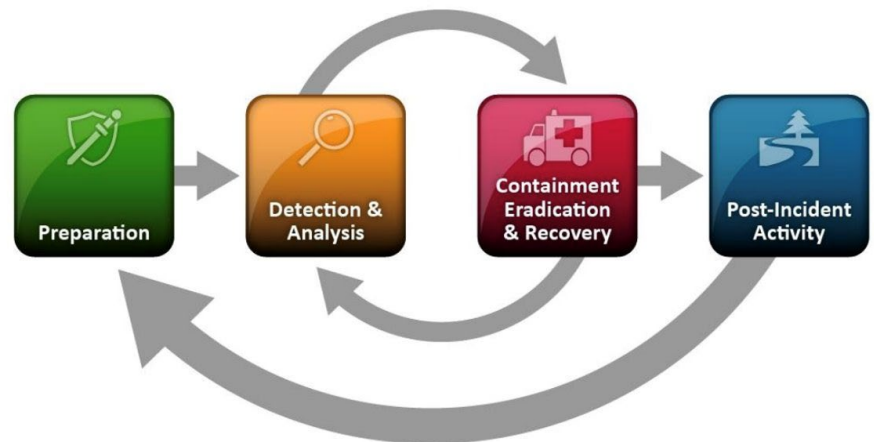


K12 SIX ESSENTIAL CYBER INCIDENT RESPONSE RUNBOOK (v 1.1)

Experiencing a cybersecurity incident involving the disruption of school operations, fraud, or a potential data breach is stressful. The actions you take in the hours and days following discovery of the incident are critical to your ability to recover and key to maintaining the trust of your school community. This resource—developed by the K12 Security Information eXchange ([K12 SIX](#)) and its members—is intended to assist leadership in U.S. K-12 school districts and other K-12 organizations in preparing to respond to a cyber incident. It is a complement to the [K12 SIX Essential Protections](#), which identifies the baseline cybersecurity controls that all school systems can and should implement to defend their school communities from emerging cybersecurity threats.

The *K12 SIX Essential Cyber Incident Response Runbook* is aligned to the [NIST Incident Response Life Cycle](#), which identifies the major phases of the incident response process—preparation, detection and analysis, containment, eradication and recovery, and post-incident activity.



This resource is designed to be customized, marked up, printed, and redistributed. You may not be able to rely on your IT resources during an incident! Your adapted copy of the *K12 SIX Essential Cyber Incident Response Runbook* should be practiced regularly via tabletop exercises and updated periodically as circumstances change. When your K-12 organization is ready, it can serve as the basis for a full cyber incident response plan, ideally integrated into other organizational emergency operations and disaster recovery plans.

Even in cases where your organization will rely on the services of an external provider for most incident response services, understanding the myriad issues that may arise during a cyber incident will increase your operational resilience and speed up time to recovery.

The K12 SIX Essential Cyber Incident Response Runbook is organized by the four inter-related stages of cybersecurity incident response:

- **1.0 Preparation** – establishing policy and the gathering of information, tools, and resources
- **2.0 Detection and Analysis** – determining the scope and impact of a potential cyber incident to prioritize response and recovery efforts, including stakeholder communications

- **3.0 Containment, Eradication, and Recovery** – based on the information gathered during the prior stage, thoroughly eradicating malware/vulnerabilities and restoring normal operations
- **4.0 Post-Incident Activity** – documenting and sharing lessons learned from incident response to resolve deficiencies and strengthen the security posture of your organization, as well as those of peer institutions

Appendices include:

- Emergency contacts and key resources worksheet
- Guidance for cyber incidents involving students
- Sample post-incident learning and improvement questions
- Sample responsibility assignment matrix
- References and resources

Responding to a Live Incident?

- ✓ Stay calm
- ✓ Do follow your incident response plan
- ✓ Preserve your organization’s ability to investigate and recover by isolating, not prematurely powering off affected systems
- ✓ Do ask for assistance: in most cases, your actions should be dictated by incident response experts

Follow these initial steps:

- Review and/or assign incident response team roles (Section 1.2)
- Follow recommended initial steps upon discovering a potential incident (Section 2.3)
- Gather and document evidence (Section 2.4)
- Notify stakeholders, as appropriate (Section 2.5)



Change History Log:

Version Number	Release Date
1.0	June 22, 2022
1.1	April 4, 2024

Disclaimer: K12 SIX makes no representations or warranties with respect to the accuracy or completeness of the content herein and specifically disclaims any implied warranties of merchantability or fitness for a particular purpose. The advice contained herein may not be suitable for your situation. K12 SIX shall not be liable for any loss or damages, including but not limited to special, incidental, consequential or other damages.

1.0 PREPARATION – involving establishing policy and the gathering of information, tools, and resources.

1.1 Define a Cyber Incident	<p>How does your organization define a cyber incident?</p> <hr/> <hr/> <hr/> <p>For instance, a cyber incident can be defined as anything that violates or poses a threat to a K-12 organization and/or is a violation of its policies and procedures. Examples of K-12 incidents include:</p> <ul style="list-style-type: none"> • Misuse of district technology resources by staff, students, or third parties (Policy violations) • High volumes of connection requests to public facing servers that degrade performance or cause outages (DDoS - Distributed Denial of Service Attack) • A user opens an email and clicks on an attachment or link, leading to the installation of malware or network connections to an external system (Phishing) • An attacker exploits an unpatched server vulnerability to gain access to sensitive data and exfiltrate it before encrypting school IT systems (Ransomware)
1.2 Define Cyber Incident Response (IR) Team Roles	<p>Who is a part of our Cyber Incident Response (IR) Team and what do they do during an incident? NOTE: Roles may vary depending on district size and cybersecurity maturity.</p> <ul style="list-style-type: none"> • IR Team Leader: _____ Responsible for overall leadership and management of the IR Team. Responsible for declaring an incident and for invoking incident response plans. Assigns the IR Team Lead Investigator and identifies resources needed during all stages of incident response. • IR Team Administrator: _____ Responsible for ensuring all stages of incident response are thoroughly documented and serves as the point of contact for legal counsel, insurance representatives, communications/PR, and other internal stakeholders about the incident and response. Also, handles logistical needs necessitated by the response (e.g., meals, command center, lodging). • First Responder: <u>_____(NOTE: **Most** IT staff should be trained in this role)_____</u> First person to identify/recognize the incident. Assesses the situation and whether the incident is reportable. Preserves evidence. Contacts IR Team Leader and serves as IR Team Lead Investigator until IR Team Leader formally assigns role. Serves as ad hoc Team Leader until designated person can be notified. • IR Team Lead Investigator: _____ Named by the Team Leader. Responsible for coordinating comprehensive response activities (network/hardware/software), including most technical aspects of the incident. <i>NOTE: Role may be filled by external technical experts skilled in detection and response.</i> • Communications/PR: _____ In consultation with legal counsel, responsible for ALL inbound/outbound communications with media and other external stakeholders.

1.3 Identify Contacts and Key Resources	<p>Complete, print, and share this document, including Appendix A (“Emergency Contacts and Key Resources Worksheet”).</p> <p>Incident response is a team sport. Make sure you have identified all important stakeholders and know how to reach them, including via alternate channels in case internal systems are compromised or offline. Print and share the completed template found in Appendix A.</p> <p style="text-align: center;">  Do not proceed before completing Appendix A.  </p>
1.4 Assemble Existing Plans and Tools	<p>What relevant formal policies, plans, and procedures does your organization already have in place?</p> <p>Locate and review documents and ensure up-to-date printed copies are available offline. These may include:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Business Continuity Plan & Continuity of Operations Plan (COOP) <input type="checkbox"/> IT network, asset, contingency and emergency plans <input type="checkbox"/> Crisis/Emergency Management Plan <input type="checkbox"/> Communications Plan <input type="checkbox"/> Disaster Recovery Plan <input type="checkbox"/> Training or Phishing Mitigation Plan <input type="checkbox"/> Risk Management Plan <input type="checkbox"/> Cybersecurity Insurance Documentation <input type="checkbox"/> Other: _____
1.5 Prepare for Stakeholder Communications	<p>Prompt, clear, and consistent communication is vital in any crisis. Don’t leave it to chance.</p> <p>Prepare your communications/PR team (internal and/or external) and HR department for cyber incident communications, including via tabletop exercises. Be sure to consider:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Advising staff to not share unauthorized incident-related communications/posts on social media <input type="checkbox"/> Need for legal consultation before any (internal or external) communication <input type="checkbox"/> Pre-writing and vetting sample notifications to staff, families, and the media for common K-12 cyber incident types <input type="checkbox"/> Alternative/out of band communications if locked out of normal communications systems or internet becomes unavailable (e.g., email, website, social media) <input type="checkbox"/> The need for regular updates to stakeholders during the process of incident response and recovery <input type="checkbox"/> Tactics to address and manage reputation/brand concerns, if any

2.0 DETECTION AND ANALYSIS – Determining the potential scope and impact of a cyber incident to prioritize response and recovery efforts, including stakeholder communications.

2.1 Prepare for Common K-12 Incidents

Understand common K-12 cyber incident vectors and prepare for them. These may include:

- Brute force attacks
- Compromised/stolen credentials, including for student accounts
- Insider actions (students, staff, administration)
- Internet-exposed services
- Malware/ransomware
- Misconfiguration
- Network stressers/DDoS stressers
- Phishing/business email compromise
- Remote access/work
- Unpatched/end-of-support servers and systems
- Vendor/partner/third-party compromise

2.2 Monitor for Potential Incidents

Understand the possible sources and precursors of potential cyber incidents. These may include:

- Alerts/advisories from trusted sources (e.g., K12 SIX, MS-ISAC, CISA, FBI, vendors)
- Antivirus events
- Evidence of reconnaissance or discovery activities
- Failed logins or unusual login locations (e.g., IP ranges or impossible travel)
- Firewall alarms and mismatched traffic
- Significant increase in bandwidth usage or database activity
- Large numbers of opened/copied files
- New administrative users created, or users added to admin groups
- Reports from end users
- Unexpected deletion or modification of files
- Unexpected increase in log files
- Unexpected new objects or services (user or computer)
- Unexpected patching of systems
- Unusual files or processes, or stopped services
- Website defacement

<p>2.3 Initial Steps Upon Discovering a Potential Incident</p>	<p>Train IT staff on the steps to declare a potential cyber incident and invoke the IR Team. These steps may include:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Creating/opening a helpdesk ticket (more information is better) <ul style="list-style-type: none"> ○ What time/date did this occur? ○ Did the end user click a hyperlink or open an email? ○ Did the end user open a file attachment, such as a PDF? ○ Did the end user visit a suspicious website? ○ Did the end user download software or browser extensions recently? ○ Did the end user plug in a flash drive? ○ Are any locally stored, suspicious file extensions identified? ○ Has the end user been denied access to data or a server? ○ Does the incident affect only one or many users? <input type="checkbox"/> Making special note of potential Indicators of Ransomware (IOR) or Indicators of Compromise (IOC) such as: extortion demand/ransom notes; encrypted files; known malicious files, file hashes, ports or protocols, destination domains or IPs <input type="checkbox"/> Alerting members of the IT team responsible for security, including the IR Team Leader, who can formally declare an incident. <input type="checkbox"/> Logging/recording every action taken—including what was done, when, on which systems, by whom, and for what reasons. This will assist with later phases of incident response. <input type="checkbox"/> Alerting executive leadership* of the incident and status <input type="checkbox"/> Contacting legal counsel* and—as directed and appropriate—communications/PR team, HR, risk management, cyber insurance broker/provider, law enforcement, related vendor(s)/external partners, and others <p><i>*Be aware that attackers may have access to organizational email, messaging, and helpdesk systems. Use out-of-band communication methods/ face-to-face meetings, as appropriate.</i></p>
<p>2.4 Gather and Document Evidence</p>	<p>Gather and document evidence to assist with incident response and fulfill legal obligations. <u>Be careful not to destroy evidence or impede further investigation.</u> Consider:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Increasing log retention/snapshot duration for length of investigation <input type="checkbox"/> Collecting and archiving applicable logs, including from before the event (e.g., from IDS, SIEM, antivirus, event/system logs, content/DNS filters) <input type="checkbox"/> Taking an image/snapshot of affected systems for later forensic review <input type="checkbox"/> Reviewing firewall events in firewall logs. <input type="checkbox"/> Reviewing intrusion detection and prevention events in Microsoft 365 Defender or similar tool <input type="checkbox"/> Capturing network activity (e.g., bandwidth, open ports, DNS, packet captures) <input type="checkbox"/> Recalling offsite backups, as appropriate, for potential future restoration activities <input type="checkbox"/> Updating the incident helpdesk ticket with any new information about what you have learned and what mitigations have been taken (regarding which servers,

which domains, which clients, which user accounts, which files, which alert IDs, etc.)

- ❑ Assessing and documenting what you know for executive leadership, communications/PR team, legal counsel, and external IR consultants (if any) including:
 - Indicators of compromise (include what/when/how)
 - Attack artifacts (e.g., screenshots, scripts/code, instructions, configuration changes, email rules)
 - Attacker's goal (e.g., exfiltrating, destroying, changing, or encrypting data; disabling or disrupting systems; theft of funds; repurposing of IT resources; reconnaissance/spying, etc.)
 - Scope of attack (e.g., number of systems/users affected, types of data involved, impact on operations, estimated time to recover, etc.)
 - Estimated time to recover affected systems and overall

Pause to evaluate what you know and what you do not. Your incident may involve multiple points of entry and multiple attack methods. Should the incident involve a student, see Appendix A for further considerations and guidance.

<p>2.5 Notify Stakeholders</p>	<p>In compliance with your legal obligations and incident type/operational impact, implement your plan to notify staff, stakeholders, and other affected parties.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Seek legal guidance before initiating communications <input type="checkbox"/> Prepare to address common questions: <ul style="list-style-type: none"> ○ Who attacked you/caused the incident? Why? ○ When and how did it happen? ○ How widespread is the attack? ○ Was any PII or sensitive information exposed, including social security numbers or other financial data? ○ What steps are you taking to remediate the incident and prevent future occurrences? <input type="checkbox"/> Identify audiences that require notification (e.g., employees, management, school staff, parents/guardians) <input type="checkbox"/> Identify the type of notifications needed (e.g., an initial response, a status message, or a resolution message) <input type="checkbox"/> Consider employing pre-drafted templates that best fit the type of notification and audience in need of communication <input type="checkbox"/> Use the communication channel(s) that best fit the audience in need of notification (e.g., public website announcement, social media, email, phone, in-person, etc.) <input type="checkbox"/> Do not overstate the certainty of evolving situations (e.g., caveat with statements such as ‘at this time,’ ‘so far as we know,’ etc.). “We don’t know yet” is a legitimate response. Some questions may best be answered by law enforcement. <input type="checkbox"/> Be consistent and regular in messaging. Consider daily updates for evolving situations. <input type="checkbox"/> Engage with media, as appropriate, and monitor social media. Information voids often lead to unfounded speculation and loss of trust. <input type="checkbox"/> Remember to log and maintain all communications even on personal devices. Seek legal guidance for records retention requirements.
---------------------------------------	--

3.0 CONTAINMENT, ERADICATION, AND RECOVERY – based on the information gathered during the prior stage, thoroughly eradicating malware/vulnerabilities and restoring normal operations

3.1 Contain the Incident

Block compromised systems from communicating with other devices or with attackers.
Caution should be taken before taking steps to contain the incident. For instance:

- Incident responders/law enforcement may wish to monitor an attacker or gather additional evidence before beginning containment activities.
- Once containment and eradication efforts begin, attackers may change tactics, targets, or intensity of malicious activity. Continue to monitor systems closely and be prepared to move quickly in response.

While containment strategies vary by incident type the goal is to block compromised systems from communicating with other devices or with the attackers. Powering off systems prematurely may delete in-memory evidence of compromise. Consider:

- Blocking SSO/Cloud access
- Blocking Internet/network access
- Disabling compromised accounts (revoking tokens and deleting active connections)
- Disabling services, especially any that are being targeted
- Removing accounts from privileged groups (domain admins, etc.)
- Working with HR for advice if an employee has violated policy

Containment tools, which may be at your disposal, include:

- Endpoint configuration management tools (via Intune/SCCM and/or via AppLocker, JAMF, Google Chrome Device Management, etc.)
- EDR/Antivirus global controls
- Host-based firewall controls
- Switch ports, uplinks, and network segments (which can be disabled)
- Network firewall (for both inbound and outbound traffic)
- Content/DNS web filters
- VPNs and remote access services (which can be disabled)

3.2 Eradicate the Threat	<p>After ensuring evidence is preserved for legal and insurance purposes, eliminate all traces of the incident. This may entail:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Correcting any misconfigurations identified <input type="checkbox"/> Patching or upgrading all affected systems to fix exploited vulnerabilities <input type="checkbox"/> Removing any unauthorized accounts <input type="checkbox"/> Resetting passwords for compromised accounts <ul style="list-style-type: none"> ○ Revoking and reissuing security certificates, MFA tokens, SSO/OAUTH/SAML connections to resources ○ NOTE: If a domain administrator/root/SA-level account has been compromised, all account passwords may need to be reset or the account directory may need to be rebuilt <input type="checkbox"/> Reimaging systems affected with malware <p>Caution: To preserve evidence and ensure unwanted programs/backdoors do not cause recurring issues, some devices may need to be (physically) replaced, rather than remediated.</p>
3.3 Recover and Restore IT Operations	<p>Based on priorities and estimated recovery timelines, repair, restore, rebuild, or replace systems taken offline or otherwise affected by the incident.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Reference existing disaster recovery plans, if any, for prioritization <input type="checkbox"/> Replace/restore/reimage systems: <ul style="list-style-type: none"> ○ Verify backups have not been tampered with ○ Roll back to known good system state (but monitor for indications of compromise/latent malware) ○ Use known good OS sources and application installers ○ Apply known good firmware to address (some) rootkit infections <input type="checkbox"/> Discontinue, block, and retire vulnerable or unsupported technologies (e.g., SMB v.1, SSL 3.0, Windows XP/7, macOS 10.14 or earlier, unsigned PowerShell scripts, default community strings for SNMP, etc.) <input type="checkbox"/> Implement controls to prevent recurrence (e.g., MFA, geolocation controls, privileged/secure access workstations, updates to user training, etc.) <input type="checkbox"/> Consider creating an isolated network or a new cloud computing instance to protect recovered systems from re-compromise <input type="checkbox"/> Reset, restore, or recreate potentially compromised accounts and systems <input type="checkbox"/> Validate restored systems work as expected
3.4 Monitor for Anomalous Activity	<p>It is critical to maintain vigilance even after IT operations have been restored post-incident. Consider:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Instituting more robust system logging and network monitoring <input type="checkbox"/> Elevated monitoring of systems and network activity for anomalous activity, remote access, new/changed privileged accounts, or other signs of intrusion

3.5 Update Stakeholders on Recovery Status	Providing regular, high-quality communications about incident recovery helps maintain trust in the organization and executive leadership. <ul style="list-style-type: none"><li data-bbox="440 289 1474 394">❑ Be aware of regulatory requirements for mandatory reporting of incidents like data breaches, which may require quick-turnaround notifications, including any local, state, or federal reporting requirements.
---	---

4.0 POST-INCIDENT ACTIVITY – documenting and sharing lessons learned from incident response to resolve deficiencies and strengthen the security posture of your organization, as well as those of peer institutions	
4.1 Conduct Post-Incident Review	<p>The work of the IR team is not complete until a comprehensive assessment is prepared and shared with appropriate parties. (See Appendix B for sample learning and improvement questions.)</p> <ul style="list-style-type: none"> <input type="checkbox"/> Identify and resolve any deficiencies and root causes in your current cybersecurity risk management program (i.e., technologies, policies, and practices) that led to the incident <input type="checkbox"/> Identify and resolve deficiencies in planning and execution of your incident response <input type="checkbox"/> Assess whether additional cybersecurity risk management measures—technologies, policies, and/or practices—are needed to prevent a recurrence of the issue and strengthen the security posture of your organization <input type="checkbox"/> Ensure the incident is sufficiently documented to meet public records, law enforcement, and/or insurance requirements
4.2 Brief Executive Leadership	<p>As appropriate, prepare a final report to executive leadership on the incident and response.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Describe the root cause of the incident (non-technical) <input type="checkbox"/> Summarize the actions taken to respond and recover from the incident (non-technical) <input type="checkbox"/> Describe any remaining issues <input type="checkbox"/> Summarize actual recovery expenses incurred (such as labor, fees, consultants/contractors, equipment purchases, etc.) <input type="checkbox"/> Summarize recommended cybersecurity risk management program short-, medium-, and long-term-improvements, including estimated costs
4.3 Implement Changes	<p>Ensure that lessons learned from experiencing an incident are enacted and shared with other K-12 organizations.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Implement recommended measures to strengthen the security posture of your organization <input type="checkbox"/> Update relevant incident response plans and documents <input type="checkbox"/> Share lessons learned and recommended mitigations with other K-12 community members, including by securely reporting the incident to K12 SIX

APPENDICES

- Appendix A: Emergency Contacts and Key Resources Worksheet
- Appendix B: Guidance for Incidents Involving Students
- Appendix C: Sample Post-Incident Learning and Improvement Questions
- Appendix D: Sample Roles and Responsibilities Matrix
- Appendix E: References and Resources

APPENDIX A: EMERGENCY CONTACTS AND KEY RESOURCES

WORKSHEET

NOTE: Your organization may not have individuals in each of these roles. Be sure to include alternate contact information in case your internal communications or email systems are offline or compromised. Print and share this worksheet once completed and plan to review and update at least annually.

Date last updated: _____

TITLE/ROLE	CONTACT INFORMATION	TITLE/ROLE	CONTACT INFORMATION
<INTERNAL/EXTERNAL>	<NAME> <WORK PHONE> <ALT PHONE> <WORK EMAIL> <ALTERNATE EMAIL>	<INTERNAL/EXTERNAL>	<NAME> <WORK PHONE> <ALT PHONE> <WORK EMAIL> <ALTERNATE EMAIL>
CISO/InfoSec Lead – Internal		MSSP/SOC Provider – External	
IT Leader – Internal		General IT/MSP Provider – External	
General Counsel/Legal – Internal		Breach Counsel/Legal – External	
Superintendent/Head of School – Internal		Cyber Insurance Broker/Provider – External	Policy #: _____
Chief Financial Officer – Internal		Fusion Center/Local Law Enforcement – External	
Operations – Internal		FBI and/or CISA Representative – External	
Communications/PR – internal		Communications/PR – external	

TITLE/ROLE	CONTACT INFORMATION	TITLE/ROLE	CONTACT INFORMATION
<INTERNAL/EXTERNAL>	<NAME> <WORK PHONE> <ALT PHONE> <WORK EMAIL> <ALTERNATE EMAIL>	<INTERNAL/EXTERNAL>	<NAME> <WORK PHONE> <ALT PHONE> <WORK EMAIL> <ALTERNATE EMAIL>
Human Resources – internal		Incident Response Consultant(s) – external	
Nutrition/Food Services – internal		Financial Institution(s) – external	Acct #: _____
Payroll/Accounting – internal		Payment/Credit Card Processor – external	Acct #: _____
Physical security – internal		ISP – external	Acct #: _____
Chief Privacy Officer/Privacy lead – internal		Financial IT System(s) provider – external	
Transportation – internal		Human Resources IT System(s) provider – external	
Incident Response Team Leader – internal		Learning Management IT System(s) provider – external	
Incident Response Team Investigator – internal		Student Information IT System(s) provider – external	
Incident Response Team Administrator – internal		Cloud Productivity Application Suite provider – external	

TITLE/ROLE	CONTACT INFORMATION	TITLE/ROLE	CONTACT INFORMATION
<INTERNAL/EXTERNAL>	<NAME> <WORK PHONE> <ALT PHONE> <WORK EMAIL> <ALTERNATE EMAIL>	<INTERNAL/EXTERNAL>	<NAME> <WORK PHONE> <ALT PHONE> <WORK EMAIL> <ALTERNATE EMAIL>
State Cyber Incident Response Team/ National Guard – external		Library Services/ Other Critical Vendors – external	
State (and Other Mandatory) Data Breach Notification Agency – external		Other – internal/external	
Other Information to Record for Quick Reference			
Special URLs and resources (e.g., URLs for critical logs and resources, cybersecurity tools, shortcut locations, etc.)			
Out-of-band communication (email replacement)	<i>E.g., Slack, Discord, or similar</i>		
Out-of-band communication (voice replacement)	<i>E.g., freeconferencecall.com, ringcentral.com, or similar; cell phone tree; etc.</i>		
Email aliases (groups, network, helpdesk, etc.)			

APPENDIX B: GUIDANCE FOR INCIDENTS INVOLVING STUDENTS

Preparation: Student-Initiated Incident

- Isolate student networks from high-risk systems where possible
- Ensure all students understand and sign a network use agreement that explicitly calls out bad behaviors and consequences
- Inform district and building administrators of the type of risks posed by potential malicious student cyber activity and establish a severity scale to guide disciplinary actions (incident scope and impact should drive discipline)
- Determine level of police involvement, if any, if student-initiated incidents. Establish a relationship with local police department(s) to identify correct contacts, as well as protocols regarding whom from the district will make contact
- Educate faculty and staff on classroom behavioral “look-fors” that may indicate malicious activity (e.g. hiding of screen, quick changes between applications, etc.)

Post-Incident Activity (Short-/Mid-Term): Student-Initiated Incident

- Work with district official(s) responsible for special education services to determine if the student(s) involved have an Individualized Education Plan (IEP) or other special education accommodations. These factors impact the course of disciplinary and legal actions.
- Include building principals or designee in all conversations related to incident scope
- Follow your established discipline process, as appropriate, usually starting with a warning. A second offense might result in more limited internet access and a discussion with the parents. A third offense could result in more serious consequences
- Working in conjunction with building principal or designee, include parent/guardian in scope discussion(s), as well as conversations related to disciplinary action. Establishing a good rapport with parent(s)/guardian(s) early on can help lead to a better outcome for the school and student.

Post-Incident Activity (Long Term): Student-Initiated Incident

- Document the incident carefully, as it could be used in legal suits later
- Consider redirection of the student to more productive targets such as ‘Hack The Box,’ capture the flag (CTF) contests, or recruitment into a school-sponsored tech support program
- If the student’s device can’t record *all* activity (including, e.g., scripts run, etc.) consider adding an XDR or similar monitoring agent on student’s device moving forward

APPENDIX C: SAMPLE POST-INCIDENT LEARNING AND IMPROVEMENT QUESTIONS

Learning and improvement questions

- How well did the staff and management perform?
- Were documented policies and procedures followed?
- Were the procedures adequate?
- Was the actual cause identified?
- What information was needed sooner?
- Were any steps taken that might have inhibited recovery?
- What should/would staff/management do differently the next time a similar incident happens?
- How could information sharing (in/out) with other organizations have been improved?
- What corrective actions can prevent or lower the likelihood of similar incidents in the future?
- What precursors or indicators of compromise should be watched in the future to speed up detection?
- What additional tools and/or resources are needed to address future incidents?
- What tools, processes, metrics, or resources could be in place and/or monitored to detect a similar incident sooner?

Root cause analysis questions

- Exactly what happened, and at what times?
- How effectively was the incident identified and logged (including precursors)?
- Were there any leading-edge indicators of detection that were missed?
- Did the incident cause damage before it was detected?
- Was the actual cause identified?
- Was the incident a recurrence of a previous incident?
- What could have prevented the incident?
- Do logs, forms, reports, and other incident documentation reflect adherence to established incident response policies and procedures?
- Was there a difference between the initial impact assessment and the final impact assessment?
- What was the estimated monetary damage from the incident (e.g., information and critical business processes negatively affected by the incident, IT staff resource re-allocation, new equipment/services purchased, incident response/recovery consultant fees, etc.)?

APPENDIX D: SAMPLE RESPONSIBILITY ASSIGNMENT MATRIX

Developing a responsibility assignment matrix (also known as a 'RACI' matrix) can be a useful way of delineating roles and responsibilities for cyber incident response management. It arrays four key roles across job functions/individuals in or working for your organization:

Roles	Definition	Number of individuals/ roles to assign
[R]esponsible	Those accountable for the successful completion of the task	At least 1 per task
[A]ccountable	Responsible for assigning and signing off on completion of the task	Only 1 per task
[C]onsulted	Those whose input should be sought	No limits
[I]nformed	Those who should be provided updates on issues and progress	No limits

Since the roles in this sample matrix may vary from those in your organization (depending mostly—but not entirely—on school/district size and cybersecurity maturity) be sure to re-create and customize a version suitable for your purposes. It can also be valuable to adapt it even further by taking the recommended major tasks in the *K12 SIX Essential Cybersecurity Incident Response Runbook* (e.g., 2.3, 2.4, etc.) and breaking them down into multiple, distinct activities specific to your IT context. See the following page for an example.

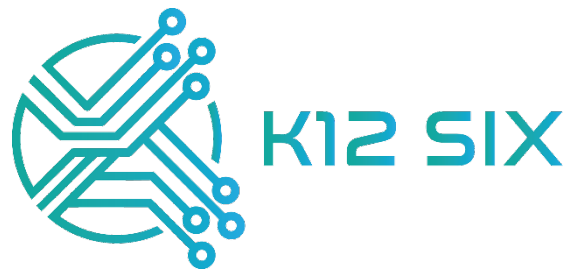
Task/activity	External Cyber Expert(s)/ Lead Investigator	Help Desk/ Technician	IR Team Leader / Administrator	CTO/CIO/ Tech Director	HR	Comms/PR	Legal	Leadership
1.0 Preparation								
1.1 Define a Cyber Incident	-	I	I	R	C	I	C	A
1.2 Define Cyber Incident Response (IR) Team Roles	-	I	R	A	I	I	I	I
1.3 Identify Contacts and Key Resources	-	C	R	A	C	C	C	-
1.4 Assemble Existing Plans and Tools	-	C	R	R	C	-	C	A
1.5 Prepare for Stakeholder Communications	-	-	-	C	C	A	C	I
2.0 Detection and Analysis								
2.1 Prepare for Common K-12 Incidents	-	R	R	A	-	-	-	I
2.2 Monitor for Potential Incidents	-	R	R	A	-	-	-	I
2.3 Initial Steps Upon Discovering a Potential Incident	I	R	R	A	I	I	I	I
2.4 Gather and Document Evidence	R	R	R	A	I	I	I	I
2.5 Notify Stakeholders	C	I	I	C	C	R	R	A
3.0 Containment, Eradication, and Recovery								
3.1 Contain the Incident	R	R	R	A	I	I	I	I
3.2 Eradicate the Threat	R	R	R	A	I	I	I	I
3.3 Restore and Recover IT operations	C	R	R	A	I	I	I	I
3.4 Monitor for Anomalous Activity	C	R	R	A	-	-	-	-
3.5 Update Stakeholders on Recovery Status	C	I	I	C	C	R	R	A
4.0 Post-Incident Activity								
4.1 Conduct Post-Incident Review	C	R	R	A	C	C	C	-
4.2 Brief Executive Leadership	-	C	C	R	I	I	I	A
4.3 Implement Changes	-	R	R	R	I	I	I	A

APPENDIX E: REFERENCES AND RESOURCES

- K12 Security Information eXchange: <https://www.k12six.org/>
 - K12 SIX Essential Cybersecurity Protections: <https://www.k12six.org/essentials-series>
 - Membership Portal Login: <https://k12six.cyware.com/webapp/auth/login>
- U.S. Department of Commerce, National Institute of Standards and Technology (NIST)
 - Computer Security Incident Handling Guide (800-61):
<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>
 - Guide for Cybersecurity Event Recovery (800-184):
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf>
- U.S. Department of Education Privacy Technical Assistance Center (PTAC)
 - Data Breach Response Checklist:
https://studentprivacy.ed.gov/sites/default/files/resource_document/file/checklist_data_breach_response_092012_0.pdf
 - Data Breach Scenario Trainings: <https://studentprivacy.ed.gov/resources/data-breach-scenario-trainings>
 - Security Best Practices: <https://studentprivacy.ed.gov/topic/security-best-practices>
- U.S. Department of Homeland Security, Cybersecurity & Infrastructure Security Agency (CISA)
 - CISA Tabletop Exercise Package Documents: <https://www.cisa.gov/resources-tools/resources/ctep-package-documents>
 - K-12 Schools CISA Tabletop Exercise Package Situation Manual:
<https://www.cisa.gov/sites/default/files/2023-09/k-12-schools-ctep-situation-manual-ncep-092023-508.docx>
 - Ransomware Response Checklist: <https://www.cisa.gov/stopransomware/ive-been-hit-ransomware>
- Cyber Security Agency of Singapore Incident Response Checklist: <https://www.csa.gov.sg/Tips-Resource/Resources/singcert/incident-response-checklist>
- Microsoft
 - Incident Response Reference Guide: <http://aka.ms/IRGuide>
 - Security Best Practices Incident Response Overview: <https://docs.microsoft.com/en-us/security/compass/incident-response-overview>
 - Security Best Practices Incident Response Playbooks: <https://docs.microsoft.com/en-us/security/compass/incident-response-playbooks>
- Black Hills Information Security Backdoors & Breaches, an Incident Response Card Game: <https://www.blackhillsinfosec.com/projects/backdoorsandbreaches/>
- SecurityStudio K12 Incident Response Management Plan Template: <https://securitystudio.com/policy-templates/k12-irp/>

About the K12 Security Information eXchange

The K12 Security Information eXchange (K12 SIX) is a cyber threat information sharing hub for K-12 organizations—including school districts, charter schools, private schools, and regional and state education agencies—to aid in preventing and mitigating attacks. This non-profit member community is a cost-effective forum for crowdsourcing security information among a vetted, trusted group of professionals with a common interest, using common technology and with supporting, independent analysis from the K12 SIX security staff and the Global Resilience Federation multisector network of information sharing communities. Visit www.K12SIX.org to learn more.



The development of version 1.0 of the *K12 SIX Essential Cyber Incident Response Runbook* was made possible with the support of Microsoft.