

Incident Management

This category asks whether your district has a written, tested incident response plan with named people, a consistent way to triage and prioritize incoming reports, and clear rules for escalating and for declaring...

Why it matters

- When ransomware locks the student information system (SIS) at 6:40 a.m., someone has to decide within minutes whether to cut the internet connection, whether buses run and whether schools open. A plan that names an incident commander and a backup means those calls are made by the right person instead of whoever happens to answer the phone.
- Cyber insurance applications ask whether the district has a written incident response plan, who leads it and when it was last exercised. A current, tested plan supports better terms at renewal, and the first call it prescribes, to the carrier's claims hotline, helps protect coverage once a claim begins.
- A short plan exercised once a year with the superintendent, principals, the business office and communications turns the worst morning of the year into familiar steps. The exercise also finds gaps while they are cheap to fix, such as a phone tree that exists only on the file server the attacker just encrypted.

It matters because ransomware has closed real districts for multiple school days, and the first hour of a mishandled incident is where one phished account becomes a district-wide event. It is also a standard question on cyber insurance applications and renewal questionnaires — no documented, exercised plan often means higher premiums, coverage exclusions, or a declined application.

What good looks like at each level

Level	What you would see	Artifacts that show it
1 · Initial	<p>There is no approved incident response plan and no one has been named or trained to run one. If something happened tonight, the technology director would improvise and the superintendent might hear about it first from a principal or a parent.</p> <p>Moving up: Write down the plan you would improvise anyway and name who owns it — a documented IR plan plus designated, trained staff is exactly what separates Initial from Repeatable. Even a 10-page plan with a phone tree counts.</p>	<ul style="list-style-type: none"> • No written incident response plan, or a downloaded template that was never filled in or approved • No named incident commander or backup, and no agreement on who may take systems offline • No printed contact list with the cyber insurance carrier's claims hotline, the internet provider or the SIS vendor's support line
2 · Repeatable	<p>A written plan exists, names an incident commander and a backup, and the people in it have been walked through their roles. Improving incident response appears as a goal in the technology or strategic plan, though testing is still informal.</p> <p>Moving up: Formalize the plan, put an annual review on the calendar, and start testing it: in-house tabletops plus at least one scenario exercise involving a third party (insurer, MS-ISAC, or a vendor), with results written up and evaluated.</p>	<ul style="list-style-type: none"> • Incident response plan with a named incident commander, backup and severity scale, kept in print as well as online • Sign-in sheet or meeting notes showing designated staff reviewed their roles and the first-hour steps • Technology plan or district strategic plan item committing to test and improve incident response
3 · Defined	<p>A formal plan covers preparation, detection, containment, eradication and recovery, and is reviewed and approved every year. It is exercised routinely both in-house and with an outside party such as the carrier, a state partner or the Multi-State Information Sharing and Analysis Center (MS-ISAC), and each exercise produces a written evaluation.</p> <p>Moving up: Build scenario-specific playbooks (ransomware, business email compromise, compromised student account) that measure impact and bake in continuity of instruction, and convert every exercise or incident finding into a tracked action plan with owners and dates.</p>	<ul style="list-style-type: none"> • Plan revision history showing this year's review and the superintendent's approval • After-action reports from an in-house tabletop and from an exercise run with or by a third party • Triage log or ticket queue where every reported event is logged, validated, categorized and assigned a severity

Level	What you would see	Artifacts that show it
4 · Managed	<p>The district keeps playbooks for its own likely scenarios, such as ransomware during the state testing window or business email compromise in the payroll office, and each one covers how instruction, meals, transportation and payroll continue. Time is set aside after every exercise to evaluate impact and update recovery plans, and findings become tracked action items.</p> <p>Moving up: Move from annual review to continuous improvement: hold a lessons-learned session after every incident and exercise, let that feedback drive plan changes immediately, and make response planning something cabinet expects rather than a document IT maintains alone.</p>	<ul style="list-style-type: none"> • Scenario playbooks for ransomware, business email compromise and compromised staff or student accounts, each with a continuity section • Action plan tracker from exercises and incidents with owners, due dates and status • Annual readiness report to the board covering exercises held, response times and open action items
5 · Optimized	<p>Response readiness is part of how district leadership works rather than a binder the technology office maintains. Lessons-learned sessions follow every incident and exercise, and agreed changes go into the plan right away instead of waiting for the annual review.</p>	<ul style="list-style-type: none"> • Lessons-learned notes after each incident and exercise, each linked to the plan change it produced • Incident response woven into the district continuity and strategic plans, with cabinet members owning their sections • Plan change log showing several updates during the year, not a single annual edit

Quick wins

Quick win and how	Cost	Effort	Usual owner
<p>Print the phone tree and store copies in the tech office, superintendent's office, and each school</p> <p>Put the incident commander, backup, superintendent, principals, carrier claims hotline, internet provider, and SIS and backup vendors on one page with after-hours numbers, then place printed copies in a labeled binder at each site. Reprint at the start of each school year and whenever a name on the list changes.</p>	Free	Hours	Technology director
<p>Join MS-ISAC (check current membership terms) and add its 24/7 SOC number to the plan</p> <p>Apply through the Center for Internet Security's Multi-State Information Sharing and Analysis Center (MS-ISAC) membership page, confirm which dues tier applies and whether incident response support is included, and ask the business office to budget it. Add the 24/7 Security Operations Center (SOC) number to page one of the plan and to the printed phone tree.</p>	Low cost	Days	Technology director
<p>Confirm your cyber carrier's breach hotline number and put it on page one of the plan</p> <p>Pull the current cyber policy or ask the broker for the claims or breach hotline, the policy number and the notice requirements, then put all three on page one of the plan and on the printed phone tree. Confirm the number again at every renewal, since carriers and panel vendors change.</p>	Free	Hours	Business and finance officer
<p>Define a simple three-level severity scale on one page</p> <p>Use plain levels: Level 1 for a single account or device, Level 2 for a building or a whole system such as the SIS, and Level 3 for district-wide impact or any student or staff data involved. For each level, list who is notified and who has authority to take systems offline, and have the superintendent sign off.</p>	Free	Hours	Technology director
<p>Run a 45-minute tabletop with the superintendent using a free CISA scenario or a K12 SIX one</p> <p>Pick one scenario, such as ransomware discovered before first bell, from the Cybersecurity and Infrastructure Security Agency (CISA) Tabletop Exercise Packages or the portal's tabletop library, and invite the superintendent, a principal, the business officer and the communications lead. Record each decision and gap in a one-page after-action report with an owner for every fix.</p>	Free	Days	Technology director

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

Common pitfalls

- Keeping the only copy of the plan on the network. Ransomware can encrypt the file server and an attacker may be reading email, so keep printed copies with the superintendent, the technology office and each principal, plus an offline copy each responder can open on a phone.
- Making the technology director the whole plan. One person cannot contain the attack, call the carrier and brief the board at the same time, and will eventually be on vacation; name a backup commander and separate the technical lead from the person handling leadership and family communication.
- Running tabletops with the technology staff only. The hardest decisions, such as closing schools, approving outside help or notifying families, belong to the superintendent, the business office and communications, so put cabinet in the room.
- Filing the after-action report and moving on. Findings without an owner and a due date rarely get fixed; turn each one into a tracked action item and review the list at a cabinet meeting until it is closed.
- Adopting a template written for a large organization. A plan that assumes an in-house security operations center or staff the district does not have fails its first test; write for the people, contracts and carrier requirements you actually have.

Evidence that proves it

- Incident response plan with revision history and last-reviewed date
- Printed phone tree and contact roster including carrier hotline and MS-ISAC, dated this school year
- Tabletop exercise after-action report with assigned follow-up items
- One-page severity and triage matrix
- Incident log or ticket queue showing triage and categorization of past events
- Cabinet or board agenda and minutes showing annual IR plan review

Who usually owns it

Technology director

Maintains the plan, contact roster and severity scale, serves as incident commander unless someone else is designated, and schedules and documents exercises.

Superintendent

Approves the plan each year, receives escalations for significant incidents, and makes district-wide calls such as closing schools or shutting down systems.

Emergency management lead

Aligns the cyber plan with the district's emergency operations plan so school closures, family reunification and continuity of instruction follow familiar procedures.

Principals

Keep printed rosters at each school, take part in exercises, and run building-level continuity such as paper attendance and dismissal procedures when systems are down.

Insurance relevance · High

Carriers ask directly whether a written incident response plan exists, who leads it, when it was last reviewed and whether it was exercised in the past year. Underwriters read an exercised plan with documented lessons learned as a sign the district can keep an incident, and the claim, small.

- Do you have a written incident response plan that names an incident commander and defines escalation paths?
- When was the plan last reviewed and approved, and by whom?
- Have you exercised the plan through a tabletop or drill in the past 12 months, and what changed afterward?
- Does the plan say who notifies the carrier and how, and can staff reach that information if district systems are down?

Tip: Answer from the plan's revision date and the latest after-action report, and if the last exercise is more than a year old, run one before signing the application rather than rounding up.

Funding and free help

MS-ISAC membership (Center for Internet Security)

Paid membership · rolling

Threat intelligence, 24x7 SOC advisories, incident response help and services for state and local governments. Fee-based since October 2025, tiered by operating budget; some CIS tools remain free.

State and Local Cybersecurity Grant Program (SLCGP) — Georgia subawards

Georgia FY2024 round closed May 15, 2026 · watch for the FY2025 round

Federal cyber grant passed through the state to local governments, including school districts. Georgia accepted FY2024 subaward applications April 1 – May 15, 2026. Federal authority beyond September 30, 2026 depends on Congress.

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

- Cybersecurity Incidents (Georgia Technology Authority) <https://gta.georgia.gov/contact-us/cybersecurity-incidents>
- CISA Tabletop Exercise Packages (CISA) <https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages>
- SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile (NIST) <https://csrc.nist.gov/pubs/sp/800/61/r3/final>
- #StopRansomware Guide (CISA) <https://www.cisa.gov/resources-tools/resources/stopransomware-guide>
- The K12 SIX Essentials Series (K12 SIX) <https://www.k12six.org/essentials-series>
- Online Toolkit: Partnering to Safeguard K-12 Organizations from Cybersecurity Threats (CISA) <https://www.cisa.gov/topics/cybersecurity-best-practices/K12cybersecurity/online-toolkit-partnering-safeguard-k-12-organizations-cybsecurity-threats>