OIT Operational Protocol Information Security Incident Management

Purpose:

This document describes the protocol to be followed by the LACCD Office of Information Technology (OIT) to create, monitor, manage and close information security incidents that are reported through OIT Operational Protocol Information Security Incident Response. This protocol is intended to complement the District's Breach Notification Requirements described in OIT Operational Protocol Computer and Network Use, by providing a uniform protocol to record and investigate security incidents that could result in a security breach.

Scope:

This protocol is to be used by members of the LACCD OIT to manage information security incidents, and addresses the following areas:

- Management of Information Security Incidents
  - Incident Definition
  - Incident Management Team, Roles and Responsibilities
  - Incident Management Protocol
  - Collection of Evidence
  - Learning from Information Security Incidents

This protocol is used in conjunction with OIT Operational Protocol Information Security Incident Response, to manage the full lifecycle of information security incidents.

Roles:

The following roles apply to this protocol:

1. Incident Reporter: An Incident Reporter can be any LACCD employee or contractor that suspects an information security incident has taken place. It may also be an outside party who believes an LACCD information technology resource initiated an incident.
2. Chief Information Security Officer: The Chief Information Security Officer (CISO) of LACCD is responsible for assuring appropriate security incident response protocols are implemented.
3. Information Security Analyst: The Information Security Analyst monitors the published reporting email address and phone number for reporting of incidents from LACCD employees or contractors.
4. Incident Handler: The Incident Handler is responsible for coordinating the gathering and dissemination of evidence and information regarding the incident. It is typically an Information Security Analyst located at the Educational Services Center (ESC).

5. ISIRT: The CISO may enlist an Information Security Incident Response Team (ISIRT) to coordinate the response to an information security incident. The membership of the ISIRT may vary depending upon the scope, scale and nature of the incident.

Protocol:

Monitoring the Incident Reporting Email and Phone Number

The Information Security Analyst will monitor the information security incident reporting phone number Monday through Friday from 8:00AM to 5:00PM.

The email address infosecincidents@laccd.edu will be monitored by the Chief Information Security Officer and all Information Security Analysts. The email address will also be monitored through the Pager Duty phone verification service, which will call designated monitors via phone to notify them that a new email has been sent to infosecincidents@laccd.edu.

When a phone call to (213) 891-2248 is made and/or an email is sent to infosecincidents@laccd.edu, the assigned Information Security Analyst will create a ticket in the District's ticket management system, and contact the Incident Reporter to begin investigation of the incident.

Create Incident Ticket and Assign Priority

The Incident Handler will create the incident ticket, assign a classification/priority to the ticket, and record known details about the incident as follows.

- Log on to the Security Operations Project within the System
- Select "New Case" under the "Cases" menu
- Select "Case Type" of "Incident" from the dropdown menu and complete the relevant case details
- Select the "Incident" tab and complete the relevant details, including assigning an incident classification/priority
- Click the "Submit" button to create the incident

High Priority Incident Management Protocol

Confirm Priority

If the incident handler has a reasonable belief that the security incident may be Priority 1 or Priority 2, the incident handler is to contact the CISO immediately to confirm known details of the incident and finalize the priority. If the CISO is not immediately available, the Incident Handler is to contact the following people (in order) to confirm the priority:

- Chief Information Officer
- Deputy Chief Information Officer
- Systems and Programming Manager

The CISO will confirm the priority of the incident, and the Incident Handler will update the priority of the ticket. If the incident is Priority 1 ticket, the "High Priority Incident Management Protocol" will be followed. If the incident is Priority 3 or Priority 4, the "Low Priority Incident Management" protocol will be followed. If the incident is Priority 2, the CISO will determine which protocol are followed.

Assemble ISIRT

Based upon the nature of the incident, the CISO will assemble an Information Security Incident Response Team (ISIRT), and notify the team of the incident with the Incident Handler in copy. For priority 1 incidents, the CISO and/or Incident Handler will assemble a conference call as soon as possible with the ISIRT to review the nature of the incident and coordinate a response. The Incident Handler will enter the names and roles of the ISIRT in the ticket. ISIRT members will be reminded of the confidentiality of the incident, and that information must not be shared outside of the ISIRT unless and until warranted.

Breach Notification

If a breach of legally protected information is confirmed, the CISO or Incident Handler will notify required parties of the incident in accordance with OIT Operational Protocol Computer and Network Use. The CISO or Incident Handler will document the notification in the ticket, including the date and approximate time of each notification. All written notifications must have the LACCD Office of General Counsel in copy.

In the event that the ISIRT determines a breach of sensitive information has occurred, the ISIRT will determine appropriate external parties and timelines required for breach notification, and notify the appropriate District executive team to make the required arrangements. Examples of breach notification requirements may include, but not be limited to:

- The State of California (in Compliance with California 1798.28)
- The Los Angles Division of Public Social Services (in compliance with the CalWorks contract)
- The LACCD acquiring bank (in compliance with PCI-DSS)
- The California Chancellor's Office, and state or Federal departments of education (in compliance with FERPA)

Incident Containment and Remediation

The CISO will coordinate with the ISIRT and external resources, as applicable, to determine and implement the best path forward to:

- Stop the effects of the incident from spreading
- Preserve evidence
- Remediate information systems associated with the incident to prevent it from happening again
- Identify the scope and scale of confidential information, as applicable, that may have been affected through the incident
- Make reasonable efforts to retrieve copies of and/or gain assurances that all confidential information is accounted for
- Identify any confidential information that may not be accounted for, and identify associated reporting requirements

The Incident Handler will document ISIRT steps to contain and remediate the incident in the ticket, until the CISO and ISIRT have determined the incident is resolved.

Incident Reporting

The Incident Handler will coordinate drafting of the incident report, with input from the ISIRT. Once a draft report is completed, the Incident Handler may choose to confer or consult with the General Counsel to determine whether the report has any confidentiality implications. The final incident report will be reviewed with the ISIRT, and include:

- A log of all actions taken by the ISIRT
- A communications plan for the timing, preparation, acceptance and delivery of internal communications (to applicable District personnel), and external communications (e.g. affected individuals, state reporting authorities, the media, etc.)
- Regulatory reporting and/or notification requirements, including deadlines

The Incident Handler will upload all documentation into the incident ticket.

Closing the Incident

High Priority incidents will be closed by consensus of the ISIRT. The Incident Handler will store all documentation and evidence by attaching it to the incident ticket, and document a log of all actions taken by the ISIRT in the Incident Ticket. The CISO will review the documentation and close the incident in the ticket system.

Low Priority Incident Management Protocol

Confirm Priority

The incident handler will determine the incident priority by using the general incident classification matrix in the IT Operational Protocol SEC-OPS-INCIDENT-001: Security Incident Response Protocol as a guide. If the incident handler has a reasonable belief that the security incident may be Priority 3 or Priority 4, then the incident handler will work with the CISO to confirm the priority. Once confirmed as a low priority incident, the following general approach will be taken.

Incident Containment and Remediation

Depending on the nature of the incident, the incident handler will coordinate with the appropriate resources (an ISIRT Team may be assembled if needed) to determine and implement the best path forward to:

- Stop the effects of the incident from spreading
- Preserve evidence
- Remediate information systems associated with the incident to prevent it from happening again

This may be done using various technical methods (e.g. disconnecting a device from the network, removing malware, changing passwords, etc.). The specific actions will vary based on the type of incident,

but some common scenarios include resetting passwords for compromised accounts and removing malware from an infected device by using anti-malware software.

Incident Reporting

The incident handler will update the incident ticket with the actions taken to deal with the incident, along with any recommendations to prevent recurrence.

Closing the Incident

Low priority incidents will be closed by OIT upon completion. This will typically be done by the incident handler after ensuring that the incident ticket has been updated with all the relevant information pertaining to the incident.

Related Documents:

- LACCD Administrative Procedure 3720 Computer and Network Use
- LACCD OIT Operational Protocol Computer and Network Use
- LACCD OIT Operational Protocol Information Security Incident Response

Version Control				
#	**Date**	**Editor**	**Approved**	**Changes**
0.8	10/18/2019	P. Luce		Initial Document
0.9	10/22/2019	G. McCalmon		Added content to "Low Priority Incident Management procedure" section
1.0	10/28/2019	P. Luce		Published Procedure
1.1	10/2/2020	G. McCalmon		Updated Procedure/Protocol Terminology
1.2	10/23/2020	P. Luce		Updated notification protocol
1.3	5/21/2021	P. Luce		Updated document references to AP 3720
1.4	6/3/2021	P. Luce		Format Edits
1.5	10/29/2021	P. Luce	C. Lidz	Updated Version Control to have approval section