Incident Response Plan

Cybersecurity Incident Response Plan

[School Name]

Version: 1.0 **Effective Date:** [Date] **Last Updated:** [Date] **Plan Owner:** [Title]

CRITICAL: Print and Store Offline

Print multiple copies of this document and store in secure physical locations. During a cyberattack, your digital systems may be inaccessible.

---

1. Incident Response Team

1.1 Core Team Members

Role	Primary Contact	Backup Contact
Incident Commander (Head of School or designee)	Name:	Name:
	Phone:	Phone:
	Email:	Email:
IT Lead	Name:	Name:
	Phone:	Phone:
	Email:	Email:
Communications Lead	Name:	Name:
	Phone:	Phone:
	Email:	Email:
Legal/Compliance	Name:	Name:
	Phone:	Phone:
	Email:	Email:
Operations Lead	Name:	Name:

Role	Primary Contact	Backup Contact
	Phone: Email:	Phone: Email:

1.2 External Contacts

Resource	Contact Information
Cyber Insurance Carrier	Company: Policy #: Claims Phone: 24/7 Hotline:
Legal Counsel	Firm: Contact: Phone:
IT Security Vendor	Company: Contact: Phone:
FBI Local Office	Phone:
Local Police Cyber Unit	Phone:

---

2. Incident Classification

Level 1 - Low Severity

- Single device malware (contained)
- Phishing attempt (no credentials compromised)
- Minor policy violation
- **Response Time:** Within 24 hours
- **Notification:** IT Lead only

Level 2 - Medium Severity

- Multiple systems affected
- Potential data exposure (unconfirmed)
- Successful phishing (credentials compromised)
- Extended system outage (>4 hours)
- **Response Time:** Within 4 hours
- **Notification:** Incident Commander + IT Lead

Level 3 - High Severity (CRITICAL)

- Confirmed ransomware

- Confirmed data breach
- Student/staff PII exposed
- Systems encrypted or destroyed
- Regulatory notification required
- **Response Time:** IMMEDIATE
- **Notification:** Full Response Team + Insurance + Legal

---

3. Response Procedures

Phase 1: Detection & Initial Response (0-1 hours)

Whoever discovers the incident:

□ Do NOT turn off affected systems (preserves evidence)

□ Do NOT attempt to "fix" the problem yourself

□ Document what you observed (time, symptoms, affected systems)

□ Immediately contact IT Lead: [Phone]

□ If IT Lead unavailable, contact: [Backup Phone]

IT Lead actions:

□ Assess severity and classify incident (Level 1/2/3)

□ For Level 2-3: Notify Incident Commander immediately

□ Document initial findings in Incident Log

□ Begin evidence preservation

Phase 2: Containment (1-4 hours)

Goal: Stop the spread without destroying evidence

□ Isolate affected systems from network (unplug ethernet, disable WiFi)

□ Disable compromised accounts

□ Block malicious IPs/domains at firewall

□ Preserve system logs before they rotate

□ Take screenshots/photos of ransom notes or unusual activity

□ Do NOT pay any ransom without legal/insurance consultation

□ Document all actions taken with timestamps

For Level 3 incidents:

□ Contact cyber insurance carrier immediately

□ Contact legal counsel

□ Prepare for potential school closure or remote operations

□ Activate communication plan

Phase 3: Eradication (4-48 hours)

Goal: Remove the threat

□ Identify root cause of incident

□ Remove malware from all affected systems

□ Reset all potentially compromised credentials

□ Patch vulnerabilities that enabled the attack

□ Verify backups are clean before restoration

□ Document all remediation steps

Phase 4: Recovery (24-72+ hours)

Goal: Restore normal operations safely

□ Restore systems from verified clean backups

□ Rebuild systems that cannot be cleaned

□ Test systems before returning to production

□ Monitor for signs of persistent threat

□

Gradually restore network access

□ Verify data integrity

Phase 5: Post-Incident (Within 2 weeks)

□ Complete incident documentation

□ Conduct lessons learned meeting

□ Update security controls

□ File insurance claim (if applicable)

□ Complete regulatory notifications (see Section 5)

□ Update this plan based on lessons learned

---

4. Communication Templates

4.1 Initial Staff Notification

Subject: Technology Systems Alert - Action Required

We are currently experiencing a technology issue that is affecting [describe impact].

What you should do: - Do not attempt to access [affected systems] - Report any unusual activity to IT immediately at [phone] - Continue teaching using offline methods

We will provide updates as more information becomes available.

[Signature]

4.2 Parent Notification (Level 3 - Data Breach)

Subject: Important Security Notice from [School Name]

Dear [School Name] Families,

We are writing to inform you of a cybersecurity incident that occurred on [date]. We take the security of your family's information seriously and want to provide you with details about what happened and what we are doing in response.

What Happened: [Brief, factual description]

What Information Was Involved: [Specific types of data - be precise]

What We Are Doing: [Actions taken and planned]

What You Can Do: [Specific protective steps]

For More Information: [Contact information, FAQ link]

We sincerely apologize for any concern this may cause. We are committed to protecting your information and will continue to enhance our security measures.

[Signature - Head of School]

4.3 Board Notification

Subject: Cybersecurity Incident Report - [Date]

This memo provides an update on a cybersecurity incident affecting [School Name].

Incident Summary: - Classification: Level [1/2/3] - Discovery Date: [Date/Time] - Current Status: [Contained/Under Investigation/Resolved]

Impact Assessment: - Systems Affected: - Data Potentially Exposed: - Operational Impact:

Response Actions: [Summary of actions taken]

Next Steps: [Planned actions]

Financial Impact: [Known or estimated costs, insurance coverage]

A full briefing is available upon request.

4.4 Media Statement (if needed)

[School Name] recently experienced a cybersecurity incident. We immediately activated our incident response plan and are working with cybersecurity experts to investigate and remediate the situation.

The security of our students' and families' information is our top priority. We are cooperating with law enforcement and will notify affected individuals in accordance with applicable laws.

We are not able to share additional details at this time as the investigation is ongoing.

---

5. Regulatory Notification Requirements

FERPA

- Notify U.S. Department of Education if federal funds are involved

- Document breach in records

State Law (Missouri)

- Notify affected individuals “without unreasonable delay”
- Notify Attorney General if >500 residents affected

HIPAA (if applicable)

- 60-day notification window
- HHS notification required

Consult legal counsel before sending any breach notifications.

---

6. Scenario-Specific Checklists

Ransomware Attack

□ Do NOT pay ransom without insurance/legal approval

□ Isolate ALL systems immediately

□ Contact insurance carrier first

□ Assess backup integrity

□ Report to FBI IC3 (ic3.gov)

□ Prepare for extended recovery (days to weeks)

Email Account Compromise

□ Reset password immediately

□ Revoke all active sessions

□ Review sent items for malicious emails

□ Check for forwarding rules

□ Review connected applications

□ Notify recipients of any malicious emails sent

Data Breach/Exfiltration

- □ Identify what data was accessed
- □ Determine notification obligations
- □ Preserve all logs
- □ Engage forensics if scope unclear
- □ Prepare breach notification

---

7. Plan Maintenance

Annual Review

- □ Update all contact information
- □ Review and update procedures
- □ Conduct tabletop exercise
- □ Train new staff on procedures

Review Date: ____________

Approved By: ____________

Appendix: Incident Log Template

Date/Time	Action Taken	Person	Notes

This template is provided by AISL (AI for St. Louis Schools). Customize for your school and review with legal counsel. Test annually through tabletop exercises.