



Association of Technology Leaders
in Independent Schools 

K12 SIX

Essential Cyber Incident Response Runbook



Independent School Adaptation

September 2026

MEMBER PREVIEW



About This Preview

This preview shows the full structure of the **K12 SIX Essential Cyber Incident Response Runbook: Independent School Adaptation**, so your school can see everything the complete resource includes. ATLIS members have access to the full, printable runbook.

Open to everyone in this preview

- Introduction, independent school operating model considerations, and runbook structure
- **0.0 First 60 Minutes:** STOP/START actions and the three response tiers
- **1.0 Preparation:** incident definitions, response team roles, contacts, plans, communications, and vendor readiness
- **Appendix A:** Emergency Contacts and Key Resources Worksheet

Available to ATLIS members

- **2.0 through 4.0:** detection and analysis, containment and recovery, and post-incident activity
- **Appendices B–F:** student incidents, post-incident questions, responsibility matrix, scenario playbooks, and communication templates
- **Appendices G and H:** vendor and third-party checklist and the in-depth vendor incident response guide, including a contact worksheet and vendor RACI matrix
- **Appendices I and J:** plain-language glossary and references

Unlock the full runbook

ATLIS members can download the complete runbook at www.theatlis.org. Not a member yet? Learn about ATLIS membership for your school at www.theatlis.org.

Contents

Independent School Operating Model Considerations 3

Runbook Structure 3

0.0 First 60 Minutes: Responding to a Live Incident 4

1.0 Preparation 5

2.0 Detection and Analysis 7

3.0 Containment, Eradication, and Recovery 9

4.0 Post-Incident Activity 10

Appendix A: Emergency Contacts and Key Resources Worksheet 11

Appendix B: Guidance for Incidents Involving Students 12

Appendix C: Sample Post-Incident Learning and Improvement Questions 13

Appendix D: Optional Responsibility Assignment Matrix 14

Appendix E: Quick Scenario Playbooks 15

Appendix F: Communication Matrix and Message Guidance 16

Appendix G: Vendor and Third-Party Incident Response Checklist 17

Appendix H: Vendor and Third-Party Incident Response Guide 19

Appendix I: Plain-Language Glossary 26

Appendix J: References and Resources 27

About K12 SIX 27

About ATLIS 27

Thank You to Our Volunteers 28

Change History Log

Version	Release Date	Notes
1.0	June 22, 2022	Original K12 SIX release
1.1	April 4, 2024	K12 SIX update
ATLIS 1.0	September 2026	Independent school adaptation incorporating peer-review feedback and an in-depth vendor and third-party incident response appendix (Appendix H)

Disclaimer: This resource provides general guidance only. Cyber incidents may create legal, regulatory, contractual, insurance, employment, student-safety, and communications obligations that vary by situation and jurisdiction. Seek advice from qualified legal counsel, your cyber insurance provider, and incident-response professionals as appropriate.

K12 SIX Essential Cyber Incident Response Runbook

Independent School Adaptation | September 2026

Experiencing a cybersecurity incident involving disrupted school operations, fraud, or a potential data breach is stressful. The actions taken in the first hours and days after discovery are critical to recovery and to maintaining the trust of the school community. This adaptation is intended to help U.S. K-12 independent schools prepare for and respond to cyber incidents while accounting for the realities of small technology teams, cloud-first systems, outsourced technology support, Head of School governance, and close relationships with families.

This resource is based on the K12 Security Information eXchange (K12 SIX) Essential Cyber Incident Response Runbook and is designed to be customized, marked up, printed, and redistributed within a school. Keep an offline copy. During an incident, normal email, collaboration tools, identity systems, or other IT resources may be unavailable.

How to use this runbook

Complete the preparation worksheets before an incident, identify outside partners, practice the runbook through tabletop exercises, and keep printed copies accessible. During a live incident, begin with the First 60 Minutes page and follow the response tier that best matches the situation.

Independent School Operating Model Considerations

- One person may hold several incident-response roles. Smaller schools should assign responsibilities by function rather than assume a large internal team.
- Cyber insurance carriers, breach counsel, managed service providers (MSPs), managed security service providers (MSSPs), and external incident-response firms may direct or perform much of the response. Know in advance whom to call and what your policy requires.
- Many independent schools are cloud-first. Incident response must account for Google Workspace or Microsoft 365, SIS, LMS, admissions, tuition/payment, HR/payroll, advancement, and other SaaS platforms.
- Schools may have limited internal forensic capability. Preserve evidence and contain harm, then rely on qualified external responders for advanced forensic work when needed.
- Head of School and senior leadership decisions, board visibility, family communications, and reputational considerations may become significant early in the response.

Runbook Structure

- **0.0 First 60 Minutes:** immediate actions for a live incident
- **1.0 Preparation:** policy, roles, contacts, tools, vendors, and communications
- **2.0 Detection and Analysis:** identify the incident, determine scope, preserve evidence, and notify the right people
- **3.0 Containment, Eradication, and Recovery:** limit damage, remove the threat, and restore operations
- **4.0 Post-Incident Activity:** learn, document, report, and improve

Appendices provide emergency contacts, student-specific guidance, post-incident questions, an optional responsibility matrix, scenario playbooks, communication guidance, a vendor/SaaS response checklist, an in-depth vendor and third-party incident response guide, a glossary, and references.

0.0 First 60 Minutes: Responding to a Live Incident

Primary objective

Protect people and school operations, stop further harm when safe to do so, preserve evidence, and quickly engage the partners who are expected to direct the response.

STOP

- ✗ Do not delete suspicious emails, logs, files, alerts, or cloud audit records.
- ✗ Do not wipe, reimage, or prematurely power off affected systems unless directed by an incident-response expert. Powering off can destroy volatile evidence.
- ✗ Do not communicate incident details broadly through systems that may be compromised.
- ✗ Do not make public statements or notify affected individuals before coordinating with leadership and legal counsel, unless immediate safety or legal obligations require action.

START

1. Record the date and time the incident was discovered and who discovered it.
2. Contact the Incident Lead and Technical Response Lead.
3. If required by your policy, notify the cyber insurance carrier, broker, breach coach, or approved incident-response provider immediately.
4. Use out-of-band communications if school email, messaging, or identity systems may be compromised.
5. Isolate affected accounts, devices, integrations, or network segments when safe and consistent with responder guidance.
6. Preserve logs, screenshots, alerts, vendor case numbers, and other evidence.
7. Brief the Head of School or designated executive decision maker with known facts, operational impact, and immediate decisions needed.
8. Open an incident log and record every material action, decision, person contacted, and time.

Choose a Response Tier

Tier	Typical Examples	Who Leads	Immediate Escalation
Tier 1: Limited	Phishing attempt; isolated malware alert; single account compromise with no evidence of sensitive-data access	Internal IT/technology lead	Escalate if scope expands, privileged access is involved, or sensitive data may be affected
Tier 2: Significant	Multiple accounts; compromised admin account; material SaaS outage or breach; suspected business email compromise; student/staff insider incident with broader impact	Technology lead with MSP/MSSP and executive leadership	Notify insurer/breach counsel when policy or facts warrant; consider board leadership based on severity
Tier 3: Major/Critical	Ransomware; widespread outage; confirmed or likely data exfiltration; payment fraud; major vendor breach; destructive attack; significant safety, legal, financial, or reputational impact	External IR/breach counsel/insurer in coordination with school leadership	Engage approved external responders immediately and activate crisis communications/business continuity plans

When uncertain, escalate.

Early involvement from cyber insurance, breach counsel, an MSP/MSSP, or an incident-response firm can prevent actions that complicate coverage, legal privilege, evidence preservation, or recovery.

1.0 Preparation

Preparation establishes the people, decision rights, contacts, vendor information, tools, and offline resources needed before an incident occurs.

1.1 Define a Cyber Incident

A cyber incident is an event that violates or threatens the confidentiality, integrity, or availability of school systems, data, accounts, services, or technology-related operations, or that violates school policies and procedures.

- Misuse of school technology resources by staff, students, contractors, or third parties
- Credential compromise or account takeover
- Phishing, business email compromise, or payment redirection fraud
- Malware or ransomware
- Distributed denial-of-service (DDoS) or other service disruption
- Unauthorized access to school data or systems
- Vendor, SaaS, or third-party breach
- Cloud identity or integration compromise, including malicious OAuth or third-party app access
- Misconfiguration that exposes data or systems
- AI-enabled impersonation, deepfake, or social-engineering incident

1.2 Define Incident Response Team Roles

Assign functions, not job titles. In a smaller school, one person may hold multiple roles. Identify an alternate for each critical function and document external partners who will fill roles the school does not have internally.

Function	Typical Independent School Assignment	Core Responsibility
Incident Lead	Technology leader, COO, or other designated leader	Declares the incident, activates the runbook, coordinates the response, assigns leads, and maintains overall situational awareness.
Technical Response	Internal IT staff, MSP/MSSP, or external IR provider	Investigates, contains, eradicates, restores, and preserves technical evidence. External specialists may perform advanced forensic work.
Executive Decision Maker	Head of School or designated senior leader	Approves major operational decisions, determines leadership/board escalation, and supports high-priority stakeholder communication.
Documentation & Coordination	Technology or operations staff member	Maintains the incident log, tracks decisions and contacts, coordinates meetings, and preserves response records.
Communications Lead	Communications, advancement, Head's office, or designee	Coordinates messages to families, employees, students, board members, donors/alumni, media, and partners.
External Advisors	Breach counsel, cyber insurer/breach coach, broker, MSP/MSSP, IR firm, relevant vendors	Provide legal, insurance, forensic, technical, contractual, and notification guidance.

Function	Typical Independent School Assignment	Core Responsibility
Finance & Fraud Response	CFO/business office	Coordinates insurer and banking/payment-provider contacts, financial controls, fraud response, and expense tracking.
Student/HR Response	Division leadership, Dean of Students, HR, or designee	Handles student or employee conduct, safety, discipline, accommodations, and related communications.

1.3 Identify Contacts and Key Resources

Complete Appendix A, print it, and store it securely offline. Include alternate phone numbers and alternate email addresses in case school communications are unavailable. Test the contact list at least annually and after major staffing or vendor changes.

1.4 Assemble Existing Plans and Tools

- Business Continuity / Continuity of Operations Plan
- Disaster Recovery Plan and backup procedures
- Crisis or Emergency Management Plan
- Communications and media plan
- Cyber insurance policy, claim instructions, approved vendors, and breach-coach contacts
- Network, identity, asset, configuration, and data maps
- Vendor contracts, breach-notification terms, backup responsibilities, service-level agreements, escalation paths, and rights to obtain logs or audit information
- Critical SaaS inventory, integrations, SSO/OAuth connections, and procedures to disable compromised integrations
- Student acceptable/responsible use and discipline policies
- HR, records retention, privacy, and data breach procedures

1.5 Prepare for Stakeholder Communications

- Pre-draft messages for common scenarios and audiences. See Appendix F.
- Define who approves communications and who serves as spokesperson.
- Plan alternate communication channels if email, website, identity systems, or messaging platforms are unavailable.
- Coordinate communication timing with legal counsel and executive leadership.
- Tell employees not to post or share unauthorized incident information.
- Plan for regular updates during prolonged incidents, even when there is little new information to report.
- Tailor detail to the audience. Parents and students usually need clear practical guidance; board members need operational, financial, legal, and reputational implications; technical responders need detailed indicators and system information.

1.6 Prepare Vendor and SaaS Response Information

- Identify the security or incident-response contact for each critical vendor.
- Document which party is responsible for breach detection, notification, remediation, backups, log retention, and restoration.
- Record contractual notification timelines, cyber insurance requirements, and any rights to audit or obtain security information.
- Map major data flows and integrations so compromised connections can be disabled without unnecessary disruption.
- Know how to revoke SSO, OAuth, API keys, service accounts, or other integrations for critical platforms.

- Confirm whether critical vendors can restore from clean backups and what evidence they will provide before service is considered safe to resume.

Appendices G and H provide a vendor response checklist and in-depth guidance for vendor-originated incidents.

2.0 Detection and Analysis

2.1 Prepare for Common Independent School Incidents



ATLIS Members Only

Log in or join at www.theatlis.org to unlock the full runbook

2.2 Monitor for Potential Incidents

2.3 Initial Steps Upon Discovering a Potential Incident



ATLIS Members Only

Log in or join at www.theatlis.org to unlock the full runbook

2.4 Gather and Document Evidence

2.5 Assess Scope and Impact

2.6 Notify Stakeholders

3.0 Containment, Eradication, and Recovery

3.1 Contain the Incident

3.2 Eradicate the Threat

3.3 Recover and Restore School Operations



ATLIS Members Only

Log in or join at www.theatlis.org to unlock the full runbook

3.4 Monitor for Anomalous Activity

3.5 Update Stakeholders on Recovery Status

4.0 Post-Incident Activity

4.1 Conduct a Post-Incident Review

4.2 Brief Executive Leadership and the Board



ATLIS Members Only

Log in or join at www.theatlis.org to unlock the full runbook

4.3 Implement Changes

Appendix A: Emergency Contacts and Key Resources Worksheet

Include alternate contact information in case school email or communications are unavailable. Print and securely store this worksheet. Review at least annually.

Date last updated: _____

Title / Role	Contact Information	Title / Role	Contact Information
Incident Lead (Internal)	<NAME> <WORK PHONE> <ALT PHONE> <WORK EMAIL> <ALT EMAIL>	MSP / MSSP / SOC Provider (External)	<NAME> <PHONE> <EMAIL> <CASE / PORTAL INFO>
Technology Leader (Internal)	<NAME> <WORK PHONE> <ALT PHONE> <WORK EMAIL> <ALT EMAIL>	Incident Response Firm (External)	<NAME> <PHONE> <EMAIL> <ENGAGEMENT INFO>
Head of School / Executive Lead	<NAME> <WORK PHONE> <ALT PHONE> <WORK EMAIL> <ALT EMAIL>	Cyber Insurance / Broker / Breach Coach	Policy #: _____ <NAME> <PHONE> <EMAIL>
CFO / Business Office	<NAME> <PHONE> <EMAIL>	Breach / General Counsel (External)	<NAME> <PHONE> <EMAIL>
Communications Lead	<NAME> <PHONE> <EMAIL>	Board Chair / Board Leadership	<NAME> <PHONE> <EMAIL>
HR / Employee Relations	<NAME> <PHONE> <EMAIL>	Student Life / Division Leadership	<NAME> <PHONE> <EMAIL>
Operations / Physical Security	<NAME> <PHONE> <EMAIL>	Law Enforcement / Fusion Center	<NAME> <PHONE> <EMAIL>
Financial Institution(s)	Acct #: _____ <NAME> <PHONE> <EMAIL>	Payment Processor	Acct #: _____ <NAME> <PHONE> <EMAIL>
SIS Vendor	<NAME> <SECURITY PHONE> <SECURITY EMAIL>	LMS Vendor	<NAME> <SECURITY PHONE> <SECURITY EMAIL>
Google Workspace / Microsoft 365	<ADMIN / SECURITY CONTACT> <SUPPORT CASE INFO>	Admissions / Enrollment Vendor	<NAME> <SECURITY PHONE> <SECURITY EMAIL>
HR / Payroll Vendor	<NAME> <SECURITY PHONE> <SECURITY EMAIL>	Advancement / Donor System	<NAME> <SECURITY PHONE> <SECURITY EMAIL>
ISP / Network Provider	Acct #: _____ <NAME> <PHONE> <EMAIL>	Other Critical Vendor	<NAME> <PHONE> <EMAIL>

Other Information to Record for Quick Reference

Category	Information
Out-of-band email/messaging	
Out-of-band voice / conference bridge	
Incident log location	
Cyber insurance claim portal / instructions	
Critical security dashboards / URLs	
Offline password vault / emergency access procedure	
School status page / emergency website process	

Appendix B: Guidance for Incidents Involving Students

Preparation

During the Incident

After the Incident



ATLIS Members Only

Log in or join at www.theatlis.org to unlock the full runbook

Appendix C: Sample Post-Incident Learning and Improvement Questions



ATLIS Members Only

Log in or join at www.theatlis.org to unlock the full runbook

Appendix D: Optional Responsibility Assignment Matrix



ATLIS Members Only

Log in or join at www.theatlis.org to unlock the full runbook

Appendix E: Quick Scenario Playbooks

Compromised Google Workspace or Microsoft 365 Account

Phishing / Business Email Compromise / Payment Redirection

Ransomware or Widespread Malware

Vendor / SaaS Breach or Critical Vendor Outage

Student-Initiated or Insider Incident

AI-Enabled Impersonation / Deepfake Social Engineering

Appendix F: Communication Matrix and Message Guidance



ATLIS Members Only

Log in or join at www.theatlis.org to unlock the full runbook

Message Template: Initial Holding Statement

Message Template: Internal Staff Instructions

Message Template: Recovery Update

Appendix G: Vendor and Third-Party Incident Response Checklist

Before an Incident



ATLIS Members Only

Log in or join at www.theatlis.org to unlock the full runbook

When a Vendor Reports an Incident



**ATLIS Members Only**
Log in or join at www.theatlis.org to unlock the full runbook

Appendix H: Vendor and Third-Party Incident Response Guide

Contributed by Kevin J. Warenda, MBA, CISM, TLIS, Director of Information Technology Services, The Hotchkiss School

Introduction



ATLIS Members Only

Log in or join at www.theatlis.org to unlock the full runbook

H.1 Preparation: Vendor Risk and Readiness

H.1.1 Maintain a Vendor Inventory

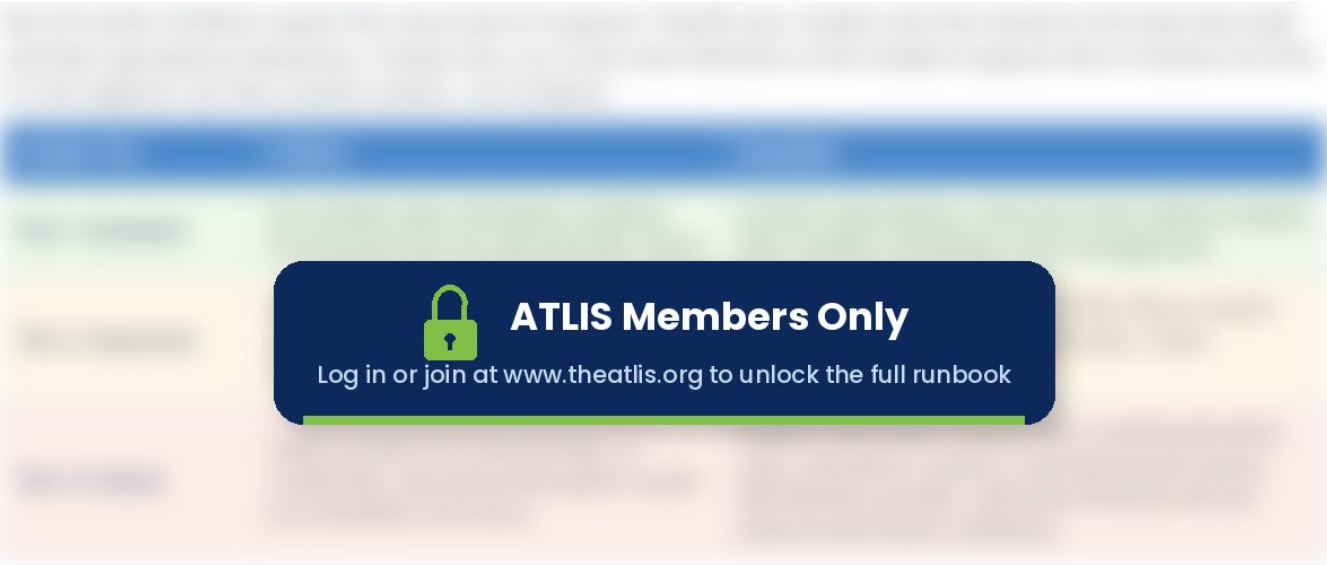
H.1.2 Review Vendor Contracts for IR Provisions



H.1.3 Establish Vendor Communication Channels



H.1.4 Classify Vendors by Criticality



ATLIS Members Only

Log in or join at www.theatlis.org to unlock the full runbook

H.2 Detection and Analysis: Identifying a Vendor Incident

H.2.1 How You May Learn of a Vendor Incident



ATLIS Members Only

Log in or join at www.theatlis.org to unlock the full runbook

H.2.2 Initial Assessment Questions

H.2.3 Assess Impact on School Operations

H.3 Containment, Eradication, and Recovery

H.3.1 Immediate Containment Actions



ATLIS Members Only

Log in or join at www.theatlis.org to unlock the full runbook

H.3.2 Coordinate with the Vendor

H.3.3 Reconnection Criteria

H.4 Post-Incident Activity

H.4.1 Internal Lessons Learned

H.4.2 Vendor Relationship Review

H.4.3 Communicate Findings Appropriately



ATLIS Members Only

Log in or join at www.theatlis.org to unlock the full runbook

 ATLIS Members Only
Log in or join at www.theatlis.org to unlock the full runbook



Log in or join at www.theatlis.org to unlock the full runbook

H.6 Sample Vendor Incident RACI Matrix

Sample Vendor Incident RACI Matrix									
	Incident Response Plan	Incident Response Team	Incident Response Process	Incident Response Tools	Incident Response Training	Incident Response Awareness	Incident Response Communication	Incident Response Documentation	Incident Response Review
Incident Response Plan	R	A	A	A	A	A	A	A	A
Incident Response Team	A	R	A	A	A	A	A	A	A
Incident Response Process	A	A	R	A	A	A	A	A	A
Incident Response Tools	A	A	A	R	A	A	A	A	A
Incident Response Training	A	A	A	A	R	A	A	A	A
Incident Response Awareness	A	A	A	A	A	R	A	A	A
Incident Response Communication	A	A	A	A	A	A	R	A	A
Incident Response Documentation	A	A	A	A	A	A	A	R	A
Incident Response Review	A	A	A	A	A	A	A	A	R



ATLIS Members Only

Log in or join at www.theatlis.org to unlock the full runbook

Appendix I: Plain-Language Glossary



ATLIS Members Only

Log in or join at www.theatlis.org to unlock the full runbook

Appendix J: References and Resources



ATLIS Members Only

Log in or join at www.theatlis.org to unlock the full runbook

About K12 SIX

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. Its member community supports the prevention and mitigation of cyber threats through trusted information sharing and security resources.

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

Learn more at <https://www.k12six.org/>

About ATLIS

The Association of Technology Leaders in Independent Schools (ATLIS) is dedicated to empowering independent schools to thrive through technology leadership. Founded in 2014 to address the unique challenges of independent school technology leaders, ATLIS now supports the full range of technology practice in schools through professional learning, community, resources, and leadership development. ATLIS helps schools strengthen their technology strategy, cybersecurity, operations, teaching and learning, data practices, and institutional resilience while preparing for what comes next.

Learn more at www.theatlis.org

Thank You to Our Volunteers

ATLIS extends its sincere thanks to the independent school technology professionals who reviewed this adaptation and contributed their expertise, practical experience, and thoughtful recommendations. Their feedback helped make this resource more actionable and better aligned with the realities of independent school technology leadership.

Special thanks to Kevin J. Warenda, MBA, CISM, TLIS, of The Hotchkiss School for authoring Appendix H: Vendor and Third-Party Incident Response Guide.

Name	Title	School / Organization
Amit Chopra	Head of Information Systems & Digital Security	Lakefield College School
Louis Fierro	IT Director	Collegiate School
Mario Fishery	IT Director	American School of Bombay
Bill Freitas	Retired	Formerly Lawrenceville, Webb, and St. Andrews
Jennifer Lamkins	Coordinator of Member and Technology Support Services	NWAIS
Louis Tullo, TLIS	Chief Information and Innovation Officer	Ravenscroft School
Kevin J. Warenda, MBA, CISM, TLIS	Director of Information Technology Services	The Hotchkiss School
Ally Wenzel, TLIS	Former Director of Technology	Formerly Stevenson School

Unlock the Full Runbook

The complete runbook gives your leadership team everything it needs to move from preparation to a coordinated response: detection and analysis, containment and recovery, post-incident review, scenario playbooks, communication templates, a responsibility matrix, and an in-depth vendor and third-party incident response guide.

ATLIS members

Download the full, printable runbook at www.theatlis.org.

Not yet a member?

Learn how ATLIS membership supports your school's technology leadership, cybersecurity, and institutional resilience at www.theatlis.org.