Cyber Incident Response Plan

1. Goals and objectives

This document outlines the procedures for identifying, responding to, and recovering from Cyber incidents. The goal is to minimize the impact on business operations and ensure a swift return to normalcy.

2. Incident Response Team (IRT)

Superintendent: [Hunter Nolen]

Responsibilities: Approval of Incident Response Plan, and Administer Communications Plan

Deputy Superintendent [Becky Hart]

Responsibilities: Works in absence of Superintendent

MIS Director: [Jennifer See]

Responsibilities: Liaison between IT and Superintendent's office; Formalize communications plan, report to and gain approval from superintendent's office for Incident Response Plan

IT Supervisor: [Kelly Lanier]

Responsibilities: Reports to MIS Director; Activation and Administration of Incident Response Plan; Administration of Incident Identification, Incident Response Steps, Draft Communications Plan for MIS Director formalization; Document Incident; Review and Update Incident Response Team

Network Analyst: [Ethan Smith]

Responsibilities: Report any Incident Identification to IT Supervisor, Begin Incident Response Steps, and Documentation, as necessary

Low Voltage and Electronics Technician: [Aaron Hamilton]

Responsibilities: Report any Incident Identification to IT Supervisor, Begin Incident Response Steps, and Documentation, as necessary

Tech Coordinator: [Rusty Simpson]

Responsibilities: Report any Incident Identification to IT Supervisor, Begin Incident Response Steps, Communicate with school technicians as needed, Documentation as necessary

3. Incident Identification

Detection: Monitor systems for unusual activity using IDS/IPS, SIEM tools, and user reports.

Classification: Categorize incidents (malware, data breach, DDoS attack) based on severity and impact.

4. Incident Response Steps

A. Preparation

Ensure all team members are trained and aware of their roles.

Maintain up-to-date contact lists and incident response tools.

B. Identification

Verify the incident through logs, alerts, and user reports.

Document the nature and scope of the incident.

C. Containment

Short-term: Isolate affected systems to prevent further damage.

Long-term: Implement temporary fixes to allow continued operation while addressing the root cause.

D. Eradication

Identify and remove the cause of the incident (malware removal, patching vulnerabilities).

Verify that the threat has been eliminated.

E. Recovery

Restore affected systems and data from backups.

Monitor systems for any signs of residual issues.

F. Lessons Learned

Conduct a post-incident review to analyze the response and identify areas for improvement.

Update the incident response plan based on findings.

5. Communication Plan

Internal: Notify relevant stakeholders (board, admin, faculty, staff, students) about the incident and response actions.

External: Communicate with consortium, parents, vendors, and regulatory and authoritative bodies as necessary.

6. Documentation

Complete the **Cyber Incident Response Form**

Maintain detailed records of the incident, response actions, and recovery efforts.

Ensure all evidence and documentation is stored securely and accessible to the IRT.

7. Review and Update

Regularly review and update the incident response plan to reflect new threats, technologies, and organizational changes.

Conduct periodic drills and simulations to test the effectiveness of the plan. Administrative roundtable discussions to walk through the process will be considered an accurate test of the plan.