NEW LEBANON CENTRAL SCHOOL DISTRICT

Cyber Security Incident Response Plan

October 1, 2021

Table of Contents

Cyber Security Incident Response Plan

Revision History

Version	Change	Author(s)	Date of Change
0.1	Initial Draft		xx/xx/2021

Supporting Documents - See Appendix

- Cyber Security Incident Response Policy (to be developed)
- Cyber Security Incident Communications Template
- Cyber Security Incident Runbooks:
    - Social Engineering
    - Information Leakage
    - Insider Abuse
    - Phishing
    - Scam
    - Trademark Infringement
    - Ransomware
    - Worm Infection
    - Windows Intrusion
    - Unix Linux Intrusion Detection
    - DDOS
    - Malicious Network Behavior
    - Website Defacement
    - Windows Malware Detection
    - Blackmail
    - Smartphone Malware
- Lessons learned Analysis Report Template

Introduction

Purpose

The purpose of this document is to define a high-level incident response plan for any cyber security incident. It is used to define general communication processes for managing cyber security incidents, which may help minimize the impact and scope of the incident on the organization.

Defining standard incident handling protocols helps reduce ambiguity in the case of an incident and helps keep stakeholders accountable and aware of the incident.

This Cyber Security Incident Response Plan will be regularly reviewed, evaluated, and updated as part of New Lebanon CSD on-going cyber security program. This also involves appropriate training of resources expected to respond to cyber security incidents, as well as the training of general employees regarding New Lebanon CSD expectations of them regarding cyber security responsibilities.

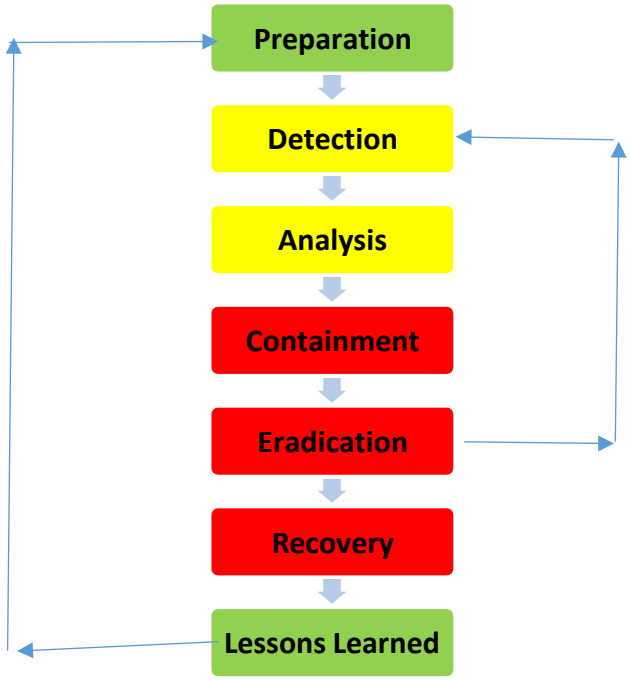
Definitions –

Term	Definition
Cyber Security Event	Identified occurrence of a system, service, or network state indicating a possible breach of information cyber security policy or failure of controls, including false alarms.
Cyber Security Incident	Single or series of unwanted or unexpected information cyber security events that have a significant probability of compromising business operations and threatening information security.
Data Loss Prevention (DLP)	A systems' ability to identify, monitor, and protect data in use, data in motion, and data at rest through content inspection, contextual security analysis of transaction, within a centralized management framework. Data loss prevention capabilities are designed to detect and prevent the unauthorized use and transmission of data or information. (NIST Computer Security Resource Center)
Family Educational Rights and Privacy Act (FERPA)	The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.
Incident Responder	A member of an incident response team, which is established to handle the intake, communication, and remediation of security incidents. If there is no dedicated incident response team, staff responding to incidents when required may be referred to as "incident responders."
Indicators of Compromise (IoC)	Indicators of Compromise are "pieces of forensic data, such as data found in system log entries or files that identify potentially malicious activity on a system or network." Indicators of compromise aid information security and IT professionals in detecting data breaches, malware infections, or other threat activity. By monitoring for indicators of compromise, organizations can detect attacks and act quickly to prevent breaches from occurring or limit damages by stopping attacks in earlier stages.
Intrusion Detection System (IDS)	Software that looks for suspicious activity and alerts administrators. (NIST Computer Security Resource Center)
Intrusion Protection System (IPS)	Software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents. (NIST Computer Security Resource Center)
Protected Health Information (PHI)	Protected health information is considered to be individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations (PHI healthcare business uses). (HIPAA Journal)
Personally Identifiable Information (PII)	PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing

	this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available - in any medium and from any source - that, when combined with other available information, could be used to identify an individual. (OMB Memorandum M-07-1616)
Runbook	A Runbook consists of a series of conditional steps to perform actions, such as data enrichment, threat containment, and sending notifications, automatically as part of the incident response or security operations process. This automation helps to accelerate the assessment, investigation, and containment of threats to speed up the overall incident response process. Runbooks can also include human decision making elements as required, depending on the particular steps needed within the process and the amount of automation the organization is comfortable using.
SIEM	Security Information and Event Management is a software solution that aggregates and analyzes activity from many different resources across the entire IT infrastructure. SIEM software typically collects security data from network devices, servers, domain controllers, and other monitoring systems.
Threat Escalation Protocol (TEP)	Incidents should be assessed based on their impact on the organization and the scope of IT systems within the organization. The combination of these two factors will provide insight into the threat escalation protocol, indicating the types of stakeholders typically needed for those types of incidents.

Organizational Approach to Cyber Security Incident Response

New Lebanon CSD's organizational approach to cyber security incident response and management is based on and follows the general guidelines in alignment with NIST SP 800-61 Rev. 2, which includes the following phases:



Incident Response Phases based on NIST SP 800-61 Rev. 2

This program fits into the New Lebanon CSD overall cyber security incident response program by following similar procedural protocol. By adhering to similar processes across the board, we can maintain consistency and to ensure that responses are comprehensive, preventing as many potential incident information gaps as possible.

Communicating the cyber security incident both internally and externally (as needed) is an important part of this process. However, depending on the nature of the cyber security incident, communications may occur at different stages and are likely to be necessary more than once to update stakeholder groups as new information becomes available during the cyber security incident response process.

Cyber Security Incident Response Team (CSIRT)

A Cyber Security Incident Response Team (CSIRT) has been created to help New Lebanon CSD respond to cyber security incidents. The CSIRT is NOT just for IT Staff nor Management, but instead is comprised of staff with different skillsets and from different New Lebanon CSD organizational levels.

Roles and Responsibilities

The CSIRT is comprised of individuals who have roles and are responsible for responding to a cyber-security incident, also known as the incident responders. CSIRT members include:

Internal Members:

- Incident Commander – Andrew Kourt
- Management – Ethan Race/Francis Rielly
- Technical – Ethan Race
- Legal – Whiteman, Osterman, Hannah- Beth Bourassa
- Compliance – Andrew Kourt
- Human Resources – Andrew Kourt
- Communications – Jason Laz
- Public Relations – Jason Laz
- Finance – Francis Rielly
- Facilities – Francis Rielly
- Security – Deputy Patrick McMahon, Sheriff's Deputy

External Members:

- Insurance Company: Utica National
- Legal: Whiteman, Osterman, Hannah- Beth Bourassa
- Cyber Incident Response – Andrew Kourt
- Law Enforcement - Columbia County Sheriff, State Police, Homeland Security, FBI (As Needed)

RACI Matrix

The RACI matrix below is used to identify and avoid confusion in roles and responsibilities during a cyber-security incident remediation. The RACI acronym stands for:

- **Responsible.** The person(s) **who does the work** to accomplish the activity; they have been tasked with completing the activity, and/or getting a decision made.
- **Accountable.** The person(s) **who is accountable for completing the work**. Ideally, this is a single person and is often an executive or program sponsor.
- **Consulted.** The person(s) **who provides information about the work**. This is usually several people, typically called subject matter experts (SMEs).

- **Informed.** The person(s) **who is updated on progress of the work**. These are resources that are affected by the outcome of the activities and need to be kept up to date.

Legend: **R – Responsible – Who does the work** **A – Accountable – For completing the work** **C – Consulted – Provides info about the work** **I – Informed – Who is updated on progress of work**	**Users**	**IT Manager**	**Superintendent**	**Business Official and Facilities**	**Legal / Compliance**	**Communications**	**NERIC**	**Law Enforcement**		
Detection										
Report a suspected incident, such as a service disruption, a suspicious email, or an unusual endpoint behavior.	R/A	R/A	R/A	R/A	-	R/A	R/A	-	-	-
Analysis										
Gather answers to incident-related questions.	R	R/A	I	I	C	-	C	C/I	-	-
Perform Indicators of Compromise (IoC) search (firewall, IDP, email gateway, SIEM, logs, etc.).	-	R/A	I	I	-	-	C	-	-	-
Determine what, if any, systems or devices were compromised (e.g., end-user devices, servers, applications).	-	R/A	I	I	-	-	C	-	-	-
Assess the impact to servers, applications, storage, or other systems.	-	R/A	I	I	-	-	C	I	-	-
Determine the scope/breadth of the incident.	-	R/A	I	I	-	-	C	I		-
Review security events and determine if a true security incident occurred.		R	A	I	-	-	C	I	-	-
Communicate with senior management about significant incidents.	-	R/A	A	R/A	-	-	-	I	I	-
Communicate with organization about significant incidents.	-	R/A	A	I	-	-	-	-	-	-
Determine if any regulatory, legal, or compliance mandates have been impacted, including breach notification requirements.	-	R/A	A	A	C	-	-	-	-	-
Determine if any employee disciplinary actions are required.	-	-	R/A	R/A	C/A	R	-	A	-	-
Determine if any public reputational or brand damage needs addressing.	-	-	A	I	C	R	-	-	-	-
Determine if a crime was committed.	-	-	A	I	R	-	C	A	-	-
Containment										
Isolate or disconnect any infected endpoints or servers from the network, if necessary.	-	R/A	I	I	-	-	C	-	-	-
Disable compromised user accounts, change passwords, or remove privileges, if necessary.	-	R/A	I	I	-	-	C	-	-	-

Notify affected users and stakeholders of containment efforts that will affect services.	-	R	R/A	R/A	-	-	C	I	-	-
Create an OS-level image of any endpoint, servers, or storage arrays.	-	R/A	I	I	-	-	C	-	-	-
Provide senior management with incident updates.	-	R/A	I	I	-	-	-	-	-	-
Commence any legal actions, if necessary.	-	-	R/A	I	R	-	-	R	-	-
Implement public relations/communications campaign to reduce reputational damage as appropriate.	-	-	R/A	C	C	R	C	-	-	-
Eradication										
Seize, prepare replacement, and reissue end-user device(s).	-	R/A	I	I	-	-	C	-	-	-
Eliminate the root cause of the incident (e.g., remove malware, block unauthorized users).	-	R/A	I	I	-	-	C	-	-	-
Install system and security patches to resolve malware/network/other vulnerabilities.	-	R/A	I	I	-	-	C	-	-	-
Build replacement servers, if necessary.	-	R/A	I	I	-	-	C	-	-	-
Recovery										
Re-issue devices and/or credentials, if necessary.	-	R/A	I	I	-	-	C	-	-	-
Restore data from backups.	-	R/A	I	I	-	-	C	-	-	-
Restore servers and other systems, as necessary.	-	R/A	I	I	-	-	C	-	-	-
Perform vulnerability assessments, anti-virus, anti-malware scans, and other tests to verify that operations are back to normal.	-	R/A	I	I	-	-	C	-	-	-
Maintain communication with end users (e.g., informing when operations are back to normal).	-	R	A	I	-	I	-	I	-	-
Communicate with stakeholders that the incident is resolved, next steps, etc.	-	R	A	I	-	I	-	-	-	-
Ensure appropriate incident record/ticket is updated and closed, if resolved.	-	R	I	I	-	-	C	-	-	-
Lessons Learned										
Perform root-cause analysis.	-	R/A	I	I	-	-	C	-	-	-
Facilitate post-incident lessons learned meetings, when appropriate.	C	R	A	A	-	-	C	-	-	-
Identify changes to current technology to reduce the chance of reoccurrence.	-	R	A	A	-	-	C	-	-	-
Implement updates to current technology to reduce the chance of reoccurrence.	-	R	A	A	-	-	C	-	-	-
Update incident response material, including runbooks, with new processes.	-	R	A	A	-	-	C	-	-	-
Enforce any employee disciplinary actions, if required.	-	-	R/A	R/A	C	-	-	-	-	-
Conduct tabletop exercises or attack		R	R/A	R/A	-	-	C	-	-	-

Source: https://us-cert.cisa.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-IM.pdf

simulations.										

Communications with Stakeholders

Cyber security incident response communications, both internal and external, should be drafted and delivered according to a formal process designed to maximize the efficiency and effectiveness of statements, memos, press releases, etc. made during the discovery and remediation of a cyber-security incident.

Cyber security incidents are often chaotic, and they pose a significant risk to an organization's reputation and client base. Stability can be provided by outlining regulatory obligations and their reporting procedure and by defining proper communications protocols for various groups, such as employees, external stakeholders, and the media.

Communicating during an incident is a critical part of the Incident Response Process. To the extent possible it is recommended that pre-written templates be used. During an incident it is very important that relevant parties are informed, and that messaging conveys the proper tone and level of information necessary.

The communications should be specifically tailored to the end user of the messaging which could be employees, the public, or possibly law enforcement.

Please see the “Communication Templates” section in Appendix A for more details.

Cyber Security Incident Assessment

Cyber security incidents should be assessed based on their impact to the organization and the scope of IT systems within the organization. The combination of these two factors will provide insights necessary to develop an effective TEP, indicating the types of stakeholders typically needed for those kinds of incidents.

Impact Criteria

Evaluate the impact on business functions, information, and recovery efforts. Overall incident impact should be assessed based on the *highest* impact level of the three incident types below:

1. **Functional impact:** The impact as it relates to the availability and delivery of services and business functions. Is a critical system affected? Does it hinder functionality for users?
2. **Information impact:** The impact as it relates to the confidentiality, integrity, and availability of the organization’s data. What sensitivity of data is affected? What does it mean for the organization (e.g., notification requirements, regulatory fines)?
3. **Recoverability impact:** The time and resources required to recover from the incident. What needs to be done for recovery?

Table 1. Impact Criteria

Impact Criteria	
Rating	**Definition**
High	There is a **high** impact if at least one of the following is true: • The organization is no longer able to provide some critical service(s) to any users and a critical business function cannot be performed OR • Regulated or highly sensitive data has been compromised. Regulatory actions may be required OR • Full recovery from the incident is not possible or will require significant external resources. There is severe reputational damage OR • Financial loss is $50,000 or greater.
Medium	There is a **medium** impact if at least one of the following is true and the impact was **not** high: • The organization is no longer able to provide some secondary services to any users OR • The organization is no longer able to provide some critical services to a subset of users, but a workaround is available OR • Sensitive/confidential data has been exposed, but no regulatory actions are required OR • Recovery from the incident is possible, but requires additional resources (e.g., overtime) OR • Financial loss is between $10,000 to $50,000.
Low	There is **low** impact if at least one of the following is true and the impact was not high or medium: • The organization is experiencing minimal effects to services. All services are available, but efficiency has been affected OR • Public data has been affected, but no regulatory actions or penalties are required OR • Recovery from the incident is possible and predictable with existing processes OR • Financial loss is less than $10,000.
None	There is **no** impact if all the following are true (e.g., false alarm; not a true security incident): • There is no effect to the organization's ability to provide service to users AND • No information was exposed or affected in an unauthorized manner AND • No significant recovery time or resources are required AND • Financial loss is negligible.

Scope Criteria

Evaluate the scope (i.e., breadth/magnitude) of the incident on systems, users, endpoints, etc. Incident scope is a critical component that aids in decision making throughout the incident response process.

Table 2. Scope Criteria

Scope Criteria	
Rating	**Definition**
High	>99 individuals, systems, or processes affected AND/OR 1+ server was compromised, AND/OR 1+ executive was targeted, AND/OR >9 sensitive records exposed, AND/OR a crime was committed.
Medium	11-99 individuals, systems, or processes affected AND/OR 1-9 sensitive records exposed.
Low	<10 individuals, systems, or processes affected.

Threat Escalation Protocol

A Threat Escalation Protocol (TEP) outlines the types of stakeholders needed during the cyber security incident response process. Informing and consulting these stakeholders during the cyber security incident response process is crucial when defending the organization against incidents. The TEP clearly defines escalation procedures for incidents.

Table 3. Threat Escalation Protocol

Threat Escalation Protocol (TEP)			
Impact	**Scope**		
	Low	**Medium**	**High**
High	**Tier 2**	**Tier 1**	**Tier 1**
Medium	**Tier 2**	**Tier 2**	**Tier 1**
Low	**Tier 3**	**Tier 2**	**Tier 2**

Threat Escalation Protocol (TEP)	Criteria	Stakeholders
Tier 1	• High impact, high scope • High impact, medium scope • Medium impact, high scope	• End User • Help Desk • IT Operations • Technical Lead • Legal / Compliance • Human Resources • Communications / PR • Senior Management • Executive Management • External Third Parties
Tier 2	• High impact, low scope • Medium impact, medium scope • Medium impact, low scope • Low impact, high scope • Low impact, medium scope	• End User • Help Desk • IT Operations • Technical Lead • Legal / Compliance (as needed) • Senior Management (as needed)
Tier 3	• Low impact, low scope	• End User • Help Desk • IT Operations

Response Procedures

The actions required to deal with cyber security incidents are detailed below for each relevant stakeholder, in each of the seven phases (preparation, detection, analysis, containment, eradication, recovery, and lessons learned).

Phase 1 - Preparation

During the Preparation Phase teams begin to put in place what they will need to help them respond to an incident in the best way possible. Proper policies, procedures, and tools need to be put into place.

Technologies involved in this phase include:

- Firewalls
- IDS/IPS
- Web proxy
- Antivirus
- Anti-malware
- Email gateway
- SIEM

Preparation Phase			
Team	**Description**	**Questions**	**Action**
Preparation: End User	No incident response responsibilities.		
Preparation: Help Desk	During the preparation phase, help desk staff will make sure they are ready to respond to incidents.	• Am I aware of my responsibilities as they relate to incident response? • Do I need any additional training?	☐ Review and understand incident response roles and responsibilities. ☐ Take training courses and participate in available webinars
Preparation: IT Operations	During the preparation phase, cybersecurity staff configure firewall, IDS/IPS, web proxy, antivirus, anti-malware, email gateway, SIEM, DLP, and other systems to enable them to better detect potential issues	• Have we kept up to date with patches to our systems? • Have we researched new technologies to increase our cybersecurity posture? • Are we taking advantage of new features and functionality? • Do we need any additional training?	☐ Review new technologies on a regular basis. ☐ Update firewalls, IDS/IPS, DLP, web proxy connections, antivirus, anti-malware, and other systems. ☐ Take training courses and participate in available webinars
Preparation: Technical Lead	During the preparation phase the TECHNICAL LEAD will ensure that the CSIRP is up to date and tested and that the organization is ready to respond to an incident.	• Has the IR plan been updated and tested? • Have employees received up to date, relevant cyber security training? • Do employees know how to report a potential incident? • Are the members of the	☐ Plan and execute a tabletop exercise. ☐ Ensure all employees are trained to help avoid and report potential cybersecurity incidents. ☐ Hold meetings with the CSIRT on a regular basis.

		CSIRT aware of their roles and responsibilities?	
Preparation: Legal, Compliance, HR, PR, Communications	During the preparation phase these areas will try to identify changes to laws, policies, etc. that could require changes to the IR plan or response procedures. These areas will work together to create appropriate communications templates.	• Are there any new laws or policies that New Lebanon needs to comply with? • Do we have any additional reporting requirements?	☐ Take training courses and participate in available webinars.
Preparation: Senior Management	No incident response responsibilities.		

Phase 2 - Detection

During the Detection Phase, teams evaluate a potential cyber security incident. Once an incident has been detected, a help desk ticket or incident record/ticket is opened to initiate the detection phase.

Incident triggers can include:

1. End users reporting to help desk.
2. Technology trigger (FW, IDS/IPS, etc.)
3. Pen tests (vulnerability management)
4. Hunt function (threat intel)

Technologies involved in this phase include:

- Firewalls
- IDS/IPS
- Web proxy
- Antivirus
- Anti-malware
- Email gateway
- SIEM

Detection Phase			
Team	**Description**	**Questions**	**Action**
Detection: End User	During the detection phase, the end user may report suspicious behaviors or issues and system/service disruptions.	• Did I receive a suspicious email? • How do I resolve the issue with my endpoint? • Why is a system or service not available or behaving abnormally? • Is my device possibly lost or stolen? • Why can't I access my data or account?	☐ Report a suspected incident or issue to help desk. Examples include: ○ Data is missing/altered. ○ Passwords aren't working. ○ Experiencing significant number of pop-up ads. ○ Computer keeps crashing. ○ Account/network cannot be accessed.
Detection: Help Desk	During the detection phase, help desk staff will monitor calls and submitted tickets.	• Are any end users experiencing potential security incidents?	☐ Open a help desk ticket. (see Appendix for examples of information to be included in a help desk ticket.) ☐ Determine if incident needs to be escalated to other stakeholders. ☐ Assign help desk ticket to appropriate team and/or begin the Analysis phase.
Detection: IT Operations	During the detection phase, cybersecurity staff monitor firewall, IDS/IPS, web proxy, antivirus, anti-malware, email gateway, SIEM, DLP, and other events, and escalate to incidents as needed.	• Are assets or services being impacted by a security incident? • Has data been exposed or exfiltrated? • Has an executive been targeted or affected by a security incident? • Are security technologies identifying one or a series of events?	☐ Identify suspicious behavior of assets or services. ☐ Review events from sources such as a firewall, IDS/IPS, DLP, web proxy connections, antivirus, anti-malware, email gateway, SIEM logs, or other security. ☐ Determine if incident needs to be escalated to initiate the incident management process.

Detection: Technical Lead	No incident response responsibilities.		
Detection: Legal, Compliance, HR, PR, Communications	No incident response responsibilities.		
Detection: Senior Management	No incident response responsibilities.		

Phase 3 - Analysis

During the Analysis Phase, teams will investigate the incident to determine the impact and scope of the threat. Depending on the impact and scope, a threat escalation tier level will be assigned, indicating the number of teams that will be involved in the remediation of the incident, and the notification of the threat will be escalated as appropriate. A third party may be involved if deep forensic analysis is needed.

Technologies involved in this phase include:

- Firewalls
- IDS/IPS
- Web proxy
- Email gateway
- SIEM or another log correlator
- Digital forensics tools, including:
    - File viewing and analysis tools
    - OS analysis tools
    - Network analysis tools
    - Database analysis tools
- Threat intelligence

Analysis Phase			
Team	**Description**	**Questions**	**Action**
Analysis: End User	During the analysis phase, end users will provide information related to the incident as required.	• What are the events that led up to this suspected incident? • What did I do as a result?	☐ Provide information related to the incident to the help desk.

Analysis: Help Desk	During the analysis phase, help desk staff directly interact with the end user, ask incident-related questions, take actions, and document findings in the help desk ticket.	• What may have caused the incident?
		  ○ Did the end user click a hyperlink or open a file attachment?
		  ○ Did the end user visit a suspicious website?
		  ○ Did the end user download software recently?
		  ○ Did the end user plug in a flash drive?
		• What type of user is affected – i.e., what privileges does the user have?
		• Are any locally stored suspicious file extensions identified?
		• Has the end user been denied access when accessing data or a server?
		• If a device was misplaced, where was it last seen?
		• What types of data or
			☐ Open a help desk ticket, if not opened.
			☐ Gather answers to incident-related questions and document findings in the ticket.
			☐ Identify incident-related keywords *(malware, ransomware, distributed denial of service [DDoS], compromised credentials)*.
			☐ Search ticketing platform to identify other impacted end users. If multiple end users are impacted, create a parent/child ticket.
			☐ Determine the impact and scope of the incident.
			☐ Assign help desk ticket to cybersecurity team, as appropriate.
			☐ Facilitate end-user notifications.
			☐ If the incident was a false positive, update the ticket and close the incident record.

		equipment were involved?	

Analysis: IT Operations	During the analysis phase, cybersecurity staff will analyze appropriate logs, conduct open-source intelligence research, provide technical support, provide incident coordination support, interact with the end user directly, ask incident-related questions, take actions, and document findings in the incident record.	• What may have caused the incident?
		  ○ Did the end user click a hyperlink or open a file attachment?
		  ○ Did the end user visit a suspicious website?
		  ○ Did the end user download software recently?
		  ○ Did the end user plug in a flash drive?
		• Are any other IoCs identified within the organization?
		• What type of user is affected; i.e. what privileges does the user have?
		• Are any locally stored suspicious file extensions identified?
		• Has the end user been denied access when accessing data or a server?
		• If a device was misplaced, where was it last seen?
		What types of data or equipment were involved?
			☐ Gather answers to incident-related questions.
			☐ Conduct open-source threat intelligence analysis to identify comparative IoCs.
			☐ Perform IoC search in firewall, IDS, IPS, email gateway, and system and server logs.
			☐ Determine the scope of the incident, such as how much of the network was impacted, how many endpoints, or how many files were compromised.
			☐ Determine the scope and impact of the incident, and the resulting TEP tier level.
			☐ Determine if any end-user device or devices were compromised.
			☐ Assess if any servers were impacted and decide if any server infections are to be assigned to the infrastructure team.
			☐ Based on the scope and impact, determine the TEP tier level. Inform necessary parties, as required.
			☐ If there are any indications that a crime was committed, immediately escalate to the TECHNICAL LEAD.
			☐ If the incident was a false positive, update the ticket and close the incident record.
			☐ Investigate and respond to security events.

Analysis: Technical Lead	During the analysis phase, TECHNICAL LEAD will notify and coordinate with the relevant stakeholders and senior management.	• Has a crime been committed? • Has data been lost or stolen? • Are any business applications impacted? • Does a disaster recovery plan need to be enacted?	☐ Publish corporate-wide situational awareness alerts to inform end users of any system outages. ☐ Coordinate and inform senior management of any incident updates. ☐ Approve disaster recovery plan enactment, if necessary. ☐ Report any external criminal activities to senior management. ☐ Engage Legal, HR, and PR to address the incident, as appropriate. ☐ Determine if any incident information should be shared with external parties.
Analysis: Legal, Compliance, HR, PR,	During the analysis phase, legal, HR, and PR staff will analyze any insider	• Are there potential legal repercussions to the incident? • Was there any insider	Legal: ☐ Determine if any regulatory, legal, or compliance mandates have been violated or impacted.

Communications	activity, legal requirements, and brand/ reputational damage.	activity or other misuse of assets? • Was there any brand or reputational damage?	☐ Determine if any breach notifications are required. ☐ Begin process to notify required parties. Human Resources: ☐ Determine if any employee acceptable-use or security policies have been violated. ☐ Determine if any preliminary employee disciplinary actions are required immediately. Public Relations: ☐ Determine if any public reputational or brand damage has occurred. If so, begin process/campaign to address it.
Analysis: Senior Management	During the incident response analysis phase, senior management staff will notify and coordinate with the relevant stakeholders.	• Was there any insider activity or other misuse of assets? • Have any core business functions been affected? • Was there any brand or reputational damage? • Has a crime been committed? • Has data been lost, and does a disaster recovery plan need to be enacted?	☐ Provide an incident summary and updates to the board of directors/ stakeholders. ☐ Approve reporting crime to law enforcement, if necessary. ☐ Analyze and approve emergency budget, resource, or control requests, as appropriate. ☐ Approve communication of incident information with external parties.

Phase 4 - Containment

During the Containment Phase, teams will isolate and contain the incident to limit its ability to spread to the rest of the organization.

Technologies involved in this phase include:

- Network isolation
- Endpoint isolation
- Endpoint containerization

Containment Phase			
Team	**Description**	**Questions**	**Action**
Containment: End User	No containment responsibilities beyond ongoing cooperation with incident responders.		
Containment: Help Desk	During the containment phase, the help desk will maintain communications with any impacted end users.	• Do any end users need to be notified?	☐ Maintain communications with any impacted end users. ○ Inform users if any critical systems or data will be unavailable or affected during the response process.
Containment: Cybersecurity	During the containment phase, the cybersecurity team will provide support to isolate the incident and remove compromised assets/users, if necessary.	• How can the issue be isolated with minimal disruption (sandboxing, quarantining, revoking user access, etc.)? • Was a server infected? Can it be quarantined? • What stakeholders need to be notified?	☐ Provide incident coordination support. ☐ Isolate or disconnect any infected endpoints from the network, shut down organizational Internet access, if necessary. ☐ Disable compromised user accounts, change passwords, or remove privileges, if necessary. ☐ Determine if other actions are necessary to contain the spread of the incident. ☐ Notify affected users and stakeholders. ☐ Create an OS-level image of any endpoint, servers, or storage arrays to prevent future data loss. ☐ Isolate or disconnect any servers and/or infected endpoints. ☐ Disable compromised accounts or change passwords. Change the password to the affected system.
Containment: Technical Lead	During the containment phase, the TECHNICAL LEAD will evaluate any control weaknesses and make recommendations for	• Are the current security controls sufficient?	☐ Provide senior management with incident updates. ☐ Approved additional resourcing of controls or processes, as necessary for the containment of the incident.

	remediation.		
Containment: Legal, Compliance, HR, PR, Communications	During the containment phase, PR may address the public and other stakeholders to inform them of the status of the incident and contain possible rumors, speculation, and reputational damages. Legal and HR will continue ongoing efforts that began in the Analysis phase.	• What types of communication are required? • Are there any Legal and HR processes that need to be continued?	Legal: ☐ Continue legal actions as necessary, informing affected parties as required by regulations. PR: ☐ If necessary, address the affected stakeholders (including the public), informing them of the steps that have been taken to contain the incident and future steps to fully remediate the incident. HR: ☐ Continue HR actions, as necessary, particularly containing any further employee misuse or violations.
Containment: Senior Management	During the containment phase, senior management will determine if any core business function is impacted and will provide final approval for drastic measures.	• Do any business-critical services, systems, or data need to be taken offline for effective containment of the incident?	☐ Determine if any additional stakeholders need to be notified. Provide the notification. ☐ Provide final approval for taking business-critical systems offline or other major containment decisions.

Phase 5 - Eradication

During the Eradication Phase, teams will eliminate components of the incident, such as deleting malware and removing unauthorized user access, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, it is important to identify all affected hosts within the organization so that they can be remediated. For some incidents, eradication is either not necessary or is performed during recovery.

Technologies involved in this phase include:

- Network isolation
- Endpoint isolation
- Endpoint containerization

Eradication Phase			
Team	**Description**	**Questions**	**Action**
Eradication: End User	No eradication responsibilities beyond ongoing cooperation with incident responders.		
Eradication: Help Desk	During the eradication phase, the help desk will maintain communications with impacted end users and reissue devices, if necessary.	• Does the end user need to be notified of any updates? • Do any users need new/updated devices issued?	☐ Seize, prepare replacement, and reissue endpoint, if necessary. ☐ Maintain communications with any impacted end users.
Eradication: IT Operations	During the eradication phase, IT Operations will ensure possible sources of compromise are eliminated. IT Operations will install patches and eliminate other possible sources of the incident.	• Are there any infected endpoints still on the network? • Are there any compromised user accounts still on the network? • Have systems been adequately patched? • What data needs to be restored? • Are there any control gaps that allowed this incident to occur?	☐ Eliminate the root cause of the incident (e.g. remove malware/virus, block all unauthorized users, de-escalate elevated privileges). ☐ Backup affected systems for later investigation and forensics. ☐ Install system/security patches to resolve malware/network/other vulnerabilities. ☐ Build replacement server. ☐ Disable breached user accounts. ☐ Inform the TECHNICAL LEAD of any organizational security control gaps, if necessary.
Eradication: Technical Lead	During the eradication phase, the TECHNICAL LEAD will approve new or updated controls.	• Do any new controls need to be implemented? • Do any controls need to be updated? • Are there any control gaps that allowed this incident to occur?	☐ Approve new controls and the updating of existing ones.
Eradication: Legal,	During the eradication phase,	• Are there any changes to Legal, HR, or PR	☐ Reassess if any new findings have changed the required

Compliance, HR, PR, Communications	Legal, HR, and PR staff will evaluate if any new findings have led to new actions, otherwise they will continue any ongoing processes.	requirements?	Legal, HR, or PR actions. If so, address those requirements. ☐ Otherwise continue Legal, HR, and PR efforts already begun.
Eradication: Senior Management	No specific eradication responsibilities beyond ongoing support and approval, as necessary.		

Phase 6 - Recovery

During the Recovery Phase, teams will enact processes and procedures for recovery and full restoration of any systems, devices, or accounts during the incident. In recovery, responders will restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents.

Recovery may involve actions such as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, re-issuing devices, and tightening network perimeter security (e.g., firewall rulesets, boundary router access control lists).

Technologies involved in this phase include:

- System backup tools
- Patches
- Vulnerability scanners

Recovery Phase			
Team	**Description**	**Questions**	**Action**
Recovery: End User	No recovery responsibilities beyond ongoing cooperation with incident responders.		
Recovery: Help Desk	During the recovery phase, the help desk will maintain communications and coordinate recovery with affected end users.	• Does the end user need to be notified? What do they need to know? • Is the ticket up to date?	☐ Maintain communications with any impacted end users. Inform users: ○ When operations are back to normal. ○ Of any required changes (e.g. updates to systems, passwords). ○ Of updated training and awareness material regarding the incident. ☐ Re-issue end-user devices and credentials, if necessary. ☐ Ensure help desk ticket is updated with all relevant information.
Recovery: IT Operations	During the recovery phase, IT Operations will recover and restore systems back to regular operations.	• Do any other servers or systems need to be restored? • Is the incident report comprehensive? • Has the incident been successfully remediated?	☐ Rectify any component that was compromised; restore systems and data, as necessary. ☐ Once restored, perform system/ network/device validation and testing to verify that the system functions the way it was intended/had functioned in the past. Coordinate with the business units as needed. ☐ Perform vulnerability assessment, antivirus, and anti-malware scans

			on any endpoints or servers to ensure that operations are back to normal. ☐ Ensure incident record/ticket is updated with relevant information. ☐ Advise the TECHNICAL LEAD of any controls, processes, or policies that need to be updated.
Recovery: Technical Lead	During the recovery phase, the TECHNICAL LEAD will evaluate any weaknesses in security controls or policies as appropriate.	• Do any controls or policies need to be updated?	☐ Review any security policies or controls, as appropriate. ☐ Inform senior management that operations have been restored.
Recovery: Legal, Compliance, HR, PR, Communications	During the recovery phase, Legal, HR, and PR staff will complete their respective processes, and ensure all actions are documented.	• Do any employees need disciplinary action? • What message needs to be communicated to stakeholders/the public? • What legal or regulatory next steps are required?	☐ Legal: Follow-up with any legal implications and requirements. ☐ HR: Ensure employee records are updated with any infractions (e.g., misuse of corporate resources causing an incident) and subsequent disciplinary actions. If disciplinary actions have not been issued yet, begin process in coordination with the employee's manager. ☐ PR: Communicate with stakeholders/public that the incident has been resolved, including next steps.
Recovery: Senior Management	No incident response responsibilities.		

Phase 7 – Lessons Learned

During the Lessons Learned Phase, teams will perform root-cause analysis and lessons learned activities with various teams and stakeholders within the organization. Any recommended outcomes should be implemented to ensure continuous improvement, and all related active tickets should be updated and closed.

This phase involves performing a post-mortem, root-cause analysis, and lessons learned activities with various teams and stakeholders within the organization. Any recommended outcomes should be implemented to ensure continuous improvement, and all related active tickets should be updated and closed.

Lessons Learned Phase			
Team	**Description**	**Questions**	**Action**
Lessons Learned:	During the lessons learned phase,	• What happened? • What was learned?	☐ If necessary, a primary affected user may answer questions

End User	affected users may provide additional details for post-incident meetings/reports and may participate in additional awareness and training.	• What has changed?	regarding the source of the incident. ☐ General end users may participate in updated awareness and training as a result of the incident.
Lessons Learned: Help Desk	During the lessons learned phase, the help desk may participate in post-incident meetings, as necessary.	• What happened? • How did we respond? • What should we do next time?	☐ Participate in lessons learned (post-mortem) meetings, as necessary.
Lessons Learned: IT Operations	During the lessons learned phase, IT Operations will support any post-incident activities, as appropriate.	• What happened? • How did we respond? • What should we do next time? • Are there any IT operations processes that need to be improved?	☐ Participate in any post-incident meetings, as appropriate. ☐ Update and close incident ticket
Lessons Learned: Technical Lead	During the lessons learned phase, the TECHNICAL LEAD will facilitate any post-incident activities.	• How can the incident response process be improved?	☐ Determine if a full-fledged post-mortem/lesson learned meeting is necessary. ☐ Determine who should participate (e.g. end users, Legal, Compliance, HR, PR, Communications). ☐ Facilitate post-incident meetings (or assign the responsibility to another individual). Ensure a record is maintained.
Lessons Learned: Legal, Compliance, HR, PR, Communications	During the lessons learned phase, Legal, HR, and PR staff will support any post-incident activities, as appropriate.	• Are there any Legal, HR, or PR processes that need to be improved?	☐ Participate in any post-incident meetings, as appropriate. ☐ If new findings become known as a result of post-incident activities, follow-up with any new or ongoing Legal, HR, and PR duties that have not already been addressed. ☐ Legal: Follow up with any legal actions, if required. ☐ HR: Follow up with any employee disciplinary action, if required. ☐ PR: Follow up on public and internal communications to address the resolution of the incident and steps being taken to prevent reoccurrences.
Lessons Learned: Senior Management	During the lessons learned phase, senior management will	• Are there any senior management processes that need to be improved?	☐ Participate in any post-incident meetings, as appropriate. ☐ Address stakeholders/board of directors, if necessary.

	support any post-incident activities, as appropriate.		☐ Approve future investments to help prevent reoccurrences.

Help Desk Ticket Information

The following are examples of the information that should be collected by the help desk when generating an incident ticket:

- Contact name and number of people reporting the incident.
- Type of data, systems, or equipment involved.
- Category of the incident and surrounding circumstances.
- Whether the compromise puts any person or other data/systems/equipment at risk.
- Location of the incident.
- Inventory numbers of any equipment affected.
- Date and time the security incident occurred.
- Location of data, systems, or equipment affected.

New Lebanon CSD
Incident Reporting Template

Date: _____ Name of individual completing this form: _____

Tracking number: _____

Incident Priority

☐ HIGH	☐ MEDIUM	☐ LOW	☐ OTHER
Additional notes:			

Incident Type

Check all that apply.

☐ Compromised System ☐ Compromised User Credentials (e.g., lost password) ☐ Network Attack (e.g., DoS) ☐ Malware (e.g., virus, worm, Trojan) ☐ Reconnaissance (e.g., scanning, sniffing)	☐ Lost Equipment/Theft ☐ Physical Break-in ☐ Social Engineering (e.g., Phishing) ☐ Law Enforcement Request ☐ Policy Violation (e.g., acceptable use) ☐ Unknown/Other (Please describe below.)
Incident description notes:	

Incident Timeline

Please provide as much detail as possible.

A. Date and time when the incident was discovered	
B. Date and time when the incident was reported	
C. Date and time when the incident occurred	

Incident Scope

Please provide as much detail as possible.

A. B. Estimated quantity of systems affected	
Estimated quantity of users affected	
C. Third parties involved or affected (e.g., vendors, contractors, partners)	
Additional scoping information:	

Systems Affected by the Incident

Please provide as much detail as possible.

A.

B.

D.

Users Affected by the Incident

Please provide as much detail as possible.

A. Names and job titles of the affected users: B.	
System access levels or rights of the affected user (e.g., regular user, domain administrator, root)	
Additional user details:	

Incident Handling Log

Please provide as much detail as possible.

A

Actions taken to identify the affected resources	
B. Actions taken to remediate the incident	
C. Actions planned to prevent similar incidents	
Additional remediation details:	

Incident Reporting Information

Complete this section if incident report was system generated.

A Software package	
B. Host ID and location	
Additional system information:	

Complete this section if an incident report was submitted by an individual.

A. Full name	
B. Job title	
C. Business unit	
D. Work phone	
Mobile phone	
F. Email address	
Additional contact information:	

Incident Contact Information

A. Full name	
B. Job title	
C. Business unit	
D. Work phone	
E. Mobile phone	
F. Physical location of affected systems (e.g., state, city, building, room, desk)	

B.

A. Full name	
D. Job title	
E. Business unit	
C. Work phone	
F. Mobile phone	
Physical location of affected systems (e.g., state, city, building, room, desk)	

A.
B.

D. Full name	
E. Job title	
C. Business unit	
Work phone	
Mobile phone	
F. Physical location of affected systems (e.g., state, city, building, room, desk)	

A. Full name	
B. Job title	
E. Business unit	
C. Work phone	
F. Mobile phone	
D. Physical location of affected systems (e.g., state, city, building, room, desk)	

A.
B.

D. Full name	
E. Job title	
C. Business unit	
Work phone	
Mobile phone	
F. Physical location of affected systems (e.g., state, city, building, room, desk)	

Reporting Requirements

Board Policies 8635 and 8635-R Information Security Breach and Notification
Ed Law 2-d and NYCRR Part 121.4
What to do if you believe or have evidence that protected data has been breached or released without authorization?

1. Submit complaint in writing to the DPO (parent, teacher, staff)
2. Complaint shall be acknowledged promptly (must define what that means)
3. Investigate and notify complainant of outcome within 60 days of complaint or notify when investigation expected to be complete (communicate with complainant if cannot conclude investigation within 60 days)
4. Maintain copies of complaints and outcomes.

What does a Third-Party Contractor have to do if there is a Breach or unauthorized Breach?
Promptly notify the Data Privacy Officer, without unreasonable delay, but no more than seven calendar days after the breach's discovery.

What does the Data Privacy Officer have to do when there is a discovery or report of a breach or unauthorized release?

1. Notify the State Chief Privacy Officer of the breach or unauthorized release no more than 10 calendar days after it receives the third-party contractor's notification using a form or format prescribed by the State Education Department.
2. Report every discovery or report of a breach or unauthorized release of student, teacher or principal data to the Chief Privacy Officer without unreasonable delay, but no more than 10 calendar days after such discovery. (8 NYCRR Part 121.10(d))

What are the procedures to provide breach notification?

The District Superintendent, or designee in consultation with the Data Protection Officer, shall establish procedures to provide notification of a breach or unauthorized release of student, teacher or principal PII, and establish and communicate to parents, eligible students, and district staff a process for filing complaints about breaches or unauthorized releases of student and teacher/principal PII.

Technology/Labor Law (PII Definition different than Ed Law 2-d Definition)

Procedure for Identifying Security Breaches

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, consider:

1. indications that the information is in the physical possession and control of an unauthorized person, such as removal of lost or stolen computer, or other device containing information;
2. indications that the information has been downloaded or copied;
3. indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; and/or
4. any other factors which New Lebanon CSD shall deem appropriate and relevant to such determination.

Notification of Breaches to Affected Persons

Once it has been determined that a security breach has occurred, New Lebanon CSD will take the following steps:

1. If the breach involved computerized data *owned or licensed* by New Lebanon CSD, New Lebanon CSD will notify those New York State residents whose private information was or is reasonably believed to have been accessed or acquired by a person without valid authorization.
2. The disclosure to affected individuals will be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and to restore the integrity of the system.

3. Consult with the New York State Office of Information Technology Services to determine the scope of the breach and restoration measures.
4. If the breach involved computer data *maintained* by New Lebanon CSD, New Lebanon CSD will notify the owner or licensee of the information of the breach immediately following discovery, if the private information was or is reasonably believed to have been accessed or acquired by a person without valid authorization.
5. The required notice will include (a New Lebanon CSD contact information, (b) a description of the categories information that were or are reasonably believed to have been accessed or acquired without authorization, (c) which specific elements of personal or private information were or are reasonably believed to have been acquired and (d) the telephone number and website of relevant state and federal agencies that provide information on security breach response and identity theft protection and prevention. This notice will be directly provided to the affected individuals by either:

1. Written notice
2. Electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form; and that New Lebanon CSD keeps a log of each such electronic notification. In no case, however, will New Lebanon CSD require a person to consent to accepting such notice in electronic form as a condition of establishing a business relationship or engaging in any transaction.
3. Telephone notification provided that New Lebanon CSD keeps a log of each such telephone notification.

However, if New Lebanon CSD can demonstrate to the State Attorney General that (a) the cost of providing notice would exceed $250,000; or (b) that the number of persons to be notified exceeds 500,000; or (c) that New Lebanon CSD does not have sufficient contact information, substitute notice may be provided. Substitute notice would consist of all of the following steps:

1. E-mail notice when New Lebanon CSD has such address for the affected individual;
2. Conspicuous posting on New Lebanon CSD website, if they maintain one; and
3. Notification to major media.

However, New Lebanon CSD is not required to notify individuals if the breach was inadvertently made by individuals authorized to access the information, and New Lebanon CSD reasonably determines the breach will not result in misuse of the information, or financial or emotional harm to the affected persons. New Lebanon CSD will document its determination in writing and maintain it for at least five years and will send it to the State Attorney General within ten days of making the determination.

Additionally, if New Lebanon CSD has already notified affected persons under any other federal or state laws or regulations regarding data breaches, including the federal Health Insurance Portability and Accountability Act, the federal Health Information Technology for Economic and Clinical Health (HI TECH) Act, or New York State Education Law §2-d, it is not required to notify them again. Notification to state and other agencies is still required.

D. Notification to State Agencies and Other Entities

Once notice has been made to affected New York State residents, New Lebanon CSD shall notify the State Attorney General, the State Department of State, and the State Office of Information Technology Services as to the timing, content, and distribution of the notices and approximate number of affected persons.

If more than 5,000 New York State residents are to be notified at one time, New Lebanon CSD will also notify consumer reporting agencies as to the timing, content and distribution of the notices and the approximate number of affected individuals. A list of consumer reporting agencies will be furnished, upon request, by the Office of the State Attorney General.

If New Lebanon CSD is required to notify the U.S. Secretary of Health and Human Services of a breach of unsecured protected health information under the federal Health Insurance Portability and Accountability Act (HIPAA) or the federal Health Information Technology for Economic and Clinical Health (HI TECH) Act, it will also notify the State Attorney General within five business days of notifying the Secretary.

Communications Templates

The below document contains some sample communications templates.

Communication Templates