Cybersecurity Incident Response Plan

Prepared by: Cheektowaga-Sloan
Union Free School District

Last Modified
June 2025

PURPOSE

The Cheektowaga-Sloan UFSD is a trusted public education provider to K-12 students in Western New York. Cheektowaga-Sloan UFSD stores information related to students, staff, and internal business operations and manages and maintains technical infrastructure required to house and maintain this information. Additionally, Cheektowaga-Sloan UFSD contracts with the Western New York Regional Information Center (WNYRIC) and vendors of digital services and products to manage and maintain this data and infrastructure.

This Cybersecurity Incident Response Plan outlines Cheektowaga-Sloan UFSD's procedures to detect and respond to unauthorized access or disclosure of private information from systems utilized, housed, maintained, or serviced by Cheektowaga-Sloan UFSD. More specifically, this plan defines the roles and responsibilities of various Cheektowaga-Sloan UFSD staff with respect to the identification, isolation, and repair of data security breaches, outlines the timing, direction, and general content of communications among affected stakeholders, and defines the different documents that will be required during various steps of the incident response.

Cheektowaga-Sloan UFSD also implements practices designed to proactively reduce the risk of unauthorized access or disclosure, such as training staff with respect to legal compliance requirements, following appropriate physical security and environmental controls for technical infrastructure, and deploying digital security measures such as firewalls, malware detection, and numerous other industry-standard systems.

In the event of a cybersecurity incident, Cheektowaga-Sloan UFSD staff have been trained to deal with the matter expeditiously. Cheektowaga-Sloan UFSD staff are trained every year to recognize anomalies in the systems they regularly utilize and to report any such anomalies as soon as possible to the Incident Response Manager so the Incident Response Team can be mobilized. Throughout the year, the Incident Response Manager and members of the Incident Response Team are kept up to date on the latest security threats and trained in modern techniques of incident remediation.

The availability and protection of the information resources managed by the systems we maintain are paramount to our school district and will always be a core value of our organization.

DEFINITIONS

Cybersecurity Incident -

A Cybersecurity Incident is any event that threatens the confidentiality, integrity, or availability of the information resources we support or utilize internally, especially sensitive information whose theft or loss may harm individual students, our partners, or our organization.

Incident Response Team (IRT) -

The IRT comprises experts across different fields in the organization whose charge is to navigate the organization through a Cybersecurity Incident from the initial investigation to mitigation to post-incident review. Members include an Incident Response Manager, technical hardware and networking experts, front-end software experts, communications experts, and legal experts.

Incident Response Manager (IRM) -

The IRM oversees all aspects of the Cybersecurity Incident, especially the IRT. The key focuses of the IRM will be to ensure proper implementation of the procedures outlined in the Cybersecurity Incident Response Plan, to keep appropriate Incident Logs throughout the incident, and to act as the key liaison between IRT experts and the organization's management team. After a Cybersecurity Incident, the IRM will review the incident and produce an Incident Summary Report and a Process Improvement Plan.

Assistant Incident Response Manager (AIRM) -

The AIRM assists the IRM and oversees all aspects of the Cybersecurity Incident in the absence of the IRM.

Cybersecurity Incident Log -

The Cybersecurity Incident Log will capture critical information about a Cybersecurity Incident and the organization's response to that incident and will be maintained while the incident is in progress.

Incident Summary Report (ISR) -

The ISR is a document prepared by the IRM after a Cybersecurity Incident. It will provide a detailed summary of the incident, including how and why it may have occurred, estimated data loss, affected parties, and impacted services. Finally, it will examine the Cybersecurity Incident Response Plan procedures, including how the IRT followed the procedures and whether updates are required. The template for the ISR may be seen in Appendix A.

Process Improvement Plan (PIP) -

The PIP is a document prepared by the IRM after a Cybersecurity Incident. It will provide recommendations for avoiding or minimizing the impact of future Cybersecurity Incidents based on the "lessons learned" from the recently-completed incident. This plan should be kept confidential for security purposes. The template for the PIP may be viewed in Appendix B.

INCIDENT RESPONSE TEAM

INCIDENT RESPONSE MANAGER

Name Brian Zybala	Email bzybala@cheektowagasloan.org
Work Phone 716-897-7888	Mobile Phone

ASSISTANT INCIDENT RESPONSE MANAGER

Name Elizabeth Zaccarine	Email ezaccarine@cheektowagasloan.org
Work Phone 716-897-7800	Mobile Phone

TECHNICAL CONTACTS

Name Robert Oddo (Senior Technician)	Email
Work Phone 716-897-7800	Mobile Phone

Name James Bachert (Microcomputer Specialist)	Email
Work Phone 716-897-7800	Mobile Phone

Name Robert Rinaldi (BOCES District Tech Manager)	Email
Work Phone	Mobile Phone

LEGAL COUNSEL

Name	Email
Work Phone	Mobile Phone

COMMUNICATIONS SPECIALIST

Name (Superintendent)	Email
Work Phone 716-897-7800	Mobile Phone

ADDITIONAL MEMBERS

In addition to those individuals listed above, additional experts may be included on the IRT, depending upon the nature and scope of the incident. In particular, a software support expert from the team that supports the software in question will likely be necessary. These additional members will be chosen by the IRM.

INCIDENT MANAGEMENT PRINCIPLES

CONFIDENTIALITY

Investigation

During a Cybersecurity Incident investigation, the IRM or IRT members will gather information from multiple computer systems and/or conduct interviews with key personnel based on the scope of the incident in question. All information gathered or discovered during a Cybersecurity Incident will be strictly confidential throughout the investigative process. All Cybersecurity Incident Response Team members are trained in information security and data privacy best practices. After the investigative process, the IRM will brief District Administration on the relevant details of the incident and the investigation (see Briefing of Administration in the Response Phase on page 12). During this phase, no confidential information will be shared unless it is strictly relevant to the investigation and/or the incident.

Affected Stakeholders

In the event the incident involves the unauthorized access or disclosure of confidential student or staff information, Cheektowaga-Sloan UFSD will communicate information relevant to the incident as well as any additional requested information to which they have a right (e.g., specific student records, staff records, etc.). Cheektowaga-Sloan UFSD does reserve the right to withhold certain information at the discretion of the IRM if that information may jeopardize current or future investigations or pose a security risk to Cheektowaga-Sloan UFSD or other entities.

In the event the incident involves information about a non-Cheektowaga-Sloan UFSD district stakeholder group, such as a neighboring district or vendor partner, Cheektowaga-Sloan UFSD will take appropriate steps to notify those entities as efficiently as possible.

If the incident is limited to Cheektowaga-Sloan UFSD systems not containing sensitive or confidential information, it will be the discretion of Cheektowaga-Sloan UFSD administration and the IRM whether or not to share information related to the incident with outside stakeholders.

Report Management

All reports generated during an investigation and any evidence gathered will be stored and managed by the IRM. Any physical records will be stored in the IRM's office in a locked file. Any digital records will be stored on the internal school district network in a network share only accessible by the IRM and approved District Administrators. That share will be backed up and stored in accordance with Cheektowaga-Sloan UFSD's regular backup procedures. If records of incidents need to be reviewed, a written request must be made to the IRM that includes the requestor, the information requested, and the reason for the request. The IRM will review the request and has the discretion to approve or deny any request. Incident summary information will always be made available by the IRM.

COMMUNICATION GUIDELINES

- Communication with parents/community members, will be disseminated via the school district superintendent or designee.

- Although every incident is unique, sample communications are found in Appendices D-F in this document, and can be used as deemed appropriate by the superintendent or designee.

- Initial communication to affected stakeholders should occur as expeditiously as possible upon identifying an incident. In some cases, this may include an initial communication (letter, email, phone call) that simply states that this district is aware of the issue and is addressing it, with the promise of future communication. Scenarios for the release of Personally Identifiable Information (PII) are as follows:

    - Should the unauthorized release of student data occur, the district shall notify the parents (or eligible students) affected by the release in the most expedient way possible. Part 121 of the Commissioner's Regulations requires this notification to occur within **14 calendar days** after discovering the breach or unauthorized disclosure.

    - Should the unauthorized release of protected staff data occur, the district shall notify the staff members affected by the release in the most expedient way possible. Part 121 of the Commissioner's Regulations requires this notification to occur within **14 calendar days** after discovering the breach or unauthorized disclosure.

    - Should the unauthorized release of student and/or protected staff data occur, the district shall notify the Chief Privacy Officer (CPO) at the New York State Education Department (NYSED) within **10 calendar days**, as required by Part 121 of the Commissioner's Regulations.

    - Should the release of Social Security Number, Driver's License or Non-Driver ID Number, Account Number, or Credit/Debit Card number combined with PII occur, districts should consult Section 208 of the NYS Technology Law for notification obligations (https://its.ny.gov/sites/default/files/documents/business-data-breach-form.pdf).

- Updated communications will come from the superintendent or the Incident Response Manager. As staff members receive requests for district information, they should pass those requests along to the Incident Response Manager.

- District staff should be clearly informed by the Management Team what information is public and what is internal/confidential. However, district leadership should be aware that any material or information communicated to staff can and likely will be shared with the public, including the news media.

- The school district superintendent will initiate communication with news media if deemed appropriate. Incoming news media calls and requests for information will be directed through the Incident Response Team Communication Specialist. A communication response plan (talking points, interview refusal statement, etc.) will be formulated as needed, with information coming from the superintendent.

- Electronic Telecommunications Broadcast System (ETBS) messages, if used, should have broad language that offers basic information (1 sentence), reassurance, and refer to separate detailed communication pieces as a follow-up.

CYBERSECURITY INCIDENT PHASES

IDENTIFY

Overview

All Cheektowaga-Sloan UFSD staff are responsible for remaining vigilant and protecting the data stored within the systems we support. Any event that threatens the confidentiality, integrity, or availability of the information resources we support or utilize internally should immediately be reported to a supervisor or the IRM if a supervisor is unavailable. Supervisors should immediately bring the incident to the attention of the IRM. Parents are encouraged to notify the district of possible breaches or improper data disclosures using a form available in the Superintendent's clerk's office (see Appendix G).

Incident Types

Types of cyber incidents that may threaten the organization are:

- Unauthorized attempts to gain access to a computer, system or the data within
- Service disruption, including Denial of Service (DoS) attack
- Unauthorized access to critical infrastructure such as servers, routers, firewalls, etc.
- Virus or worm infection, spyware, or other types of malware
- Non-compliance with security or privacy protocols
- Data theft, corruption or unauthorized distribution

Incident Symptoms

Signs a computer may have been compromised include:

- Abnormal response time or non-responsiveness
- Unexplained lockouts, content or activity
- Locally hosted websites won't open or display inappropriate content or unauthorized changes
- Unexpected programs running
- Lack of disk space or memory
- Increased frequency of system crashes
- Settings changes
- Data appears missing or changed
- Unusual behavior or activity by Cheektowaga-Sloan UFSD staff, students, partners or other actors

ASSESS

Overview

Once anomalous activity has been reported, it is incumbent upon the IRM to determine the level of intervention required. Other members of the IRT may be required to provide input during this phase to help determine if an actual security threat exists. If it is determined there is an active security threat or evidence of an earlier intrusion, the IRM will alert the entire IRT immediately so that the situation may be dealt with as expeditiously as possible.

Considerations

- What are the symptoms?
- What may be the cause?
- What systems have been/are being/will be impacted?
- How widespread is it?
- Which stakeholders are affected?

Documentation

Regardless of whether it is determined there is a security threat, the IRM will accurately document the scenario in a Cybersecurity Incident Log. All Cybersecurity Incident Logs will be stored in a single location so incident information may be reviewed in the future. This report should contain information such as:

- Who reported the incident
- Characteristics of the activity
- Date and time the potential incident was detected
- Nature of the incident (Unauthorized access, DDoS, Malicious Code, No Incident Occurred, etc.)
- Potential scope of impact
- Whether the IRT is required to perform incident remediation?

RESPOND

Briefing of Administration

Upon determining that a significant incident or breach has occurred, District Administration should be notified immediately. As additional information is uncovered throughout the investigation, Administration should be briefed by the IRM, so appropriate decisions, such as allocating additional staff, hiring outside consultants, and involving law enforcement, can be made. Additionally, based on the incident, it will be incumbent on Administration to determine the appropriate stakeholders to notify of the incident and the appropriate medium to do so. The administration should consider the nature of the information or systems involved, the scope of the parties affected, timeliness, potential law enforcement interests, applicable laws, and the communication requirements of all parties involved. Sample communications documents may be found in Appendices C - F.

Initial Response

The first two steps in any cyber incident response should be to determine the origin of the incident and isolate the issue. This may involve measures up to and including immediately disconnecting particular workstations, servers, or network devices from the network to prevent additional loss. While this is occurring, it is necessary to examine firewall and system logs, as well as possibly perform vulnerability scans, to ensure the incident has not spread to other areas. These actions are necessary to define the entire scope of the incident.

Throughout this process, preserving all possible evidence and documenting all measures taken in detail will be critical. Thorough review and reporting on the incident will be required once the threat has been removed, the vulnerabilities have been reinforced, and the systems have been restored.

Remediation and Recovery**

Once the cause has been determined and appropriately isolated, the IRT must remove the vulnerabilities leading to the incident. This may involve some or all of the following:

- Install patches and updates on systems, routers, and firewalls
- Infections cleaned and removed
- Re-image or re-install operating systems of infected machines
- Change appropriate passwords
- Conduct a vulnerability scan of any compromised machines before reconnecting them to the network
- Restore system backups where possible
- Document all recovery procedures performed and submit them to the IRM
- Closely monitor the systems once reconnected to the network

REPORT

Overview

Once the threat has been mitigated and normal operation is restored, the IRM will compile all available information to produce an accurate and in-depth summary of the incident in an Incident Summary Report (ISR). A copy of the ISR is located in Appendix A. Throughout the incident, the IRT will have kept Incident Logs containing detailed records wherever possible, which shall serve as the basis of the report. Interviews will also be conducted with appropriate members of the IRT to obtain any additional information that may be available to augment the logs and records kept throughout the process. Additionally, as required by Part 121 of the Commissioner's Regulations the district will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies using the log in Appendix H.

Report Contents

The Incident Summary Report (ISR) will include all pertinent information to the incident, but at a minimum:

- Dates and times of milestones throughout the process (e.g., incident detection, verification, notifications, remediation steps, completion, etc.)
- List of symptoms or events leading to the discovery of the incident
- Scope of impact
- Mitigation and preventative measures
- Restoration logs
- Stakeholder communications (including copies of memos, emails, etc. where possible)

Timeframe

The ISR should be prepared as expeditiously as possible following the incident so future preventative measures may be taken as quickly as possible. Information to prepare the ISR and interviews with the IRT should be completed immediately to ensure the greatest possible accuracy of information.

REVIEW

Post-Incident Review Meeting

After the incident's conclusion, the IRM and possibly select members from the IRT will meet with management to discuss the event in detail, review response procedures, and construct a Process Improvement Plan (PIP) to prevent a reoccurrence of that or similar incidents. The compiled Incident Report constructed by the IRM will serve as a guide for this meeting.

In the meeting, a full debrief of the incident will be presented, and the findings will be discussed. The IRM will share the full scope of the breach (as comprehensively as possible), the causes of the breach, how it was discovered, potential vulnerabilities that still exist, communication gaps, technical and procedural recommendations, and the overall effectiveness of the response plan.

The group will review the information presented, determine any weaknesses in the process, determine appropriate actions moving forward to modify the plan, address any vulnerabilities, and determine what communication is required for various stakeholders.

Process Improvement Plan

The IRM will draft a Process Improvement Plan (PIP) based on the results of this meeting. The plan should discuss any necessary items to prevent future incidents to the extent practicable, including cost and time frame requirements where possible. The PIP will also include a review strategy to ensure all recommendations made in the PIP are met promptly and functioning appropriately. Areas of focus may include but are not limited to:

- New hardware or software required
- Patch or upgrade plans
- Training plans (Technical, end users, etc.)
- Policy or standard operating procedure recommendations
- Recommendations for changes to the Incident Response Plan
- Recommendations for changes to the Disaster Recovery Plan
- Regional communications recommendations

Additionally, the PIP must be kept strictly confidential for security purposes. Any communication required to clients or the public must be drafted separately and include only information required to prevent future incidents.

APPENDIX A:

INCIDENT SUMMARY REPORT

INCIDENT SUMMARY

Type of Incident	
Date Incident Originated	
Date Incident Was Detected	
By Whom Was Incident Detected	
How Was Incident Detected	
Scope of Incident (Districts / Systems Affected)	
Date Incident Corrected	
Corrective Action Types (Training, Technical, etc.)	

Summary of Incident Symptoms

Summary of Incident Type and Scope

Summary of Corrective Actions

Summary of Mitigation Processes and Internal Communication

Communications Log (Attach drafts for written communications, synopsis for verbal communication)

Communication Date	Communication Type	Recipient(s)	Purpose

APPENDIX B:

PROCESS IMPROVEMENT PLAN

PROCESS IMPROVEMENT PLAN

Areas of Success Summary

Areas in Need of Improvement Summary

Recommended Improvements to Avoid Future Incidents

Recommended Improvements to the Cybersecurity Incident Response Plan

Recommended Improvements to the Disaster Recovery Plan

Improvement	Timeframe	Cost

APPENDIX C:

INCIDENT LOG

INCIDENT LOG

Incident Title **Incident Opened Date**

Incident Description

Action / Event	Date/ Time	Performed / Reported by	Details

APPENDIX D:

SAMPLE PARENT LETTER

[DATE]

Dear Parents/Guardians,

This letter is to inform you of an incident that occurred within the Cheektowaga-Sloan UFSD. This incident resulted in student/staff/etc. data being compromised by an outside entity. Our Incident Response Team acted quickly to assess and mitigate the situation.

At this time, we can share the following details:
[insert a brief description of the breach or unauthorized release, the dates of the incident and the date of discovery; a description of the types of personally identifiable information affected; an estimate of the number of records affected; a brief description of the educational agency's investigation or plan to investigate]

Please know that Cheektowaga-Sloan UFSD is committed to protecting and securing educational data. Our team has extensive data security and privacy training, and our systems have many controls in place to protect your child's educational records. Our team is working with a group of experts to review the incident and implement appropriate measures to protect against this type of incident from occurring in the future.

Please contact Cheektowaga-Sloan UFSD with any questions regarding this incident and our response.

Sincerely,

APPENDIX E:

SAMPLE STAFF MEMO

[DATE]

Dear Staff,

This letter is to inform you of an incident that occurred on **[DATE]** within the Cheektowaga-Sloan UFSD's **[Name of System]** system. This incident resulted in **[student/staff/etc.]** data being compromised by an outside entity. Our response team acted quickly to assess and mitigate the situation.

I wanted to ensure that you have key details of the incident to be well informed when speaking with your students and colleagues. Please note that the Cheektowaga-Sloan UFSD administration handles communication with the community and affected parties. Should you receive any related inquiries, please direct them to Cheektowaga-Sloan UFSD**.**

At this time, we are able to share the following details:
[insert a brief description of the breach or unauthorized release, the dates of the incident and the date of discovery; a description of the types of personally identifiable information affected; an estimate of the number of records affected; a brief description of the educational agency's investigation or plan to investigate]

As more details become available we will disseminate them as appropriate. Please contact the Director of Data and Technology should you have any questions or immediate concerns regarding this incident.

Sincerely,

APPENDIX F:

SAMPLE
ETBS MESSAGE

ETBS MESSAGE

The Cheektowaga-Sloan Union Free School District experienced a technical issue today with its **[Name of System]** system that may have resulted in **[student/staff]** data being compromised. The issue is currently under investigation. More detailed information will be distributed shortly via **[email, text, phone]**.

APPENDIX G:

PARENT COMPLAINT FORM

Parents, eligible students (students who are at least 18 years of age or attending a postsecondary institution at any age), principals, teachers, and employees of an educational agency may file a complaint about a possible breach or improper disclosure of student data and/or protected teacher or principal data using this form. A privacy complaint may be made using this online form or by mailing the form to the district's Data Protection Officer at 166 Halstead Avenue, Sloan, NY, 14212.

CONTACT INFORMATION

First Name:

Last Name:

Phone Number:

Email:

Role

IMPROPER DISCLOSURE OR BREACH INFORMATION

Date Violation Occurred:

Description of Data Compromised:

Description of Improper Disclosure or Breach:

Additional Information:

APPENDIX H:

PARENT COMPLAINT LOG

PARENT COMPLAINT LOG

Complainant Name	Date Complaint submitted
Description of the Complaint	
Findings	
Date the Finding Report was Shared with Complainant	

PART 121 OF THE COMMISSIONER'S REGULATIONS REQUIREMENT

Educational agencies must maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1 (1988; rev. 2004), as set forth in section 185.12, Appendix I of this Title.

APPENDIX I:

SAMPLE PARENT COMPLAINT REPORT

DATE

Dear **[Complainant Name]**,

On **[Date]** you notified the Director of Data and Technology about a possible breach or improper disclosure of student data. Our Incident Response Team acted quickly to assess the situation, and the report below summarizes the results of our investigation.

[insert a brief description of the complaint and findings]

Cheektowaga-Sloan UFSD is committed to protecting and securing educational data. Please contact The Director of Data and Technology with any questions regarding the investigation and this report.

Sincerely,

Brian Zybala
Director of Data and Technology
bzybala@cheektowagasloan.org
716-897-7800 ext. 2124

PART 121 OF THE COMMISSIONER'S REGULATIONS REQUIREMENT

Following its investigation, the educational agency shall provide the parent or eligible student with a report of its findings within a reasonable period but no more than 30 calendar days from receipt of such complaint by the educational agency. In extenuating circumstances, where the educational agency requires additional time to investigate the complaint or cooperate with law enforcement, or where releasing the report may compromise security or impede the investigation of the incident, the educational agency shall provide the parent or eligible student with a written explanation that includes the approximate date when the educational agency anticipates that the report will be released.

This resource is relevant to the INCIDENT REPORTING AND NOTIFICATION

Part 121 of the Commissioner's Regulations Requirements.