

Roles, Responsibilities, and Authorities

This category asks who owns cybersecurity in the district — by name, in writing, with budget to match — and whether security is wired into HR from onboarding to offboarding.

Why it matters

- In a small district, cybersecurity often rests on one person. If that person is out when an account is compromised, a written list of duties with named backups is what lets someone else disable accounts, call the insurer and reach vendors without guessing.
- Removing access the same day staff, substitutes and contractors leave depends on HR and IT working from one checklist. When that is nobody's written job, former employees can keep access to email, the student information system (SIS) or payroll long after they leave.
- A named, accountable executive with a budget line lets the superintendent answer the board, auditors and the insurance application with confidence. It also gives the technology director standing to require multi-factor authentication (MFA) or training without it turning into a personal dispute.

In small districts everything defaults to the technology director, which fails when that person is out during an incident and leaves the superintendent accountable for a program they cannot describe. Orphaned accounts from sloppy offboarding are a well-known breach entry point, and insurance applications now routinely ask for a named security lead and mandatory staff training.

What good looks like at each level

Level	What you would see	Artifacts that show it
1 · Initial	<p>Cybersecurity is whatever the technology director has time for. No executive is named as accountable, privacy questions go to whoever answers first, and there is no budget line for security. Moving up: Name an executive-level leader responsible for cybersecurity policy and practice, start defining roles for internal and external stakeholders, and get basic needs identified with budget allocated against them.</p>	<ul style="list-style-type: none"> • No written designation of a cybersecurity or data privacy lead • Security costs buried in general technology supply or software lines • Accounts issued before any security training, and offboarding that relies on someone remembering to tell IT
2 · Repeatable	<p>An executive leader, often an assistant superintendent or the superintendent, is identified as responsible for cybersecurity, and roles for staff and key vendors are being written. Basic needs such as MFA licensing or backup storage are identified and at least partly funded. Moving up: Document roles until they are understood by the people holding them, designate staff to maintain privacy and security policies, align resources system-wide to current and future needs, and put cyber training into HR onboarding plus a recurring cycle.</p>	<ul style="list-style-type: none"> • Superintendent memo or cabinet minutes naming the accountable executive • Draft responsibility list covering IT, HR, the business office and any managed service provider • Budget request that identifies basic security needs, even if not fully funded
3 · Defined	<p>Roles are written down and the people who hold them can describe them, including outside partners such as the Regional Educational Service Agency (RESA) or a managed service provider. Named staff maintain privacy and security policies, the budget covers current and planned needs, and HR runs security training at hire and on a recurring cycle. Moving up: Build an awareness program that measurably changes workforce behavior, and review the practice areas (CoSN TLE is the rubric's reference model) annually with improvement initiatives driven by evaluation results.</p>	<ul style="list-style-type: none"> • One-page responsibility chart (responsible, accountable, consulted, informed, often called a RACI) with a named backup for each duty • Job descriptions for the technology director, HR director and data privacy lead that include security duties • HR records showing training completed before credentials are issued, an annual refresher, and separation tickets closed the same day

Level	What you would see	Artifacts that show it
4 · Managed	<p>The awareness program targets behavior, not just completion: staff report suspicious messages and the district measures it. Each year leadership reviews the CoSN Trusted Learning Environment (TLE) practice areas (leadership, business, data security, professional development and classroom) and sets improvement goals from the results.</p> <p>Moving up: Define detection roles so accountability is unambiguous, audit governance annually against federal, state, and local requirements, and work toward the CoSN TLE Seal as external validation.</p>	<ul style="list-style-type: none"> Phishing-report and simulation trends presented to cabinet Role-specific training for finance, HR and school office staff who handle payments and records Annual TLE practice-area review with improvement initiatives assigned to owners
5 · Optimized	<p>Accountability is clear down to who watches security alerts and who escalates them, including after hours and through managed partners. Governance is audited each year against federal, state and local requirements, and the district holds or is actively pursuing the CoSN Trusted Learning Environment (TLE) Seal.</p>	<ul style="list-style-type: none"> Written detection and escalation duties, including who covers alerts outside school hours Annual governance compliance audit report with corrective actions TLE Seal application materials or award letter

Quick wins

Quick win and how	Cost	Effort	Usual owner
<p>Draft the one-page RACI this month and have cabinet confirm it</p> <p>List recurring duties down the side (policy upkeep, account creation and removal, patching, backup checks, vendor vetting, training, incident lead, public statements) and roles across the top, marking who is responsible, accountable, consulted and informed (RACI). Add a named backup for each duty and bring the chart to cabinet for confirmation.</p>	Free	Days	Technology director
<p>Add a same-day account-disable step to the HR offboarding checklist</p> <p>Add a step requiring HR to notify the help desk on the last day, and have IT suspend the Google Workspace or Microsoft 365 account, SIS access, finance and payroll access and door badges, recording the ticket number on the checklist. Cover substitutes, coaches and contractors as well as full-time staff.</p>	Free	Hours	HR director
<p>Issue a superintendent memo naming the security lead and a backup</p> <p>A half-page memo is enough: name the accountable executive, the day-to-day security lead and the backup, and state their authority to act in an incident, such as disabling accounts or taking systems offline. Share it with cabinet and principals.</p>	Free	Hours	Superintendent
<p>Move security awareness training into the onboarding packet before credentials are issued</p> <p>Assign a short module from your existing training platform or the free Cybersecurity and Infrastructure Security Agency (CISA) Secure Our World materials as part of new-hire paperwork. Have IT release credentials only after HR confirms completion, and apply the same rule to long-term substitutes and student teachers who get district accounts.</p>	Free	Days	HR director
<p>Request a cybersecurity line item, even a small one, in the next budget cycle</p> <p>With the technology director, move existing security costs (MFA licenses, backup storage, filtering, training) into one visible line, then add the next priority from the risk register. Note which items may qualify for E-Rate Category 2, the Federal Communications Commission (FCC) cybersecurity pilot if the district participates, or state grant programs.</p>	Needs budget	Weeks	Business and finance officer

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

Common pitfalls

- Making the technology director accountable for everything. Accountability for risk belongs with an executive who can set priorities and budget, while the technology director runs the program; write both names down so decisions do not stall in the IT office.
- Having no backup for critical duties. Incidents do not wait for the one person who knows the admin passwords; name a backup for each duty, store emergency administrator credentials in a sealed or vaulted location, and have the backup practice key steps once a year.
- Offboarding only full-time staff. Substitutes, coaches, student teachers, contractors and board members often have accounts that outlive their role; send every account type through the same separation process and review leftover accounts each semester.
- Measuring training by completion alone. Staff can click through a module and still approve a fraudulent bank change request; track reported phishing, give finance and front office staff role-specific training, and follow up with people who struggle.
- Leaving managed service providers off the role chart. If an outside firm runs the firewall or backups, its incident duties and after-hours contacts belong in both the contract and the responsibility chart.

Evidence that proves it

- Board policy or superintendent memo naming the accountable executive and security lead
- One-page RACI chart with named backups for each duty
- Job descriptions that include cybersecurity responsibilities
- Onboarding checklist showing security training before account issuance
- Offboarding checklist with same-day account disablement steps and completion records
- Budget documents showing a dedicated cybersecurity line item
- Training completion and phishing-report metrics presented to leadership

Who usually owns it

Superintendent	Names the accountable executive and security lead in writing and makes sure staffing and budget match their duties.
Technology director	Runs the program day to day, maintains the responsibility chart and backups, and coordinates training content.
HR director	Builds security into hiring, onboarding, role changes and separations, and tracks training completion.
Business and finance officer	Creates and protects a dedicated cybersecurity budget line and identifies funding sources.

Insurance relevance · Medium

Carriers ask whether a specific person is responsible for cybersecurity and whether staff are trained regularly, because both suggest the program will hold up under pressure. Some applications also ask how quickly access is removed when staff leave.

- Who is responsible for information security, and do they report to senior leadership?
- Do all employees complete security awareness training at hire and at least once a year?
- Do you run phishing simulations, and what happens when staff fall for them?
- How soon after an employee leaves is their access removed?

Tip: Answer the training and offboarding questions from HR and help desk records, and include substitutes and contractors, because a claim review looks at every account.

Funding and free help

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

- Protecting Our Future: Partnering to Safeguard K-12 Organizations from Cybersecurity Threats (CISA) <https://www.cisa.gov/resources-tools/resources/report-partnering-safeguard-k-12-organizations-cybersecurity-threats>
- Cybersecurity Rubric (CR) (CoSN) <https://www.cosn.org/cybersecurity-rubric/>
- Cross-Sector Cybersecurity Performance Goals (CISA) <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>

- Cybersecurity Awareness Month (CISA) <https://www.cisa.gov/cybersecurity-awareness-month>
- Cybersecurity Pilot Program (USAC) <https://www.usac.org/e-rate/cybersecurity-pilot-program/>