the previous level(s).

APPENDIX D:
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, that can be of administrative, technical, physical, management, or legal nature.

Event: An observable occurrence in a network or information system.

Evidence Preservation: The process of maintaining the integrity of the evidence for later testing or analysis.

Information Security Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Information Security Incident Identification: The process of recognizing and assessing an information security incident to determine the appropriate response.

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

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

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

Information Security Incident Response Program: Combination of information security incident response policy, plan, and processes.

Information Security Incident Log: A record of the events occurring 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 Asset Classification: A critical first step to ensure that the state's information assets have a level of protection corresponding to their sensitivity and value. All state agency information must be classified and protected based on its confidentiality and sensitivity requirements.

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 during 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 username 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 username 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 username, 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 protected by law, rule, regulation, or contract. This can be Protected Health Information as defined by the Health Insurance Portability and Accountability Act (HIPAA), Personal Information as defined by the Oregon Consumer Information Protection Act (OCIPA), and the Oregon Consumer Privacy Act (OCPA), Social Security Administration (SSA), Federal Tax Information (FTI) and Criminal Justice Information (CJI)

APPENDIX E
Information Security Incident Command System: Incident Response Team Members

NOTE: All core and auxiliary ICS & IRT Members should keep a current copy of the Plan in other locations (e.g., desk, home, car)

Core ICS & IRT Team Members		
ICS Position	**Name and Job Title**	**Contact Information**
Agency Information Security Incident Commander	IT Regulatory Compliance Manager	DHS.Infosecurity@odhsoha.oregon.gov
	Information Security Risk and Compliance	DHS.Infosecurity@odhsoha.oregon.gov
IT Team Managers	IT Infrastructure Operations	INFRAOPS@odhsoha.oregon.gov
	Endpoint Security Team	workstation.management@odhsoha.oregon.gov
	Incident Management Team	DHS.OIS-IncidentMgt@odhsoha.oregon.gov
Senior IT Leadership	Chief Information Officer	Debbie.Estabrook@odhsoha.oregon.gov
	Deputy Chief Information Officer	Travis.Paakki@odhsoha.oregon.gov
	Chief Information Risk Officer	Kristine.M.Cornett@odhsoha.oregon.gov
	Chief Technology Officer	SIMON.HAYES@odhsoha.oregon.gov
ISPO	Privacy Compliance Officer	Lyssette.Young@odhsoha.oregon.gov dhs.privacyhelp@odhsoha.oregon.gov
	CJIS Administrator and LASO	Frank.t.miles@odhsoha.oregon.gov

DAS	EIS Security Operations Center	SOC Hotline: 503.378.5930 eso.soc@das.oregon.gov
Third Party Security Incident Response	MS-ISAC Security Operations Center	866-787-4722 soc@cisecurity.org

APPENDIX F
Regulatory Information Security Incident Response Supplemental Information

The Privacy Compliance Officer will advise the ICS & IRT Teams and the Agency of the legal and regulatory reporting obligations upon notification of a data disclosure. The Privacy Compliance Officer will inform or seek out the Office of the Attorney General (AG) for any Department of Justice services if additional counsel is needed.

The regulatory authority and role in the IRP are referred to the Privacy Compliance Officer. The Agency's Privacy Compliance Officer will act in full authority and responsibility for analysis of regulatory breach reporting obligations at the federal and state levels and will work closely with the ICS & IRT Teams to assess and comply with those obligations.

The Office of the Attorney General (AG) will be sought when there is a criminal act of wrong that results, in the opinion of the Oregon State Police, as a cyber-crime.

GUIDANCE FOR IMPACTED DATA -Privacy Compliance Officer

Analysis and remediation in an information security incident involving affected individuals requires a risk analysis of the data disclosed and evaluation of the impact on affected individuals. The Privacy Compliance Officer will identify level of risk (probability of compromise), reporting and notification obligations, and if credit monitoring or identity theft protection services would be appropriate.

Other factors to consider:

- Classification of Data compromised and disclosed (level 1, 2, 3, 4)
- Impact to individuals.
- Volume of data records affected.
- Notification to business and community partners, contractors, and business associates.
- Security controls of impacted data (such as encryption) and discern high, medium, or low probability of compromise.
- Address reporting requirements for different data classifications (FTI, SSA, PHI, CJI etc.)
- Notification requirements, including timing, content, website, and other public notifications as required by state law.
- Notification to Attorney General's Office, Governor's Office, Tribal Affairs, or other governmental entities.
- Cause of breach (contractor or agency user) including support of contractual obligations etc.

- Discussion with Human Resources on credit monitoring availability.

Personally Identifiable Information

- Identify any (partner, contractor, or vendor) contractual provisions for breach notification (see Third Party Obligations below).
- Determine which, if any, state regulations may affect notification timing or methodology.
- Assess requirements for telecommunications service providers or hosting vendors, if relevant.
- Define notification strategy.
- Engage agency's communications office to help develop and manage internal and external communication, including media strategy.
- Draft notification letters or scripts, along with internal talking points.
- Ensure all communication is approved by the Agency or other levels of authority.
- Coordinate and execute third-party notification.
- Monitor social media and communication plans.
- Execute an information security incident debrief to facilitate process improvement.

Third Party Obligations: Partners and Contractors

- In the event of a third-party breach, the Privacy Compliance Officer will work with Third Party reporting partners and contractors regarding advisory and consulting services to support appropriate remediation steps and reporting. The Agency is not responsible for dictating or reporting on third party breaches unless there is a global impact that may cause harm to the State of Oregon.

The Privacy Compliance Officer may take the following measures:

- Inform Agency Executive Leadership, Attorney General's Office, and enforcement agency's when appropriate.
- Inform the Governor's Office.
- Identify business associate agreements when appropriate.
- Engage Agency's communications office to help develop and manage internal and external communications, including media strategy.
- Draft notification letters or scripts, along with internal talking points.
- Coordinate and review third party notification.
    - Monitor media and other communication outlets for transparency of information.

APPENDIX G
Law Enforcement Notifications

Local Law Enforcement
ODHS and OHA in coordination with ICS is responsible for deciding which agencies to involve, depending on the nature of the information security incident. (Oregon State Police, Federal Bureau of Investigations (FBI)

FBI
9109 NE Cascades Pkwy.
Portland, OR 97220
portland.fbi.gov
(503) 224-4181

Oregon State Police (OSP)
Criminal Justice Information Services Division
LEDS Help Desk – available 24 hours a day
3565 Trelstad Ave. SE
Salem, OR 97317
Email: helpdesk.leds@osp.oregon.gov
Phone: 503-378-5565
Fax: 503-588-1378

Oregon State Police Command Centers
For non-emergency assistance, contact OSP in the following ways:

- Dial *OSP or *677 if you are calling from a mobile phone; or,
- Northern Command Center (NCC)
  Phone: 800-442-0776
  Non-emergency assistance for these counties: Benton, Clackamas, Clatsop, Columbia, Crook, Deschutes, Gilliam, Hood River, Jefferson, Klamath, Lane, Lincoln, Linn, Marion, Multnomah, Polk, Sherman, Tillamook, Wasco, Washington, Wheeler, and Yamhill.
- Southern Command Center (SCC)
  Phone:800-442-2068
  non-emergency assistance for these counties: Baker, Coos, Curry, Douglas, Grant, Harney, Jackson, Josephine, parts of Klamath, Lake, Malheur, Morrow, Umatilla, Union, and Wallowa.

If unsure about which OSP dispatch to dial, call either the NCC or SCC for assistance.

OSP General Headquarters (Administration Office)
3565 Trelstad Avenue SE,
Salem, OR 97317
Email: ask.osp@osp.oregon.gov
Phone: 503-378-3720
Fax: 503-378-8282
Hours: 8:00 AM-5:00 PM

APPENDIX H:
Points of Contact

Internal Agency ODHS and OHA Notifications:

- ODHSOHA Chief Information Officer-Debbie Estabrook: 971-600-6429
- ODHSOHA Chief Information Risk Officer-Kristine Cornett: 503-689-2767
- ODHSOHA Privacy Compliance Officer Lyssette Young 503-881-4443
- ODHS Agency Director-Fariborz Pakseresht: 503-945-5600
- Liesl Wendt Deputy Chief: 503-891-2607
- ODHS Chief Operating Officer-Seth Lyon: 971-673-7212
- OHA Agency Director-Dr. Sejal Hathi: 971-446-1555
- OHA Deputy Director-Kris Kautz: 503-383-5147
- ODHS|OHA CJIS Local Agency Security Officer--Frank Miles: 503-507-7851

Department of Administrative Services (DAS):

- Department of Administrative Services (DAS) Enterprise information Services (EIS) Cyber Security Services (CSS) Security Operations (SOC) Hotline: 503-378-5930
- DAS EIS CSS Chief Information Security Officer-Ben Gherezgiher: 503-586-6978
- State Chief Information Officer-Terrence Woods: 503-378-3175
- DAS State Chief Operating Officer and DAS Director-Berri Leslie: 503-378-5797
- DAS Office Communication Director-Andrea Chiapella: 971-345-1333

Agency Communications Division, ODHS Directors Office:

- Lisa Morawski- Lisa.Morawski@odhs.oregon.gov (503) 8714828
- OIS Communications - ois.communications@odhsoha.oregon.gov
- OHA External Communications - oha.externalrelations@odhsoha.oregon.gov
- ODHS Communications: 503-945-5600: Communications.DHS@odhsoha.oregon.gov

Governor's Office Public Affairs and Communications:

- Press Line: 503-378-5965
- Public Affairs and Communications Director, Elisabeth Shepard elisabeth.shepard@oregon.gov
- Public Affairs and Communications Assistant, Katie DeVore, Katie.DeVore@oregon.gov
- Press Secretary, Anca Matica, anca.matica@oregon.gov
- Press Secretary, Roxy Mayer, roxy.mayer@oregon.gov

Breach Reporting Agencies:

- Attorney General's Office -Oregon Department of Justice (DOJ)-Ellen Flint: 503-947-4342 and Online Reporting tool
- Federal Bureau of Investigations (FBI)-Portland: 503-224-4181 and IC3 Complaint Form online reporting.
- Oregon State Police: 503-378-3720 (Ask for Cybersecurity Investigative Team or Criminal Lieutenant)
- Oregon State Police Northern Command Center: 503-442-0776
- Oregon State Police CJIS Information Security Officer-Nicholas Harris: (503)302-7269
- Social Security Administration (SSA): 877-697-4889
- Internal Revenue Services (IRS) Treasury Inspector General for Tax Administration (TIGTA): Hotline Number: 800-366-4484; If unable to contact TIGTA: 800-589-3718
- Center for Medicare and Medicaid Services (CMS) Office of Communications: 202- 690-6145
- DHHS Office of Civil Rights (OCR)-Online Reporting
- Credit Monitoring Bureaus:
    - o Equifax: 1-888-378-4329
    - o Experian: 1-888-397-3742
    - o TransUnion: 1-800-916-8800

Approvals

By: Kristine M. Cornett 12/16/24

Kristine Cornett, Chief Information Risk Officer Date

By: Debra L. Estabrook 1/16/2025

Debbie Estabrook, Chief Information Officer Date

By: Kristine M Kaub 1/16/25

OHA Agency Director or Designee Date

By: 1/16/2025

ODHS Agency Director or Designee Date