Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

INCIDENT RESPONSE PLAN

Cybersecurity Playbook

Revision Level: 2
Publication Date: May 18, 2021

Copyright Information

Related Documents

- NIST National Institute of Standards and Technology, U.S. Department of Commerce
- New York State Education Department
- New York State Regional Information Center, RICOne Twelve Regional Information Centers

Change History

Rev #	Date	Author	Section	Nature of Change
2	January 2022	Wendy Villone	All	Updates

Table of Contents

Revision Level: 2
Publication Date: May 18, 2021

1.0 Executive Summary

This document provides the operational protocols and tactics when responding to a critical or unexpected security incident. This document will be known as the ***District Incident Response Plan,*** and it will include a general overview of preparedness. The plan will consist of record-keeping investigation and communications templates, NIST Cybersecurity Framework pre-checklists, and a current district data flowchart. Also included are team roles with district staff names and contact information and an emergency vendor call list. The ***District Incident Response Plan*** (IRS) is essential for an efficient and swift response to a cyber incident. This plan provides steps and procedures that will be activated when responding to an incident.

The goals of the plan will be to:

- To identify, outline and document the control and support of critical systems and place a high level of security that will be identified with documentation and training.
- Hold the incident response plan as a confidential document that will be sealed to only critical stakeholders involved in supporting and protecting the critical areas identified.
- To create an emergency response team prepared to act in times of crisis.
- To create a process of prevention and preparedness from district stakeholders.
- To provide a high-level approach for how the incident response capability fits into the overall organization.
- To create a process that will activate when an incident is discovered.
- To protect and document any or any further vulnerabilities from an incident.
- To protect the district's critical systems, data, and student and staff record integrity.
- To meet all guidelines of state and federal regulations.

If a school district experiences a cybersecurity incident, it is essential to observe and follow the steps below to ensure the safety of district resources and assist in protecting the component districts.

1. **Identity**: Identify the systems that are impacted.

2. **Isolate**: Take those devices that are compromised offline immediately.

3. **Communicate**: Notify all relevant stakeholders and the appropriate agencies to assist in the correct mitigation response. During the communication process, the priorities must be identified, and a timeline created that will help to make decisions as the active incident investigation continues.

    a. Notify the District Superintendent

Revision Level: 2
Publication Date: May 18, 2021

b. Notify the Director of EduTech
c. Notify the NYS Chief Privacy Officer
d. Notify the District Insurance Carrier
e. Notify the District Legal Counsel

4. **Investigate**: Investigate the impacted system to identify the primary cause of the incident with guidance from resources, such as EduTech and MS-ISAC. In ransomware or malware, there may be secondary infections not present at the time; however, the possibilities of reinfection are high because of the likelihood of undetected auxiliary infections. Identify if personally identifiable information (PII) for staff and students may have been comprised.

5. **Mitigate**: Begin the cleanup process to ensure that all traces of the infections identified are removed from the environment. This will be the most time-consuming part of the process and is critical to restoring the environment to a secure and functional status. Refresh all computers with a clean operating system and software.

6. **Recovery:** The process of restoring and returning affected systems and devices to a secure state and using tools to return systems into production and restore business as usual.

7. **Lessons Learned:** Once the investigation is completed, the ***Incident Response Team*** (IRT) should discuss and review the documentation of the process and analyze the event. The IRT is looking for security holes, vulnerabilities, and areas needed for training. The lessons learned should prevent future incidents and create a more secure district environment.

The response to a cyber incident being reported is **critical**. The purpose of the Regional Information Center's response will be used to protect all parties. In partnership with district technology staff, EduTech, and the New York State Education Department, this team will respond swiftly in containing any further damage.

1.1 Definitions

Cybersecurity Incident – A cybersecurity incident is any event that threatens the confidentiality, integrity, or availability of the information resources supported or utilized internally, especially sensitive information whose theft or loss may be harmful to individual students, our partners, or our organization.

Cybersecurity Data Breach - A cybersecurity breach means the unauthorized release, access, or disclosure of students' personally identifiable information (PII) or teacher and principal APPR by or to a person not authorized to access, use, or receive the student, teacher, or principal data.

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

Incident Response Plan is a step-by-step walk-through of high-level procedures and templates that prepare districts for a cyber incident and develop an effective action plan.

Incident Response Manager (IRM) – The Incident Response Manager has the overall responsibility and authority during the incident. To coordinator and direct all facets of the incident response efforts.

Revision Level: 2
Publication Date: May 18, 2021

Incident Response Team (IRT) – The IRT is made up of experts across different organizations 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 Summary Report (ISR) – The Incident Summary Report (ISR) is a document prepared by the IRM at the conclusion of 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 guidelines and required updates.

Isolate Thread – To prevent the spread of malware across local and regional networks, unplug the ethernet cable or turn off Wi-Fi on infected workstations.

Process Improvement Plan (PIP) – The PIP is a document prepared by the IRM at the conclusion of a Cybersecurity Incident. It will provide recommendations for avoiding or minimizing the Impact of future Cybersecurity Incidents based upon the "lessons learned" from the recently completed incident. This plan should be kept confidential for security purposes.

Report Attack – School districts must report every discovery or report of a breach or unauthorized release of a student, teacher, or principal data to the Chief Privacy Officer no more than ten calendar days after discovery.

Secure Network – To help limit the scope and progression of an attack, information systems may be taken offline or have access terminated. The network may be isolated from regional or outside communications.

2.0 Purpose

The **Wyoming Central School District** (Wyoming CSD) is a trusted public education provider to PK-8 students in **Wyoming, New York**. **Wyoming CSD** stores information related to students, staff, and internal business operations and manages and maintains the technical infrastructure required to house and maintain this information.

Additionally, **Wyoming CSD** contracts with EduTech, and vendors of digital services and products to manage and maintain this data and infrastructure.

This Incident Response Plan outlines the procedures **Wyoming CSD** uses to detect and respond to unauthorized access or disclosure of private information from systems utilized, housed, maintained, or serviced by **Wyoming CSD**. More specifically, this plan defines the roles and responsibilities of various 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.

Wyoming CSD 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

Revision Level: 2
Publication Date: May 18, 2021

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, **Wyoming CSD** staff have been trained to deal with the matter expeditiously. **Wyoming CSD** staff is trained on a yearly basis to recognize anomalies in the systems they regularly utilize and to report any such irregularities as soon as possible to the **Incident Response Manager** (IRM), so the **Incident Response Team** (IRT) can be mobilized. Throughout the year, the IRM and the IRT members 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 of paramount importance to our school district.

3.0 Roles

The **Incident Response Team (IRT)** leads, guides, manages, and controls the process of an incident. During the phases of investigation, the team works together to maintain and support the security, information, and operation of running the situation. All team members are trained in information security and data privacy best practices. The team keeps all information and processes confidential and secures the district's data and systems by enforcing the protection or containment of security issues.

3.1 Incident Response Team

- **District Personnel:**
  - Data Protection Officer
  - Superintendent
  - Incident Response Manager
  - Edutech Technology Coordinator
  - Additional DPO Team Members as needed
- **Outside Personnel:**
  - Director of EduTech
  - District Legal Counsel
  - District Insurance Carrier

Wyoming Central School District Incident Response Plan
District Superintendent: _____
Approved by The Board of Education: _____ **Date:** _____ **Version:** _____

4.0 Public Summary Concluded

Revision Level: 2
Publication Date: May 18, 2021

(Optional statement to conclude public version of Incident Response Plan)

PUBLIC SUMMARY CONCLUDED

5.0 Confidential District Documents

Revision Level: 2
Publication Date: May 18, 2021