Lake Preston Cybersecurity Incident Response Plan

This Cyber Security Incident Response Plan outlines the procedures that the Lake Preston School District uses to detect and respond to unauthorized access or disclosure of private information from systems utilized, housed, maintained, or serviced by the school district. This document defines an Incident Response Team's roles and responsibilities, including identifying, isolating, and repairing data security breaches.

This Response Plan governs incidents that have a significant negative impact on information technology systems and/or sensitive information. Incidents can include denial of service, malware, ransomware, and/or phishing attacks that can significantly impact operations and/or result in the unintended disclosure of sensitive data. Minor events that have little impact on day-to-day operations are not considered an incident under this Plan.

The Incident Response Plan contact numbers and infrastructure information within this document should be printed, and easily accessible in hardcopy form. Digital resources may not be available during an incident.

Preparation

Preparation will be the workhorse of your incident response planning, and in the end, the most crucial phase to protect your district. This phase includes:

- Properly training your employees regarding their incident response roles and responsibilities in the event of a data breach
- Develop incident response drill scenarios and regularly conduct mock data breaches to evaluate your incident response plan.
- Ensure that all aspects of your incident response plan (training, execution, hardware, and software resources, etc.) are approved and funded in advance.

Your response plan should be well documented, thoroughly detailing team members' roles and responsibilities. The district should test the plan to assure that your employees will perform as they were trained. The more prepared your employees are, the less likely they'll make critical mistakes.

Questions to consider annually:

- Has everyone been trained in security policies?
- Has management approved your security policies and incident response plan?
- Does the Incident Response Team know their roles and the required notifications to make?
- Have all Incident Response Team members participated in mock drills?

Developing a comprehensive awareness training program is an essential component to maintaining a secure environment within a school district. Educating staff, students, and other users about potential threats and best practices can significantly reduce the risk of cyber incidents.

- Cover various cybersecurity topics, password hygiene, phishing, malware, social engineering, data protection, and safe internet browsing & information aligns with industry standards and best practices.
- Use a variety of formats, such as presentations, videos, interactive modules, gamification, and quizzes.
- Educate users about strong passwords & the importance of using unique passwords for different accounts.
- Emphasize the significance of regularly updating software and operating systems.
- Teach users to identify common phishing techniques, such as suspicious emails, attachments, & links.
- Encourage the use of multi-factor authentication for added security.

Cyber Security Incident Phases

Detection Steps

A. If a user, employee, or student observes a potential security event they should notify the Technology Coordinator immediately. If the Technology Coordinator is not available, then the event should be immediately reported to another member of the Incident Response Team.

B. The Technology Coordinator will immediately report it to the Incident Response Team. The Technology Coordinator is responsible for communicating the incident, its severity, and developing the action plan with consultation from the Response Team.

C. If the Technology Coordinator or Response Team members are not available, a user should isolate the affected devices from the network or internet by removing the network cable from the device. If operating via wireless, the user should turn off the wireless connection. If isolating the machine from the network is not possible, then the user should unplug the machine from its power source.

D. If the Technology Coordinator determines or suspects a cybersecurity breach, cyber extortion threat, or a data breach as defined in this Plan, then the team will proceed to part E. below. If it is not suspected to be a security incident, then the team will proceed to part F. below.

E. For an actual or suspected security breach, the K12 Data Center and BIT will be contacted immediately. If no answer, the team will leave a message with their contact information. When they respond, the team shall follow their directions.

F. If the incident is determined not to be a security threat, then the Technology Coordinator will work with the Incident Response team to assess the incident, develop a plan to contain the incident, and ensure the action plan is communicated and approved to all users.

G. The Technology Coordinator will ensure that all actions are documented as they are taken and the Incident Response team, and outside support are updated.

Questions to answer while identifying the security event:

- When did the event happen?
- How was it discovered and who discovered it?
- Have any other areas been impacted?
- What is the scope of the compromise?
- Does it affect operations?
- Has the source (point of entry) of the event been discovered?

Identification

During identification, the district will determine whether or not a breach has occurred. A breach or incident could originate from many different areas. A security incident is an event that is a cybersecurity breach, or a cyber extortion threat, or a data breach. In IT, an event is anything that has significance for system hardware or software, and an incident is an event that disrupts normal operations.

Identifying a breach

- **Cybersecurity breach**

A cybersecurity breach is any unauthorized access to, use, or misuse of, modification to the network, and/or denial of network resources by attacks perpetuated through malware, viruses, worms, Trojan horses, spyware, adware, zero-day attack, hacker attack, or denial of service attack.

- **Cyber extortion threat**

A cyber extortion threat is a threat against the network to:

- Disrupt operations.
- Alter, damage, or destroy data stored on the network.
- Use the network to generate and transmit malware to third parties.
- Deface the Member's website.
- Access personally identifiable information, protected health information, or confidential business information stored on the network, made by a person or group whether acting alone or in collusion with others, demanding payment, or a series of payments in consideration for the elimination, mitigation, or removal of the threat.

- **Data Breach**

A data breach is the actual or reasonably suspected theft, loss, or unauthorized acquisition of data that has or may compromise the security, confidentiality and/or integrity of personally identifiable information, protected health information, or confidential business information.

Identifying an Incident

A security incident is a compromise of an organization's systems or data.

Incident Type	Description
Malware	A computer virus, worm, and other malicious applications are computer programs that attack or infect another program. Malware can spread from computer to computer, infecting programs on each computer.
Denial of Service (DoS)	A DOS or a DDOS attack is an attack that prevents or impairs the use of network, system, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and disk space.
Malicious Code	A web application attack happens when hackers compromise an on-line form or application. One way this can happen is with a SQL injection attack. A SQL Injection attack occurs when hackers fill a field with malicious SQL code designed to execute specific commands against the forms or application's database.

Inappropriate Use	Inappropriate usage is when an individual or an entity violates acceptable use of any network, workstation, information, application, server, or data policies.
Ransomware	An attacker installs malware on a device and encrypts the hard drive. The malware announces the hard drive is encrypted and prompts the user to pay a ransom in exchange for the key to unencrypt the device.

Containment

Your initial instinct may be to wipe the affected devices as quickly as possible after discovering a breach. However, that may negatively impact your response in the future since you'll be destroying valuable evidence that you need to determine where the breach started and devise a plan to prevent it from happening again.

Instead, contain the breach so it doesn't spread and cause further damage to your organization. If you can, disconnect affected devices from the Internet. Have short-term and long-term containment strategies ready. It's also good to have a redundant system back-up to help restore operations. That way, any compromised data isn't lost. Also, update and patch your systems and reset passwords.

Questions to consider during containment:

- What have we done to contain the breach today?
- What have we done to contain the breach in the future?
- Has any discovered malware been quarantined from the rest of the environment?
- What sort of back-ups is in place?
- Does your remote access require multi-factor authentication?
- Have all access credentials been reviewed for legitimacy?
- Have you applied all recent security patches and updates?

Eradication

Eradication addresses the root cause of an incident after containment. Eradication is the removal of malicious code, accounts, or inappropriate access and also includes repairing vulnerabilities that may have been the root cause of the compromise. A complete reinstallation of the OS and applications is preferred. Securely remove all malware, harden systems, and apply updates.

Questions to consider during eradication:

- Have artifacts/malware from the attacker been securely removed?
- Has the system been hardened, patched, and updates applied?
- Can the system be re-imaged?

Recovery

Recovery is the process of restoring affected systems and devices. It is important to restore normal operations without the fear of a recurring breach. Recovery allows processes affected by the Incident to recover and resume operations. It generally includes:

- Reinstall and patch the OS and applications.
- Change all user and system credentials.
- Restore data to the system.
- Return affected systems to an operationally ready state.
- Confirm that the affected systems are functioning normally.

Questions to consider during Recovery:

- When can systems be returned to production?
- Have systems been patched, hardened, and tested?
- Can the system be restored from a trusted back-up?
- How long will the affected systems be monitored, and what will you look for when monitoring?
- What tools will ensure similar attacks will not reoccur?

Post-Incident Review

To improve the Incident Response processes and identify recurring issues each Incident should be reviewed and formally reported on. The report should include:

- Information about the Incident type
- A description of how the Incident was discovered.
- Information about the systems that were affected.
- Information about who was responsible for the system and its data.
- A description of what caused the Incident.
- A description of the response to the Incident and whether it was effective.
- A timeline of events, from detection to Incident closure
- Recommendations to prevent future Incidents.

Lessons Learned

Once the investigation is complete, hold an after-action meeting with all Incident Response Team members and discuss what you've learned from the event. You will analyze and document everything. Determine what worked well in your incident response plan and where you could improve it. Lessons learned from both mock and real events will help strengthen your systems against future attacks.

Questions to discuss during lessons learned:

- What changes should be made to security?
- How could employees be trained differently?
- What weakness did the breach exploit?
- How will you ensure a similar breach doesn't happen again?

APPENDIX A: Incident Response Flowchart