Security Incident Response Procedures

December 1, 2015

California Health and Human Services Agency, Office of Systems Integration

REVISION HISTORY			
REVISION #	**DATE OF RELEASE**	**OWNER**	**SUMMARY OF CHANGES**
OR	December 1, 2015	B. Hale	Initial Release

Table of Contents

1. Purpose

In support of OSI Information Security Incident Response Plan, OSI-AP-15-02, this document establishes the process by which the Information Security Officer (ISO) and the Chief Technology Officer (CTO) responds to security incidents. The process begins with a reported incident or potential incident and ends with required reporting and completion of applicable corrective actions.

2. Scope

This procedure applies to all OSI full-time or part-time employees, student assistants, contractors, and volunteers.

3. Terms and Definitions

ENTAC: California Highway Patrol Emergency Notification and Tactical Alert Center.

Information Security Incidents: An information security incident is any event that is reasonably believed to have compromised the confidentiality, integrity, or availability of an information asset, system, process, data storage, or transmission. Furthermore, an information security incident may also include an event that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. The Reporting Criteria section of SIMM 5340-A Incident Reporting and Response Instructions provides a list of incidents that must be reported to the California Highway Patrol (CHP) Emergency Notification and Tactical Alert Center (ENTAC).

Additionally, the following are also information security incidents:

- **Physical Intrusions into Facilities**
  Any physical intrusion into facilities that may result in a compromise to state-owned data or OSI-managed data**.**
- **E-mail SPAM or Phishing**
  The receipt of unsolicited junk or bulk emails, or the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication

OTech: California Office of Technology

PII: Personally Identifiable Information – Name, Date of Birth (DOB), Social Security Number (SSN), Home Address, Home Phone Number, Financial Account Information, Driver's License Number

PHI: Personal Health Information – Individually identifiable information created, received, or maintained by such organizations as heath care payers, heath care providers, health plans, and contractor to these entities, in electronic or physical form. See Confidentiality of Medical Information Act, Civil Code Section 56 and the Patients' Access to Health Records Act, the Patients' Access to Health Records Act, Health and Safety Code Sections 123100-123149.5

State ISO: California Information Security Office

Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that might be exercised (whether accidentally or intentionally) and cause a security breach or a violation of the system's security policy.

4. Incident Response Program

The Incident Response Program documentation is composed of this document in conjunction with the State policy and procedures, the OSI Incident Response Plan, the OSI Technology Recovery Plan, and the OSI Business Continuity Plan. The following documents should be reviewed for a complete understanding of the program:

- OSI Information Security Incident Response Plan, OSI-AP-15-02
- OSI Technology Recovery Plan
- OSI Business Continuity Plan
- CHHS Procedure for Privacy and Information Security Incident Reports
- Statewide Information Management Manual 5340-A, Incident Reporting and Response Instructions
- Statewide Information Management Manual 5340-C, Requirements to Respond to Incidents Involving a Breach of Personal Information

OSI is responsible for implementing and ensuring compliance with all applicable laws, rules, policies, and regulations, including, but not limited to:

- California Government Code section 11549.3
- California Civil Code s. 1798.29(e)
- California Civil Code s. 1798.82(f)
- California Penal Code 502
- State Administrative Manual 5300, Agency Responsibilities
- State Administrative Manual 5300.2, Governing Provisions
- State Administrative Manual 5300.3, Applicability
- State Administrative Manual 5340, Information Security Incident Management
- Statewide Information Management Manual 5340-B - Information Security Incident Report

Information about security incidents will be communicated in a manner allowing timely corrective action to be taken. This document shows how OSI will handle a response to an incident, incident communication, training for response resources, and awareness training.

The Information Security Incident Response Plan and Procedures will be reviewed annually, or if significant changes occur, to ensure their continuing adequacy and effectiveness. They will also be reviewed for updates resulting from lessons learned after an incident. The OSI ISO is the owner and is responsible for its development, review, and evaluation. Reviews will include the following:

- Assessing opportunities for improvement
- Approach to managing information security incident response with regards to integrating lessons learned, changes to OSI's environment, new threats and risks, changes to business circumstances, legal and policy implications, and changes to technical environment

5. Roles and Responsibilities

OSI 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.

Chief Deputy Directory/Agency Information Officer (AIO): Assists the OSI Director. Responsible for communicating the status of the incident to Agency.

Chief Technology Officer (CTO): Incident Response Manager. Responsible for the oversight of the incident response. Leads the incident response coordination effort.

Information Security Officer (ISO): Responsible for ensuring that OSI promptly investigates security incidents. Determines reporting responsibilities. Approves corrective actions. Completes and submits mandatory incident report. Periodically reviews security policies and procedures.

Project Directors: Responsible to ensure staff is aware of incident reporting policies. Ensure customers have appropriate procedures for reporting incidents.

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.

Supervisor: Responsible to ensure staff is aware of incident reporting policies. In coordination with the Incident Response Team, mitigates the incident, collects information, and investigates incidents.

User: Responsible for complying with the provisions of the incident response policies, procedures and practices. Responsible for reporting all actual or suspected incidents. Prepared to provide assistance in any incident investigation.

6. Communications

Because of the sensitive and confidential nature of information surrounding an incident, all communication must be delivered through secure channels. Initial and detailed information of an incident should only be communicated in person, via phone, or encrypted email. Email communications should not provide details of the vulnerability that could be exploited by a "bad actor". Disclosure of incident information will be limited to individuals on a need to know basis.

Contact information for members of the Incident Response Team is contained in Appendix B to this document (OSI Security Incident Contact List).

The California Health and Human Services Agency (CHHS) Public Information Officer (PIO) or Deputy Secretary for Communications is responsible for communicating information regarding any incident to the public. The OSI Chief Deputy Director will deliver information to the CHHS PIO for distribution. OSI employees, volunteers, and contractors are not authorized to discuss any incident with the public.

7. Implementation

The following information summarizes the various functions in an incident response. They are guidelines to be considered. Another source of information is the NIST 800-61, Computer Security Incident Handling Guide.

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 OSI systems or State systems under OSI management. Events occur routinely and will be examined for impact. Those showing either harm or intent to harm may be escalated to an incident.

All users are responsible for reporting incidents and potential incidents. The OSI ISO is responsible to ensure that the analysis of potential incidents occurs.

The term "incident" refers to an adverse event impacting one or more of OSI's information assets or to the threat of such an event. Examples include, but are not limited to, the following:

- Unauthorized use
- Denial of Service
- Malicious code (malware)
- Network system failures (widespread)
- Application system failures (widespread)
- Unauthorized disclosure or loss of information
- Design vulnerability
- Web page defacing
- Loss of computing devices, either with or without data
- Compromise of authentication credentials, i.e. usernames and passwords

Incidents can result from any of the following:

- Intentional and unintentional acts
- Actions of state employees
- Actions of vendors or constituents
- Actions of third parties
- External or internal acts
- Credit card fraud
- Potential violations of State or OSI Policies
- Natural disasters and power failures
- Acts related to violence, warfare, or terrorism
- Serious wrongdoing
- Other

Incident Prioritization

Once an event is determined to be an incident, the OSI CTO and the OSI ISO are responsible for the prioritization of incidents.

The following factors are considered when evaluating and prioritizing incidents:

- Criticality of systems that are (or could be) made unavailable
- Classification and type of data, e.g. PII, PHI
- Value of the information compromised (if any)
- 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 and begin making decisions about how to respond to it. It is critical to ensure when an incident is discovered and assessed so that the situation does not become more severe.

The Incident Response Manager is responsible for the incident triage. OTech may also assist in the triage.

The following information is needed for the triage:

- What type of incident has occurred
- Who is involved
- What is the scope
- What is the urgency
- What is the impact thus far
- What is the projected impact
- What can be done to contain the incident
- Are there other vulnerable or affected systems
- What are the effects of the incident
- What actions have been taken
- Recommendations for proceeding
- Initial analysis to identify the root cause of the incident

Evidence Preservation and Forensics

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.

For information security incidents involving computers, OSI will perform a technical analysis of the computing devices to identify the cause of an incident or to preserve evidence.

OSI will practice the following general forensic guidelines:

- Keep good records of observations and actions taken.
- Make forensically-sound images of systems and retain them in a secure place.
- Establish the chain of custody for evidence.
- Provide basic forensic training to incident response staff, especially in preservation of evidence.

The Incident Response Manager is responsible for the evidence preservation and forensics. OTech and the California Computer Investigative Unit (CCIU) may also assist in the evidence preservation and forensics.

Some examples of the type of forensic information that could be gathered and analyzed are:

- Firewall logs
- Web Server logs
- Local Windows Event logs
- Domain Controller Event logs
- Comparison with baseline system configuration

Threat/Vulnerability Identification, Removal, and Repair

After an incident, efforts will focus on identifying, removing and repairing the vulnerability that led to the incident and thoroughly clean the system. To do this, the vulnerability 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.

The Incident Response Manager is responsible for the threat/vulnerability removal/repair. OTech and system vendors may also assist in the threat/vulnerability removal/repair.

Some examples of removing threats or vulnerabilities are:

- Removal of malware
- Re-image or re-build computer systems
- Delete or disable accounts
- Disable web pages

Confirmation that Threat/Vulnerability has been Mitigated

After the cause of an incident has been removed or mitigated 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 Incident Response Manager is responsible to confirm that the threat/vulnerability has been removed/mitigated. OTech and system vendors may also assist to confirm that the threat/vulnerability has been removed/mitigated.

Resumption of Operations

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

The OSI ISO, the OSI CTO, the Project Sponsor, and Project Manager are responsible to determine when to resume operation.

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 opportunity to share and document details about the incident and to facilitate lessons learned. The meetings should be held within one week of closing the incident.

Additional after incident activities can include further root cause analysis and a corrective action plan with time lines.

A report, following the format of SIMM 5340-B, will need to be completed and transmitted to the California Information Security Office (State ISO) and CHHS.

The OSI ISO, the OSI CTO, the Project Sponsor, and Project Manager are responsible for post-incident activities.

The corrective action plan time lines will be approved by the ISO, CTO, Project Sponsors, and Project Mangers.

8. Procedures

Figure 1 gives a high level view of the procedure followed in responding to a security incident.

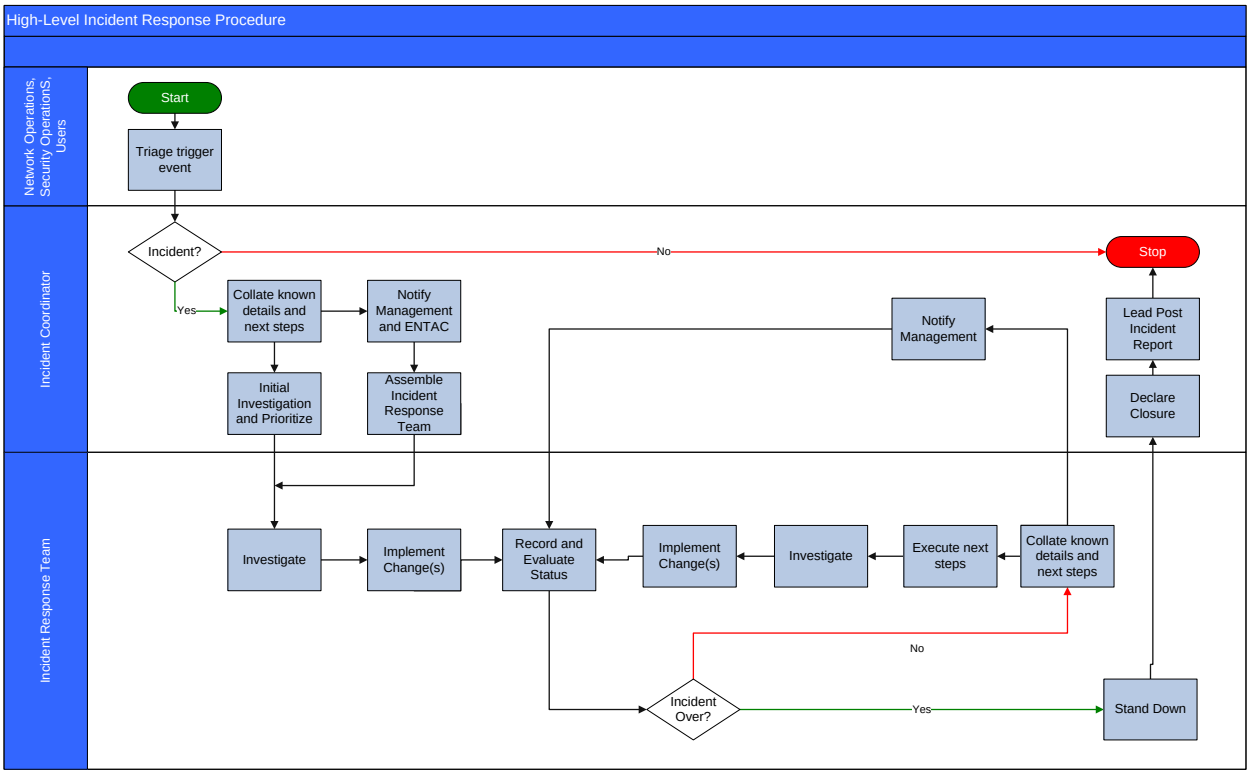

Figure 1. High-Level Incident Response Procedure

The following information summarizes the procedures that should be followed in an incident response. The details for the incident notification and reporting are contained in the following:

- SIMM 5340-A, Incident Reporting and Response Instructions
- SIMM 5340-C, Requirements to Respond to Incidents Involving a Breach of Personal Information
- CHHS Procedures for Privacy and Information Security Incident Reports

Reporting Suspected Incidents

All OSI State and Consultant Staff shall immediately report all actual or suspected information security incidents to their state supervisor and call the OSI ISO (916-825-9213) within two (2) hours of discovery and describe the incident or suspected incident. Provide as much of the following information as possible in this notification:

- Description of suspected incident
- Date and time of suspected incident
- Date and time suspected incident was discovered
- Name and phone number of person reporting suspected incident
- Indicate if there was personally identifiable information (PII), protected health information (PHI), or federal tax information (FTI) involved in the incident or if there is the potential that PII, PHI, or FTI may be compromised in the incident.
  - If the answer is yes, indicate (if known) what information may or was compromised, such as, name, Social Security Number, drivers or state identification number, health or medical information, or financial account number.
- If the number of individuals affected is known, indicate the number.
- Incident location(s).

If the incident involved removable media, indicate if the data was encrypted or was not encrypted. Specify unknown if you do not know whether it is encrypted.

Initial Investigation, Prioritization, and Initial Report

The ISO will perform a preliminary investigation and determine if the incident is a reportable security incident based upon the definitions in the Information Security Incident Response Policy. If the ISO is unsure, they can contact the State ISO at (916) 445-5239 and request direction and recommendation on how to proceed.

If it is determined it is not a security incident, the ISO will document the reported information and the reason that lead to the determination of it not being an incident. NOTE: If the incident is a virus on a desktop or laptop that was quarantined by the anti-virus software, it is not a reportable incident according to State ISO.

If the ISO determines that it is an incident, the ISO will follow the procedures outlined in SIMM 5340-A and SIMM 5340-C to contact the California Highway Patrol Emergency Notification and Tactical Alert Center (ENTAC) and provide the information needed.

The ISO will also email initial information on the incident to the CHHS ISO (infosecurity@chhs.ca.gov). This report to the CHHS ISO should contain the information requested in the CHHS Procedures for Privacy and Information Security Incident Reports.

If the security incident is with a project sponsored by another state entity, the OSI ISO will notify the Project Sponsor's ISO.

Triage

The Incident Response Manager will work with the impacted project operations manager, business unit, and/or the Information Technology Office to gather information and identify necessary actions to stop or mitigate the security incident.

Investigation

The Incident Response Manager will work with project operations manager, business unit, and/or the Information Technology Office to investigate and document the incident. The following information regarding the incident should be collected or updated from the initial report:

- Date incident occurred
- Date incident detected
- Type of personal, sensitive or confidential information lost, stolen, missing, or compromised (e.g., name, Social Security number, date of birth, medical/health information)
- Approximately how many individuals are affected by the incident
- If it is health related, what type of health information (e.g. condition, treatment, claims information, demographics and other personally identifiable information that relates to the provision of health care)
- If it is health related, approximately how many records were involved
- Incident location(s), and a general description of the incident including which project or business unit
- If the incident involved electronic equipment, devices, or media, what specific safeguards were in place (e.g., password protection, encryption)
- For computer related thefts collect information on the make and model, serial and state asset ID and location of theft. (If computing device was stolen from private car or residence then individual responsible must report theft also to their local police and provide a police report number).
- For computer related crimes (e.g. hackers, virus attacks, denial of service, SQL Injections) also document the make and model, IP address, assigned name of the affected computer(s), operating system, location of affected computers and any actions taken during and following discovery prior to contacting ENTAC.

If the investigation determines that the incident is more severe than initially determined, the ISO will email updated information on the incident to the CHHS ISO (infosecurity@chhs.ca.gov).

Business Continuity

The Incident Response Manager will determine if and when the OSI Technology Recovery Plan and/or Business Continuity Plan need to be activated in response to a security incident.

Coordination and Communication

If the incident is a major breach and/or has serious impact to the person(s) whose information was breached, the Incident Response Manager will schedule daily status meetings to keep all parties informed of the investigation and remediation. A conference call number should be made available so that all the needed parties can participate. The template in Appendix A below can be used to organize the information for the conference calls. The following table lists organizations that should be represented in these meetings and their roles:

Organization	Role
CTO	Incident Response Manager
ISO	Incident reporting and policy review/update
AIO, or designee	Advisory, oversight, and communications to Agency
Agency ISO, or designee	Advisory and oversight
State ISO	Government operations communication
As Applicable:	
Project Sponsor	Coordination and communication
Military Department	Security scanning and remediation recommendations
Vendors	Support as needed
Other Departments	Support as needed

The Incident Response Manager should weigh the need for the updates with the need for the team to continue working the incident. A suggestion is that someone on the team be designated to collect the pertinent updates that the Incident Response Manager can then provide during the status meetings.

The daily status meetings will continue at least until it is determined whether personal data was exfiltrated.

Corrective Action and Restoration

The Incident Response Manager will work with project operations manager, business unit, and/or the Information Technology Office to develop and take corrective actions (e.g. reconfigure firewall, take server(s) offline, remove or encrypt confidential information, restrict access, remove infected machine from network, provide awareness education, restore files and services, etc.). The corrective actions are to ensure that future security incidents of the same nature are mitigated.

Reporting

If the incident is for missing or stolen state property, the individual is responsible for making a Police Report and providing the Police Report Number to the ISO for the SIMM 5340-B Report.

The ISO will communicate with the Agency ISO and Project Sponsor's ISO (if applicable), the OSI Chief Deputy Director, the OSI Deputy Agency Information Officer, and the OSI Chief Technology Officer (CTO). This communication should contain a brief description of the incident, including numbers affected and type of data (if data breach), actions taken and next steps.

The ISO will continue to update the Agency ISO, the OSI Chief Deputy Director, the OSI CTO, and Project Sponsor's ISO (if applicable) when additional information is available or next steps are accomplished.

Once the investigation and mitigation is complete, the ISO will follow the procedures outlined in SIMM 5340-A to complete the Information Security Incident Report (SIMM 5340-B). If the incident was a breach of personal information, the procedures of SIMM 5340-C will be followed. A copy of the final report will also be sent to the Agency ISO, the OSI Chief Deputy Director, the OSI CTO, and Project Sponsor's ISO (if applicable)

9. Education and Awareness

OSI shall ensure that incident response is addressed in education and awareness programs. All staff members will be trained annually. Additional training will be provided as a result of lessons learned from incidents. The annual education and awareness programs shall address, at a minimum, the following topics:

- Reporting responsibilities
- Incident awareness
- Incident prevention

Members of the OSI Incident Response Team will receive team responsibility specific training within 30 days of appointment to the team. Refresher training will occur annually.

The following are the types of information, at a minimum, that should be included in the incident response training.

General Incident Response Awareness

- Incident Response Policy
- Detecting a problem
- Reporting the problem

Specific Incident Response Team Member Training

- Incident Response Policy
- Determining the cause
- Minimizing the damage
- Resolving the problem
- Lessons learned
- Escalation process
- Interaction with third-party entities
- Investigation phase objectives
- Investigation considerations
- Investigation process
- Containment
- Reporting and documentation
- Recovery and repair
- Communication

Forensics Training

- Evidence
    - Potential digital evidence
    - Standards of evidence
    - Identification of evidence
    - Collection of evidence
    - Reduce contamination

  - Protect the scene
  - Maintain chain of custody and authentication

- Collection of Digital Evidence
  - Volatile and fragile
  - Short lifespan
  - Collect quickly
  - By order of volatility
  - Document

- Chain of Custody
  - Who
  - What
  - When
  - Where
  - How

Appendix A Incident Response Briefing Template

Meeting called by: _____

Facilitator: _____

Date: _____

Time: _____

Attendees: _____

Assessment:

Action items	Current status	Responsible
1.		

Remediation:

2.		

Restoration:

3.		

Other Information

Observers: _____

Resources: _____

Special notes: _____

Appendix B OSI Security Incident Points of Contact List

This appendix is in a separate document.