

Policy

This category asks whether the district has written cybersecurity policies that are adopted, communicated, and actually enforced — an acceptable use policy alone does not cover it.

Why it matters

- Written, board-adopted policy lets the technology director require multi-factor authentication (MFA), restrict personal devices or remove an unapproved app without it becoming a personal argument with a principal or teacher. Enforcement points to the policy, not to IT.
- After an incident, breach counsel, auditors and the insurance carrier ask which policies were in force and whether staff acknowledged them. Missing or outdated policies make the district's response harder to defend and can complicate a claim.
- Clear procedures for everyday decisions, such as verifying a vendor's change of bank details or approving a new classroom app, prevent the mistakes that lead to lost funds and exposed student data, because staff know the rule before the pressure arrives.

Policies are among the first artifacts requested by cyber insurance underwriters, auditors, and breach counsel, and they are the footing for requiring MFA or acting on risky behavior. Without them, every hard decision gets re-litigated in the middle of a crisis, and enforcement looks arbitrary.

What good looks like at each level

Level	What you would see	Artifacts that show it
1 · Initial	<p>Beyond acceptable use policies for students and staff, little is in writing. Expectations about passwords, data sharing or new apps go out by email when a problem comes up, and enforcement depends on who is involved.</p> <p>Moving up: Get first policy drafts on paper with governance behind them — leadership approving strategic direction and policy creation — so risk management starts shifting from reactive to proactive.</p>	<ul style="list-style-type: none"> • No board policy on data governance, access control or incident response • An acceptable use policy not revisited since devices or cloud tools changed • No record of which staff have read or acknowledged any policy
2 · Repeatable	<p>Leadership has set a direction and core policies are being drafted, usually adapted from school boards association model language. Some procedures exist, such as an MFA requirement for administrator accounts, but the set is incomplete.</p> <p>Moving up: Finish documenting the core policy set and get stakeholder agreement, including a risk assessment policy that covers identifying new threats, vulnerabilities, and conditions that could affect district systems.</p>	<ul style="list-style-type: none"> • Cabinet or board minutes authorizing policy development • Draft data governance and incident response policies in review • A gap list comparing current policies to a core set
3 · Defined	<p>A core set of policies is board-adopted with matching administrative procedures, after review by HR, principals and the business office. Staff acknowledge policies at hire and each year, and a risk assessment policy says how new threats and vulnerabilities are identified.</p> <p>Moving up: Operate a real review-update-communicate-enforce cycle: policies change when requirements, threats, technology, or the district's mission change, acknowledgments are tracked, and enforcement is consistent.</p>	<ul style="list-style-type: none"> • Board-adopted policies for acceptable use, data governance and privacy, access control, incident response, vendor data sharing, and backup and retention • Administrative procedures linked to each policy, including a call-back procedure for any change to vendor or employee banking details • Acknowledgment records from the HR system or the annual handbook sign-off
4 · Managed	<p>Policies follow a review calendar and change when laws, threats, technology or the district's mission change, for example adding guidance on classroom artificial intelligence (AI) tools. Technical settings match the written rules, and violations are handled consistently through staff and student discipline processes.</p> <p>Moving up: Eliminate remaining gaps so policy coverage is uniform across every school and department, and share policy updates and lessons learned with other districts and the education community.</p>	<ul style="list-style-type: none"> • Policy review log with owners, review dates and summaries of changes • Admin console settings, such as enforced 2-Step Verification or Conditional Access, that match the access control policy • Records of recommunication after significant updates, such as a staff bulletin or refreshed acknowledgment

Level	What you would see	Artifacts that show it
5 · Optimized	Policy coverage is uniform across every school, department and program, including athletics, nutrition, transportation and after-school programs. The district shares updated policies and lessons learned with peer districts and associations.	<ul style="list-style-type: none"> Annual check confirming every school and department operates under current policies, with gaps tracked to closure Policies or procedures shared with a regional service agency, state association or the K12 SIX community Lessons from incidents and exercises reflected in policy revisions

Quick wins

Quick win and how	Cost	Effort	Usual owner
Gap-check your current policies against the core set in one sitting List the six core areas (acceptable use, data governance and privacy, access control and MFA, incident response, vendor and data sharing, backup and retention) and note for each whether a board policy, an administrative procedure or nothing exists. Bring the gap list to the superintendent with a proposed drafting order.	Free	Hours	Technology director
Pull model policy language from your state school boards association Ask the board secretary whether the district subscribes to the Georgia School Boards Association (GSBA) policy service or your state association's equivalent, and pull model language for technology use, data privacy and records. Adapt it to your actual systems and titles rather than adopting it word for word.	Low cost	Hours	Superintendent
Add policy acknowledgment to onboarding paperwork and the annual handbook sign-off Add the acceptable use and data privacy policies to the new-hire packet and the annual handbook acknowledgment in your HR system or learning management system (LMS), and keep the completion report. Include substitutes and contractors who receive district accounts.	Free	Days	HR director
Put version numbers and review dates on every existing policy document Add a short header to each document with version, approval date, owner and next review date, and keep a brief change history at the end. This turns documents you already have into evidence that policies are managed.	Free	Hours	Technology director
Set calendar reminders for annual policy review Create recurring calendar events for each policy owner, spread across the year so reviews do not pile up before the insurance renewal or the board's policy cycle. Link each event to the review log so completed reviews are recorded.	Free	Hours	Technology director

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

Common pitfalls

- Putting operational detail in board policy. If board policy names a product or a password length, every technical change needs a board vote; keep board policy short and principle-based and put settings and steps in administrative procedures the superintendent can update.
- Writing policies the technology cannot enforce. A requirement for MFA on all staff accounts means little if enforcement is off in the admin console; check that each policy statement has a matching technical setting or a documented exception.
- Copying model policy without adapting it. Model language may reference roles, systems or processes the district does not have, which an auditor or attorney will notice; edit for your actual titles, systems and procedures.
- Collecting no proof that staff were told. A policy staff never acknowledged is hard to enforce in a personnel matter, so keep acknowledgment records from hire and each year.
- Forgetting the business office. Payment fraud often starts with an email asking to change a vendor's bank account; without a written call-back procedure finance staff have no rule to point to, and some insurance coverage depends on that verification.

Evidence that proves it

- Board-adopted cybersecurity and data governance policies with adoption dates
- Administrative procedures paired to each board policy
- Staff acknowledgment records from the HR system or LMS
- Policy review calendar and revision history pages
- Incident response policy cross-referenced by the IR plan
- Cyber insurance application listing the policies in force

Who usually owns it

Superintendent	Presents policies to the board, maintains administrative procedures and directs the annual review cycle.
Technology director	Drafts technical policy content, puts matching technical controls in place and flags gaps revealed by incidents or new tools.
HR director	Collects acknowledgments at hire and annually and ties policies to the handbook and discipline procedures.
School board	Adopts board policies and approves significant revisions after a briefing from administration.

Insurance relevance · High

Applications commonly ask whether written, leadership-approved security policies exist and are reviewed regularly, and coverage for social engineering and funds-transfer fraud can depend on a documented verification procedure being followed. After a loss, the carrier compares the application answers with the policies actually in force.

- Do you have written cybersecurity policies approved by leadership covering acceptable use, access control, data handling and incident response?
- How often are these policies reviewed and updated?
- Do staff confirm any request to change vendor or employee banking details by calling a known phone number before making the change?
- Do employees acknowledge security policies when hired and periodically afterward?

Tip: List only policies that are adopted and in force, and keep the adoption minutes and acknowledgment records ready in case the carrier asks for them.

Funding and free help

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

- The K12 SIX Essentials Series (K12 SIX) <https://www.k12six.org/essentials-series>
- CIS Critical Security Controls Implementation Group 1 (CIS) <https://www.cisecurity.org/controls/implementation-groups/ig1>
- CSF 2.0 Quick-Start Guides (NIST) <https://www.nist.gov/cyberframework/quick-start-guides>
- Protecting Student Privacy (U.S. Department of Education) <https://studentprivacy.ed.gov/>
- Cybersecurity Rubric (CR) (CoSN) <https://www.cosn.org/cybersecurity-rubric/>