OIT Operational Protocol Information Security Incident Response

Purpose:

This document describes the protocol to be followed to report, investigate, and remediate information security incidents related to information technology resources. The protocol in this document provide a framework for identifying, investigating, responding, and documenting potential incidents and corresponding remediation plans. 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.

In the event of an information security incident, it is imperative that the incident be reported to the appropriate operational manager and the LACCD Office of Information Technology (OIT) as soon as possible. A consistent approach to security incident response can minimize the extent and severity of security exposures.

Scope:

This protocol is to be used by members of the LACCD community when reporting a potential incident, including incidents reported by outside sources as applicable. The responsibility to establish, document, and distribute information security incident response and escalation protocols to ensure timely and effective handling of all situations is assigned to the Chief Information Security Officer. Should the Chief Information Security Officer position become vacant, this responsibility will be assigned to a knowledgeable member of IT management by the Chief Information Officer.

In the event of a specific incident affecting information systems, the District must have pre-planned methods to respond to various threats, including incidents related to data confidentiality, integrity, and application availability. In addition, reporting mechanisms must be in place to ensure that proper personnel are informed of all incidents. Responsibility for incident handling operations must be assigned to an Incident Management Team, whose trained members will execute the incident response plan.

This protocol is to be used by all LACCD employees to report information security incidents, and addresses the following areas:

- Reporting of Information Security Incidents
- Incident Response and Prioritization
- Incident Management, Reporting and Closure

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

Definition of Information Security Incident:

An Information Security Incident is the act of violating an explicit or implied security policy or practice to protect the confidentiality, integrity and availability of District information systems. Information Security Incidents include but are not limited to:

- attempts (either failed or successful) to gain unauthorized access to a system or its data
- unauthorized disruption or denial of service
- the unauthorized use of a system for the transmission, processing or storage of data changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

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. 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).
4. ISIRT: The 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. The CISO will designate a single Point of Contact (POC) for high priority incidents.
5. For high priority incidents, the ISIRT will identify key business unit leaders or analysts to assist the ISIRT. If a threat, or potential threat, has been identified to specific systems, data or processes, a business analyst must be consulted to assist in quantifying the risk in business terms.

Protocol:

Identifying a Security Incident

A Security Incident is any potential violation of LACCD policies, protocols and practices that may result in:

- Misuse or release of confidential information (such as social security number, health record, student record or financial records) of one or more individuals
- Unauthorized access, abuse, destruction or theft of LACCD's information and/or computer resources
- Use of District information technology resources to harass or threaten someone
- Use of District information technology resources to gain unauthorized access to non-LACCD resources

Reporting a Security Incident

If any LACCD employee or contractor suspects and/or receives a report from any party that believes an information security incident may have occurred, and that incident has occurred on or from a District information system (such as SIS, SAP, etc.), computer, laptop, cell phone or other device, **as soon as possible**:

- Report the incident by contacting the LACCD OIT Information Security team via both email AND phone:

infosecincidents@laccd.edu

(213) 891-2248

- In the report. Provide the contact name, position, phone number and email address. Also provide a brief description of the suspected incident, including the personnel and systems that are potentially affected
- If you have been notified by a third party of a potential security incident, refer the notification to OIT by calling or emailing using the contact information above.

The control of information during investigation of an information security incident is critical. If people are given incorrect information, or unauthorized persons are given access to information, no matter how well-intentioned, there can be undesirable side effects. Do not discuss the information security incident with any person outside of LACCD without first consulting with the OIT Information Security team. If there is evidence of criminal activity, the Information Security team will coordinate with LACCD executive management to notify law enforcement and request their assistance in the matter.

Identifying an Incident

Upon receipt of a notification of a potential incident, the OIT Information Security team will:

- Record the notification, and designate an Incident Handler to lead the response.
- Coordinate with the individual(s) reporting the incident to identify the system(s) affected, type of information and scale of the potential incident.
- Assist the reporting individual in isolating compromised system(s), as applicable
- Notify the Chief Information Security Officer (CISO) or designee, who will triage the potential severity of the incident, and determine next steps. The following general classification of incidents will be used:

Severity	Description (Examples)	Action required
CRITICAL (P1)	• Successful hacking or denial of service attack of an LACCD information system • Confirmed breach of personally identifiable information (PII) • Significant operations impact • Significant risk of negative financial or public relations impact	• Activate ISIRT Team • Notify District officials as described in OIT Operational Protocol Computer and Network Use • Notify the Board of Trustees
HIGH (P2)	• Hacking or denial of service attack attempted with limited impact on operations • Widespread instances of a new computer virus not handled by anti-virus software • Possible breach of student information or PII • Some risk of negative financial or public relations impact	• Assign Incident Handler, who will coordinate the response • Assemble an ISIRT Team as required
MEDIUM (P3)	• Hacking or denial of service attacks attempted with no impact on operations • Widespread computer viruses easily handled by anti-virus software • Lost laptop / smart phone, but no data compromised	• Assign Incident Handler, who will coordinate the response • Assemble an ISIRT Team as required
LOW (P4)	• Account compromise, single user, no breach of student information or PII • Unauthorized access attempts • Malware or virus on single computer easily handled by anti-virus software • Account sharing • Account lockouts	• Assign Incident Handler, who will coordinate the response

Declaring an Incident

The CISO or designee will, as warranted, assign a priority to the incident based upon the criteria above, and assign an Incident Handler. As appropriate the CISO will assemble an Information Security Incident Response Team (ISIRT) to determine the appropriate investigation, remediation and response to the incident. The ISIRT members may include, as required:

- The Chief Information Officer
- General Counsel
- Public Information Officer(s)
- Deputy/Vice Chancellor(s)
- District/College Administrative Leaders
- District/College IT Management
- District Risk Management
- Network/System/Security Technical Resources
- Internal Audit
- External Incident Response Resources
- Law Enforcement

In order to maintain confidentiality about the incident, all communications will be coordinated through the OIT Information Security team, in consultation with General Counsel as required. The Incident Handler will maintain a log that documents the degree and reason to which parties are informed of the incident. 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.

Containing and Remediating the Incident

Upon declaration of an incident, the incident must be contained to prevent further harm. The CISO will coordinate with the ISIRT and external resources, as applicable, to determine 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
- Preserve evidence as required/feasible to assist with legal or law enforcement protocols as directed by the Office of General Counsel

Reporting the Incident

The Incident Handler will coordinate drafting of the incident report, with input from the ISIRT. As required, distribution and review of working drafts must be conducted under privilege where directed by the

General Counsel, who must be included on any distribution of the report. 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.)
    - The Office of General Counsel must be contacted in the event of an information security event to determine whether or not legal requirements dictate the necessity of reporting the security incident publicly or to an external party.
- Documentation of security policy violations for review and action by appropriate District personnel
- "Lessons Learned", as applicable. The OIT Information Security team will coordinate learning sessions for applicable areas within LACCD.

Closing the Incident

Priority 1 and Priority 2 (as applicable) incidents will be closed by consensus of the ISIRT. The Incident Handler will store all documentation and evidence in a secure location approved by General Counsel. A log of all actions taken by the ISIRT will be documented. The CISO and/or Incident Handler, as appropriate, may close lower priority incidents upon completion. Priority 3 and Priority 4 incidents will be closed by the Incident Handler.

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 Management

Version Control				
#	**Date**	**Editor**	**Approved**	**Changes**
0.5	8/20/2019	P. Luce		Initial Document
0.6	8/26/2019	P. Luce		Added language referencing LACCD policies as appropriate
0.7	10/28/2019	P. Luce		Published Version
0.8	11/18/2019	P. Luce		Minor edits to priority matrix
0.9	11/21/2019	C. Lidz		Added multiple sections
0.91	11/25/2019	P. Luce		Consolidation of input
1.0	12/4/2019	C. Lidz		Approved Final Version
1.1	10/2/2020	G. McCalmon		Updated Procedure/Protocol Terminology
1.2	10/2/2020	P. Luce		Update to Communication Protocols
1.3	5/21/2021	P. Luce		Updated document references to AP 3720
1.4	6/3/2021	P. Luce		Format updates
1.5	10/29/2021	P. Luce	C. Lidz	Version control updated to include approval section