Cybersecurity Incident Response Policy and Plan

Lake Bluff School District 65

Revision:	2024.10.B
Plan Owner:	Kevin Kolcz, Director of Technology
Plan Approver:	Lisa Leali, Superintendent of Schools

Revisions and Reviews

Date	Rev No.	Individual	Summary of Changes
09/11/24	A	Kevin Kolcz	Initial Creation
10/9/24	B	Kevin Kolcz	Finalizing Draft for Implementation

Table of Contents

Mission

To establish a comprehensive and coordinated approach to cybersecurity incident response, leveraging partnerships with stakeholders and leveraging technology and best practices to ensure the confidentiality, integrity, and availability of information, while maintaining the highest standards of transparency and accountability.

Strategy and Goals

This plan is designed to serve as a guiding document for a wide variety of cybersecurity related incidents and does not serve as a step-by-step response plan for specific issues.

Strategy

1) Stop the Spread
2) Mitigate Damage
3) Restore Functionality
4) Reduce Chances of Reoccurrence
5) Improve Response

Goals

1) Protect Student and Staff Data
2) Maintain the Continuity of Education
3) Meet Legal and Regulatory Requirements
4) Maintain Public Trust

Superintendent Statement and Approval

A comprehensive and effective cybersecurity incident response plan is critical to meet our goals:

1) **Protect Student and Staff Data:** The district holds a vast amount of sensitive and confidential information, including student and staff data, which must always be protected. Having a well-planned and executed response plan is critical in preventing data breaches and ensuring that confidential information is not compromised.
2) **Maintain the Continuity of Education:** In the event of a cybersecurity incident, it's important that the district be able to respond quickly and effectively to minimize the disruption to educational activities. A comprehensive response plan will help ensure that the district can continue to provide high-quality education to students, even in the face of an incident.
3) **Meet Legal and Regulatory Requirements:** The district is subject to various laws and regulations regarding data protection, including student data privacy laws such as the Family Educational Rights and Privacy Act (FERPA). A robust response plan will help ensure that the district is in compliance with these requirements and is prepared to respond to any incidents that may arise.
4) **Maintain Public Trust:** The district is responsible for maintaining the trust and confidence of students, parents, staff, and the community. By demonstrating a commitment to cybersecurity and being prepared to respond to incidents, the district can build and maintain public trust and confidence in its ability to protect sensitive information.

A comprehensive cybersecurity incident response plan is a critical component of the district's overall security posture and is essential for protecting sensitive information, ensuring the continuity of education, meeting legal and regulatory requirements, and building public trust.

[Signature]
Lisa Leali, Superintendent of Schools

Purpose and Objectives

The purpose of this cybersecurity incident response plan is to establish a comprehensive and coordinated approach to identifying, responding to, and mitigating the effects of potential cybersecurity incidents affecting the district, while ensuring the confidentiality, integrity, and availability of information.

Objectives

1) To prevent and mitigate the impact of cybersecurity incidents through proactive risk management, incident response, and business continuity planning.
2) To ensure timely detection and notification of potential incidents, leveraging a combination of technology and human resources to identify and respond to incidents in a coordinated manner.
3) To minimize the impact of incidents on students, staff, and operations by establishing clear roles, responsibilities, and procedures for responding to incidents, including crisis communication and media management.
4) To continuously improve the district's cybersecurity posture through regular review and testing of the incident response plan, incorporating feedback from stakeholders, and incorporating best practices and emerging technologies.

Scope

This cybersecurity incident response plan covers all incidents involving data and information entrusted to or created by the school district, all district owned information processing equipment, and any device connected to the district computer networks.

Definitions

Cybersecurity Incidents

A Cybersecurity Incident is an event or series of events that pose a threat to the confidentiality, integrity, and availability of data and information, the information processing equipment, and the learning environment of the school district.

This threat may come from external sources such as cyberattacks, or from internal sources such as accidental or intentional data breaches by employees, contractors, or students.

Declaration of Incident

The declaration of an incident is a serious matter as it initiates response plans, incurs costs, transfers authorities, involves external partners, and can disrupt normal activities.

As such, only the superintendent and the director of technology can declare an incident.

Conclusion of Incident

An incident closes in three phases. As the incident is concluded, the incident commander and district leadership must communicate and understand which authorities, responsibilities, and expectations change given the specifics of the incident.

First, all efforts that must be done immediately are complete. Most of the team can reassume daily tasks.

Second, all systems have been restored to normal operations. Any identified vulnerabilities have been remedied or an approved plan is in place to remedy those vulnerabilities.

Finally, the entire incident is documented and any lessons learned are incorporated into policies, plans, and procedures.

Related Terms

Availability: In the context of cybersecurity, availability refers to the accessibility and usability of information and systems. This means that authorized users should be able to access and use the information and systems they need, when they need them, and in a manner that is reliable and consistent.

Compromise: Compromise refers to a situation in which the security of information, systems, or networks has been breached. This can occur through a variety of means, such as a cyberattack, a data breach, or other security incident. When information, systems, or networks are compromised, there is a risk that sensitive data or intellectual property could be lost, stolen, or misused.

Confidentiality: Confidentiality refers to the protection of information from unauthorized access, use, or disclosure. This means that only authorized individuals should be able to access and use sensitive data, and that information should be protected against unauthorized access or exposure.

Credentials: Credentials are a set of information used to verify the identity of a user or device. This can include usernames and passwords, security certificates, or other forms of authentication.

Cyberattacks: A cyberattack is an intentional and unauthorized attempt to access, modify, or destroy information or systems. This can include a variety of threats, such as malware, phishing, ransomware, and other types of malicious activity.

Damage: Damage refers to any harm or destruction caused to information, systems, or networks. This can include physical damage to equipment, as well as logical damage to data or systems.

Data Breach: A data breach is an incident in which sensitive data is intentionally or unintentionally disclosed to unauthorized individuals. This can occur through a variety of means, such as a cyberattack, a lost or stolen device, or an employee mistake.

Denial of Service (DoS): A Denial of Service (DoS) attack is an attempt to make a system or network unavailable to its intended users. This can be accomplished through a variety of means, such as flooding the network with traffic or exploiting vulnerabilities in systems.

Distributed Denial of Service (DDoS): A Distributed Denial of Service (DDoS) attack is a type of DoS attack that originates from multiple sources, rather than from a lone source. This makes it more difficult to detect and mitigate and can cause widespread damage to information and systems.

Endpoints: Endpoints are devices or systems that access a network, such as computers, smartphones, or other types of internet-connected devices. These devices can be a source of security vulnerabilities and must be protected and managed appropriately to prevent cyberattacks and other security incidents.

Information Processing Equipment: Information processing equipment refers to the hardware and software used to process, store, and transmit information. This can include computers, servers, routers, switches, and other types of equipment.

Integrity: Integrity refers to the accuracy and consistency of information. This means that information should not be altered or tampered with, and that it should remain consistent and accurate throughout its lifecycle.

Internet of Things Devices: Internet of Things (IoT) devices are a type of endpoint that are connected to the internet. These devices can include smart home appliances, security systems, and other types of connected devices.

Internet Protocol (IP) Connected Devices: Internet Protocol (IP) connected devices are devices that are connected to a network and use the Internet Protocol (IP) to communicate. This can include computers, servers, smartphones, public address systems, door locks, camera systems, and other types of internet-connected devices.

Phishing: Phishing is a type of cyberattack that uses social engineering techniques to trick individuals into revealing sensitive information, such as passwords or financial information. This can occur through emails, text messages, or other forms of communication.

Ransomware: Ransomware is a type of malware that encrypts a victim's files and demands a ransom payment in exchange for the decryption key. This can cause significant damage to information and systems, and can disrupt business operations.

Sensitive Data: Sensitive data is information that is confidential and must be protected. This can include personal information, financial information, intellectual property, and other types of information that can have significant value to an organization or individual.

Servers: Servers are computers or systems that are designed to provide resources or services to other systems or devices. This can include web servers, email servers, database servers, and other types of servers.

Incident Severity Levels

All incidents are categorized into one of four severity levels. The overall severity level is determined based on an evaluation of the functional impact, information impact and the recoverability of the incident.

The below table provides definitions and examples of each. The examples provided are not an all-inclusive list.

Severity	Definition	Examples
Catastrophic	Widespread and severe harm to the district's IT systems and networks, rendering them inoperable and resulting in a complete loss of sensitive data. This type of incident could have a devastating impact on the district's operations and could take an extended period of time to recover from.	- Ransomware Attack that encrypts all data - Continuing exfiltration of sensitive data

Critical	Poses a significant threat to the district's IT systems and data, requiring immediate and coordinated action to contain and mitigate the impact. This type of incident could result in the loss or unauthorized access to sensitive data, significant disruption to operations, and damage to the district's reputation.	- Successful phishing attack that provides access to the network - Outage that prevents normal activities
Major	Significant disruption to the district's IT systems and operations, requiring a coordinated response to restore normal operations. This type of incident could result in the temporary loss of access to certain systems or data and could impact the district's ability to carry out its mission.	- Compromise of Credentials - Denial of Service attack - Major system outage preventing normal business operations
Minor	Limited impact on the district's IT systems and operations and can be resolved quickly with minimal disruption.	- Failure of network device - Loss of staff/student device

Organization, Roles, Responsibilities, and Authorities[1]

Lake Bluff School District 65 will use a centralized response team for all incidents, mirroring the Incident Command System, largely using employees.

Key Roles and Responsibilities

Incident Specific Roles

Incident Commander: Responsible for overseeing the incident, making reports to district leadership, working with external partners, delegating responsibility as appropriate.

Public Affairs Officer: Responsible for interacting with media, parents, teacher’s union, and other external parties not directly involved with the response.

Incident Response Team Leader: Responsible for conducting the direct response to the incident, to include containment, mitigation, recovery, and restoral.

Incident Response Team Members: Duties as assigned to assist the incident response team lead.

Additional roles and responsibilities may be created and assigned as necessary.

Other Active Stakeholders

Superintendent: Maintain education continuity to maximum extent possible. Provide updates to School Board, as appropriate.

CSBO: Validate, approve, and expedite necessary purchases and expenditures.

General Counsel: Provide legal advice.

[1] Computer Security Incident Handling Guide, 2.4, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Incident Commander Authorities

The below authorities are provided to the Incident Commander during a declared incident.

- May authorize the expenditure of up to the below listed amounts for Time and Materials to an Information Technology Managed Service Provider already contracted with the district
  - **Catastrophic Incident: 40 billable hours outside of business hours 7:00-4:00, up to $35,000 in materials and hardware.**
  - **Critical Incident: 20 billable hours outside of business hours 7:00-4:00, up to $15,000 in materials and hardware**
  - **Major Incident: 10 billable hours outside of business hours 7:00-4:00, up to $10,000 in materials and hardware**
  - **Minor Incident: 5 billable hours outside of business hours 7:00-4:00, up to $5,000 in materials and hardware**
- Disable any information system or IP connected system as necessary, with notification to the superintendent for any changes to life-safety systems (e.g., Fire Alarms, Public Address Systems)
- Reassign staff members as needed to incident response duties

Standard Assignments

Role	Primary	Backup
Incident Commander	Director of Technology	Data & Technology Specialist
Public Affairs Officer	Superintendent	CSBO
Incident Response Team Leader	Net56 Technology Services	Director of Technology

The Director of Technology, in Consultation with the Superintendent, may modify these assignments as needed in response to specific incidents.

An individual may take on multiple roles. *The Incident Commander maintains all roles until delegated to someone else.*

Communications

Communications should take place outside the bounds of the affected system. For example, if the email systems are suspected to be compromised, email should not be used to handle the incident. Indirect modes of communication, in priority order: District Email, District Phone, Personal Cell Phone.

Internal Communications

Communications within the response team and between the response team and leadership are crucial to resolving an incident. However, excessive communications demands can delay or disrupt incident response actions. Therefore, the below reporting requirements serve to sufficiently inform leadership without disrupting incident response.

Severity Level	Initial Notification	Updates
Catastrophic	Upon Declaration, Face to Face	2 hours
Critical	Upon Declaration, Face to Face	4 hours
Major	Upon Declaration, Via Phone	24 hours
Minor	Upon Conclusion, Via Email	N/A

External Communications[2]

Communications outside of the incident response team is often just as important as internal communications. In each incident, decisions must be made regarding nature, level, timing, frequency, and mode of communication, as well as who will be responsible for communication.

Entities to Consider

- Insurance Provider
- Internet Service Provider(s)
- Law Enforcement
- Managed Services Provider
- Media
- Parents
- School Board
- Software Vendors
- Staff
- Students
- Teacher Union
- X-as-a-Service Providers

Contact information for relevant parties is listed in Appendix A: External Contact Information.

Training and Exercises

The Director of Technology will conduct a gap analysis to identify any required or recommended training or certifications for incident responders.

Regular exercises maintain a sense of proficiency and validate the effectiveness and accuracy of incident response plans.

Tabletop Exercise

Tabletop Exercises are an inexpensive way to test and validate incident response capabilities. During the exercise, a scenario is described, and participants talk through what they would do, who they would notify, etc. Exercises can be conducted at the lowest levels, with just the incident response team. Alternatively, all stakeholders can be involved.

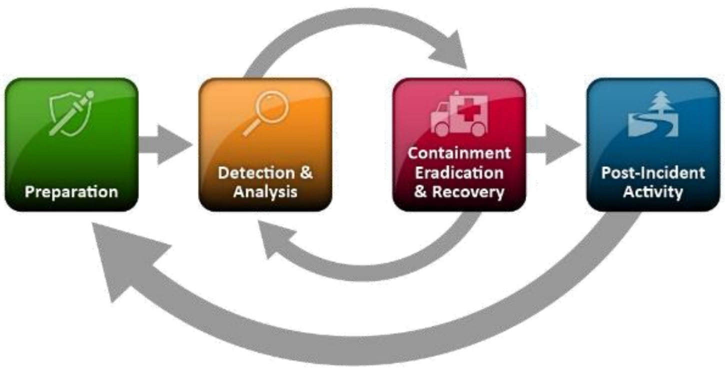
The Director of Technology will lead the incident response team in tabletop exercises of various incidents at least quarterly. Annually, the director of technology will conduct a full tabletop exercise for a Critical or Catastrophic incident coincident with the annual review of this plan. Refer to NIST SP 800-84[3] for more information.

Incident Response Life Cycle

The Incident Response Life Cycle, as described in the NIST Computer Security Incident Handling Guide (NIST SP 800-61 Rev 2), consists of four main stages:

[2] Computer Security Incident Handling Guide, 2.3.4

[3] Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, http://csrc.nist.gov/publications/PubsSPs.html#800-84



Preparation[4]

Establish Incident Response Capability

The Technology Director will update, maintain, and implement this plan, to include annual review. Key items to prepare, as listed in the Computer Security Incident Handling Guide:

Incident Handler Communications and Facilities:

- **Contact information** for team members and others within and outside the organization (primary and backup contacts), such as law enforcement and other incident response teams; information may include phone numbers, email addresses, public encryption keys (in accordance with the encryption software described below), and instructions for verifying the contact's identity.
- **On-call information** for other teams within the organization, including escalation information
- **Incident reporting mechanisms**, such as phone numbers, email addresses, online forms, and secure instant messaging systems that users can use to report suspected incidents; at least one mechanism should permit people to report incidents anonymously
- **Issue tracking system** for tracking incident information, status, etc.
- **Smartphones** to be carried by team members for off-hour support and onsite communications
- **Encryption software** to be used for communications among team members, within the organization and with external parties
- **War room** for central communication and coordination; if a permanent war room is not necessary or practical, the team should create a procedure for procuring a temporary war room when needed
- **Secure storage facility** for securing evidence and other sensitive materials

Incident Analysis Hardware and Software:

- **Digital forensic workstations[5] and/or backup devices** to create disk images, preserve log files, and save other relevant incident data.
- **Laptops** for activities such as analyzing data, sniffing packets, and writing reports
- **Spare workstations, servers, and networking equipment, or the virtualized equivalent**s, which may be used for many purposes, such as restoring backups and trying out malware

[4] CSIHG, 3.1

[5] A digital forensic workstation is specially designed to assist incident handlers in acquiring and analyzing data. These workstations typically contain a set of removable hard drives that can be used for evidence storage.

- **Blank removable media**
- **Portable printer** to print copies of log files and other evidence from non-networked systems
- **Packet sniffers and protocol analyzers** to capture and analyze network traffic
- **Digital forensic software** to analyze disk images.
- **Removable media** with trusted versions of programs to be used to gather evidence from systems.
- **Evidence gathering accessories**, including hard-bound notebooks, digital cameras, audio recorders, chain of custody forms, evidence storage bags and tags, and evidence tape, to preserve evidence for possible legal actions

Incident Analysis Resources:

- **Port lists**, including commonly used ports and Trojan horse ports
- **Documentation** for OSs, applications, protocols, and intrusion detection and antivirus products
- **Network diagrams and lists of critical assets**, such as database servers
- **Current baselines** of expected network, system, and application activity
- **Cryptographic hashes** of critical files[6] to speed incident analysis, verification, and eradication

Incident Mitigation Software:

- **Access to images** of clean OS and application installations for restoration and recovery purposes

Secure Systems, Networks, and Applications

As a normal part of duties, the technology department will secure the networks and devices in accordance with reasonable best practices. Key practices include Risk Assessments, Host Security, Network Security, Malware Prevention, and User Awareness/Training.

Detection & Analysis[7]

As a normal part of duties, the technology department will enumerate various threat vectors and implement controls to detect a use of those vectors. [Tools include: Incident Detection/Prevention Systems, Security Information and Event Management (SIEM), Antivirus and Antispam Software, File Integrity Checking, Third Party Monitoring.]

In order to assist in detection and analysis, the district will maintain logs from operating systems, services, applications, from endpoints and network devices [using a centralized log aggregation tool].

The technology department will maintain currency on new vulnerabilities and exploits through relevant information feeds.

Key items to consider, per the Computer Security Incident Handling Guide:[8]

- Profile Networks and Systems
- Understand Normal Behaviors
- Create a Log Retention Policy

[6] The National Software Reference Library (NSRL) Project maintains records of hashes of various files, including operating system, application, and graphic image files. The hashes can be downloaded from http://www.nsrl.nist.gov/.

[7] CSIHG, 3.2

[8] CSIHG, 3.2.4

- Perform Event Correlation
- Keep All Host Clocks Synchronized
- Maintain and Use a Knowledge Base of Information
- Run Packet Sniffers to Collect Additional Data
- Filter the Data
- Seek Assistance from Others

Incident Documentation

Log and maintain records documenting incident response actions, findings, and other pertinent information. These records may be used as evidence in criminal or civil litigation, so all records must be accurate and maintained appropriately.

Incident Prioritization

During this stage, the Director of Technology will make an initial judgment as to the severity of the incident, using the severity levels prescribed above. When deciding, the following items will be considered:

Functional Impact: How are the day-to-day operations of the school impacted? Are classes able to continue regularly, continue with some impact, or need to be cancelled?

Information Impact: Was information exfiltrated, changed, or deleted? Was information affected PII, HIPAA-related, or other category of protected data?

Recoverability: Are extra resources (i.e., money, equipment, personnel, overtime) required to recover? Is outside help required? Is this even recoverable?

During analysis of a declared incident, the Incident Commander may change the declared severity level as more information is available.

Incident Notification

This is the stage in which internal and external notifications are made, as previously described.

Containment, Eradication, & Recovery[9]

Containment Strategy

The precise method of containment varies based on the incident. Containment includes a range of activities between resetting a password to removing entire systems from the network. The Director of Technology will identify incident types and develop incident response playbooks for each. Key criteria during development:

- Damage/Theft/Loss of resources
- Evidence Preservation
- Service Availability
- Time/Resources to Implement
- Effectiveness
- Duration

[9] CSIHG, 3.3

Evidence Collection and Handling

Evidence is required to resolve an incident but may also be required for legal proceedings. Evidence should be collected, logged, and maintained in accordance with forensic standards. Chain of custody logs must be maintained.[10]

Eradication

Eradication, while not necessary for every type of incident, includes the removal of malware, disablement of compromised or illegitimate accounts, and the closure of any backdoors. It is important to identify all affected hosts and conduct appropriate actions on each.

Recovery

Recovery is the restoration of systems back to normal operations to include the additional steps to prevent reoccurrence of the incident. This may include restoration from backups, patching, changing settings to a more secure configuration, or implementing new policies/processes.

Post-Incident Activity[11]

After an incident, it is important to identify lessons learned and improve processes.

After *major, critical, and catastrophic incidents*, the Director of Technology will host a debrief with all those involved in the incident. During this debrief, the following questions will be answered, documented, and logged. The Director of Technology will work with the Superintendent to implement changes as appropriate.

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

As minor incidents do not warrant an organizational response, lessons learned will be documented within the minor incident report form.

[10] See NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response, for additional information on preserving evidence.

[11] CSIHG, 3.4

Appendix A: External Contact Information

Law Enforcement

Organization	*Notes*	*Contact Info*
Federal Bureau of Investigation		(800) CALL-FBI
Illinois State Police Division of Criminal Investigation		(217) 782-1320, Option 1

Insurance Provider

Organization	*Notes*	*Contact Info*
CLIC	Immediately call or email Cowbell. Prepare for a scoping call with a brief summary of what data or systems may be impacted.	claims@cowbellcyber.ai 833-706-0236

Internet Service Provider(s)

Organization	*Notes*	*Contact Info*
Illinois Century Network (ICN)		866-277-5669 312-814-3648

Vendors / X-as-a-Service Providers

Organization	*Notes*	*Contact Info*
Powerschool SIS	Powerschool	866-434-6276
Finance & Employee Information	Skyward	800-236-0001
Thrillshare	Website & Communication	501-613-0370
Cisco	Network Equipment Support	800-553-2447

Approved Managed Service Provider(s)

Organization	*Notes*	*Contact Info*
Net56 Technology Services		(224) 836-0860

Media

Organization	*Notes*	*Contact Info*
Allerton Hill Communications	Gia Harrison	614-329-8321

Internal Stakeholders

Organization	*Notes*	*Contact Info*
School Board	Anne Hill – President	303-947-4517
Teacher's Union	Michelle Grady	847-922-0790

Appendix B: Standardized Reports/Forms

Incident Handling Checklist[12]

	Action	Completed (Initial and Date/Time)
	Detection and Analysis	
1	Determine whether an incident has occurred	
1.1	Begin Documentation	
1.2	Analyze the precursors and indicators	
1.3	Look for correlating information	
1.4	Perform research	
2	Declare an Incident	
2.1	Determine the Severity of the incident based on: Functional Impact: Information Impact: Recoverability:	
2.2	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
4	Acquire, preserve, secure, and document evidence	
5	Contain the incident	
6	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered, repeat steps 1.2-1.4. Update 2.1 as required.	
7	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	Implement additional monitoring, as necessary, to look for future related activity.	
	Post-Incident Activity	
8	Create a follow-up report	
9	Hold a lessons-learned meeting (optional for minor incidents)	

[12] Adapted from CSIHG, Table 3-5. Additional checklists are available at

Notification of Minor Incident

Minor Cybersecurity Incident Report

Person Completing Report		**Date**
Employee(s)/Student(s) Involved	**Device(s) Involved**	
Type of Incident (Circle one or more)		
Lost Device	Password Compromise	Successful Phishing
	Other:________________________________	
Description of Event with Timeline		
Actions to Remedy		
Actions to Prevent in the Future (Note if actions are systemic in nature)		
Incident Cost		
Hours of Labor	Equipment	Other
Other Notes/Comments		
Signatures (with dates)		
Report Completed By	Director of Technology	Superintendent