

Incident Recovery Plan Execution

This category asks whether your district can actually rebuild after a cyber incident: restore identity, the network, the SIS, and payroll from clean backups, in a deliberate order, fast enough to keep school open.

Why it matters

- When ransomware encrypts servers and there is no agreed restore order, staff rebuild whatever someone is shouting about, and identity, the network and the student information system (SIS) come back out of sequence or not at all. Schools may close or run on paper for days or weeks, and every attendance mark, meal count and grade recorded on paper has to be re-entered later.
- Payroll, vendor payments, meal service and state reporting do not pause for an incident. A tested plan with a payroll workaround agreed with the bank or payroll processor, and printed bus routes and meal procedures, is what keeps staff paid and buildings open while a full-time equivalent (FTE) count or other state reporting window is approaching.
- Backups that have never been restored are a hope, not a plan. Dated restore tests measured against a recovery time objective (RTO) and recovery point objective (RPO) give the superintendent a real answer for the board, show the cyber insurance carrier the evidence it asks for, and make it possible to recover without even considering a ransom payment.

The stakes are concrete — districts hit by ransomware without tested recovery have lost days or weeks of instruction, scrambled to make payroll, and missed state attendance and reporting deadlines. A documented, tested recovery capability is also something cyber-insurance underwriters and incident responders ask to see.

What good looks like at each level

Level	What you would see	Artifacts that show it
1 · Initial	<p>Recovery depends on what the technology director remembers. Backups may run, but no one has written down what gets restored first, who decides, or how school keeps running while systems are down.</p> <p>Moving up: Write the plan down: restoration procedures for each critical system, clearly defined roles and responsibilities, and step-by-step actions for during and after an incident. Moving from nothing (or a plan disconnected from your goals) to a documented runbook is the whole jump.</p>	<ul style="list-style-type: none"> • No written restore order or recovery time targets; if a plan exists, it is a generic template that does not name district systems, people or priorities • Backups stored on a network share or a server joined to the same domain, with no offline or immutable copy and no record of a test restore • No paper procedures for attendance, meal service, bus routes or payroll if systems are unavailable
2 · Repeatable	<p>A written recovery plan exists with restoration steps for each critical system and named people for each step. It covers what to do during and after an incident, but it has not yet been proven with timed restores or exercised with leadership.</p> <p>Moving up: Extend the plan to asset protection and the direct and indirect processes that keep school operating, then keep dated evidence — test-restore logs, after-action notes — showing the plan was actually executed during or after real events and exercises.</p>	<ul style="list-style-type: none"> • Recovery runbook covering identity, network core, SIS, finance and payroll, food service, transportation and the learning management system (LMS), with restoration steps, a named owner and a backup person for each • One-page restore order with a recovery time and data loss target for each critical system, signed by the superintendent • Recovery contact sheet for backup vendor support, hosted SIS and LMS vendors and the insurer's claims hotline, kept on paper as well as online
3 · Defined	<p>The plan now protects the recovery assets themselves and covers the school operations that depend on technology, not just servers. Dated records show the plan being carried out in exercises or real events.</p> <p>Moving up: Manage the plan actively: test business continuity on a schedule, hold regular leadership-plus-IT reviews of recovery processes, and run gap analyses that turn identified weaknesses into improvement actions with owners and due dates.</p>	<ul style="list-style-type: none"> • Backup console report showing an immutable or offline copy, with backup administrator accounts kept separate from everyday domain accounts and protected by MFA • Continuity annex covering paper attendance, printed medication and emergency contact lists, offline meal counts, printed bus routes and a payroll workaround agreed with the bank or processor • Restore test logs and an after-action note from a tabletop or real event showing what was restored, in what order and how long it took

Level	What you would see	Artifacts that show it
4 · Managed	<p>Recovery is managed like any other district program. Restore tests succeed on a schedule, continuity procedures are practiced in buildings, and the cabinet reviews results with the technology team and assigns fixes.</p> <p>Moving up: Embed recovery into daily decisions (procurement, cloud migrations, new-system approvals), use staged and real-time recovery exercises, feed every lesson learned back into the plan, and have leadership evolve strategy based on K12 threat and market trends.</p>	<ul style="list-style-type: none"> • A full year of scheduled restore tests, each comparing time to restore against the recovery time and data loss targets, with any failure followed up • Business continuity test record, such as a school running attendance and lunch service on paper for a morning, with principal and food service feedback • Cabinet review minutes with a gap analysis and an improvement list naming owners and due dates, plus an annual recovery readiness report to the board
5 · Optimized	<p>Recovery requirements shape decisions before systems are bought or moved. The district runs staged or live recovery exercises, updates the plan after every one, and adjusts its strategy as threats to schools change.</p>	<ul style="list-style-type: none"> • Procurement checklist or board agenda item for each new critical system or cloud move that records backup provisions, recovery targets and vendor restore commitments before approval • Staged recovery exercise, such as rebuilding identity and the SIS in an isolated recovery environment, followed by dated revisions to the plan • Annual strategy review that draws on K-12 threat information from sources such as CISA, MS-ISAC or K12 SIX and records resulting changes to recovery priorities or investments

Quick wins

Quick win and how	Cost	Effort	Usual owner
<p>Write the restore order for your top 10 systems on one page, with RTO/RPO agreed by the superintendent</p> <p>List your critical systems in the order they must come back, starting with identity (Google Workspace or Microsoft Entra ID, plus any on-premises Active Directory), then network core, SIS, finance and payroll, food service, transportation and the learning management system. Spend an hour with the superintendent and business and finance officer agreeing how long each can be down (recovery time objective, RTO) and how much data each can lose (recovery point objective, RPO), then have the superintendent sign the page.</p>	Free	Days	Technology director
<p>Do one timed test restore this quarter (a file, a server, and a Google Workspace/M365 item) and save the log</p> <p>Restore one file from a staff share, one server or virtual machine onto an isolated network segment, and one Google Drive folder or Microsoft 365 mailbox from your backup tool, timing each from start to usable. Record the date, system, backup point used, time to restore and who confirmed the data was correct, and save the log as evidence.</p>	Free	Hours	Network and systems administrator
<p>Turn on immutability or add an offline copy for at least one backup set</p> <p>Check whether your backup product or storage target supports object lock or a hardened immutable repository and turn it on for the SIS, finance and file server backups; if it does not, rotate an encrypted external drive offline each week and log every swap. Make sure the backup console uses its own administrator accounts, not domain accounts, with MFA required.</p>	Low cost	Days	Network and systems administrator
<p>Ask your SIS vendor in writing for their backup schedule, RTO/RPO, and emergency restore procedure</p> <p>Email your SIS account manager asking how often your district's data is backed up, how long backups are kept, the vendor's recovery time and data loss commitments, how to request an emergency restore after hours, and whether you can pull a full export of your data on demand. File the reply with the contract and ask whoever handles contracts to write the same terms into the next renewal.</p>	Free	Days	Technology director

Quick win and how	Cost	Effort	Usual owner
Adapt the K12 SIX and CISA #StopRansomware recovery checklists instead of starting from scratch Start from the response and recovery checklist in the CISA and MS-ISAC #StopRansomware Guide and the backup and incident planning items in K12 SIX's Essential Cybersecurity Protections, remove what does not apply, and add your own system names, people and phone numbers. Check current K12 SIX and Multi-State Information Sharing and Analysis Center (MS-ISAC) membership terms for any added templates available to members.	Free	Days	Technology director

Free means staff time, existing licenses or free government services. Effort: hours, days or weeks.

Common pitfalls

- Keeping backups where the attacker can reach them. A backup server joined to the domain, or a backup share reachable with the same administrator account, can be encrypted or deleted along with everything else; keep one copy immutable or offline and use separate, MFA-protected backup credentials.
- Assuming Google Workspace or Microsoft 365 data is backed up because it is in the cloud. Trash, Google Vault and Microsoft 365 retention policies support legal holds and recent recovery, but they are not designed to give a clean point-in-time restore after mass deletion or a compromised administrator account, so back up critical shared drives, mailboxes and business office files with a backup tool or scheduled exports.
- Restoring before the environment is clean. Bringing servers back while an attacker still holds administrator credentials invites a second encryption; follow your incident responders' direction, reset privileged and service account passwords (including the Active Directory krbtgt account, twice, if domain controllers were affected), check restore points for signs of compromise and bring systems back on a segmented network first.
- Setting recovery targets no one has tested. A promise to have the SIS back in 48 hours means little if a restore has never been timed or the vendor's contract commits to something slower; compare every target with a dated test or the vendor's written commitment and change one or the other.
- Forgetting the non-technical half of recovery. Servers can be back while buildings still cannot take attendance, run the lunch line or route buses, and confidential printouts such as free and reduced-price meal eligibility or student medication lists can end up unprotected; write and practice paper procedures with principals, food service and transportation, and state where printed sensitive lists are kept and when they are shredded.

Evidence that proves it

- Written incident recovery runbook with prioritized restore order, named owners, and documented RTO/RPO per system
- Backup restore test logs with dates, systems tested, and time-to-restore compared against RTO/RPO
- Backup console report showing an offline or immutable copy (object lock, air-gapped media) and retention settings
- SIS/LMS vendor contract or SLA language stating backup frequency and restore commitments
- After-action report from a real incident or exercise showing the recovery plan was executed
- Cabinet or board minutes showing review of recovery test results and a gap analysis with assigned actions
- Continuity of operations annex covering instruction and payroll during an extended outage

Who usually owns it

Technology director	Maintains the recovery plan and restore-order runbook, schedules and logs restore tests, and leads technical recovery and reporting to the superintendent during an incident.
Network and systems administrator	Runs and protects the backups, keeps an immutable or offline copy, performs timed test restores and checks that restore points are clean before they are used.
Superintendent	Approves recovery priorities and targets, decides when recovery is complete, and reports readiness, test results and incident outcomes to the board.
Business and finance officer	Owns the payroll and vendor payment workarounds, budgets for backup storage and recovery support, and makes sure hosted-system contracts include backup and restore commitments.

Insurance relevance · High

Backup and recovery questions are a standard part of cyber insurance applications and renewals, and carriers commonly treat an offline or immutable backup copy and evidence of restore testing as central to ransomware coverage. During a claim, the carrier's incident responders will ask how quickly the district can restore without outside help.

- Are all critical systems and data, including the SIS and business office systems, backed up automatically, and how often?
- Is at least one backup copy offline or immutable, and are backup administrator credentials separate from your normal network accounts?
- When did you last restore a critical system from backup, and how long did it take?
- Do you have a written disaster recovery or business continuity plan, and has it been tested in the past year?

Tip: Quote the date and duration from your most recent restore log, and answer yes on immutable or offline backups only if the setting is turned on in the backup console and covers the SIS and finance data.

Funding and free help**AWS K12 Cyber Grant Program**

Unclear · last published deadline was 31 Jan 2024

A \$20M pool of AWS promotional credits announced in 2023 for cloud-based security and resilience projects at districts and education agencies. Awards are credits, not cash.

CISA K-12 cybersecurity resources and toolkit

Always available

Free federal guidance for K-12: the K-12 cybersecurity report and toolkit, plus access to regional CISA advisors and no-cost services. A resource, not funding.

Programs, eligibility and deadlines change; confirm on the official page before applying.

Learn more

- #StopRansomware Guide (CISA) <https://www.cisa.gov/resources-tools/resources/stopransomware-guide>
- SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems (NIST) <https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final>
- CIS Critical Security Controls Implementation Group 1 (CIS) <https://www.cisecurity.org/controls/implementation-groups/ig1>
- The K12 SIX Essentials Series (K12 SIX) <https://www.k12six.org/essentials-series>
- CISA Tabletop Exercise Packages (CISA) <https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages>