

Identity Management, Authentication, and Access Control

This category asks who can log into your systems, how you verify it is really them, and how fast access disappears when someone leaves.

Why it matters

- When a staff password is phished or reused from another breach, multi-factor authentication (MFA) is what stops the attacker at the sign-in screen instead of inside the payroll mailbox, the SIS gradebook or the Google or Microsoft admin console.
- Accounts that outlive employment are a quiet risk: a former employee, coach or long-term substitute whose account still works can read student records and send email as the district after anyone has stopped supervising that access.
- Cyber insurance applications ask about MFA for email, remote access and administrator accounts as separate questions, and an answer that does not match what the admin console actually enforces can put coverage or a claim at risk.

Compromised staff credentials are a common way attackers get into districts, and carriers can decline coverage or contest claims when the MFA box on the questionnaire does not match what the admin console actually enforces. It also covers physical access: who holds keys and badges to the server room and wiring closets.

What good looks like at each level

Level	What you would see	Artifacts that show it
1 · Initial	<p>Access is granted by whoever asks IT, a password is the only proof of identity, and departed staff accounts stay active until someone happens to notice.</p> <p>Moving up: Write down your access control procedures for physical and remote access, define conditions for group and role membership, and get at least one MFA method live - enforced MFA on staff email is the fastest path. Documented but imperfect beats undocumented.</p>	<ul style="list-style-type: none"> • No written access control procedure; requests arrive by hallway conversation or email • MFA available but not enforced, or not turned on at all, in the Google or Microsoft admin console • Shared or default passwords on the SIS, network gear or the server room door code, with no list of who knows them
2 · Repeatable	<p>A written procedure exists and at least one MFA method is live, usually enforced for IT and business office accounts, but account reviews and offboarding still depend on someone remembering.</p> <p>Moving up: Move from defined to enforced: actually run the account reviews on schedule, assign a named account manager for each system, and apply group and role membership rules every time, with sign-offs or tickets proving it happened.</p>	<ul style="list-style-type: none"> • One- or two-page access control procedure covering physical and remote access, with defined roles such as teacher, office, substitute and vendor • Admin console showing MFA enforced for at least one group, such as IT staff, while other staff are encouraged but not required to enroll • Documented quarterly account review process with few or no completed reviews on file
3 · Defined	<p>MFA is enforced for all staff through Conditional Access or 2-Step Verification enforcement, access reviews run on a schedule, and each major system has a named account manager.</p> <p>Moving up: Make evaluation routine: test whether your MFA methods still hold up (push fatigue, phishing-resistant options for admins), and review account and network access processes against state and federal requirements, feeding findings into access-control risk mitigation.</p>	<ul style="list-style-type: none"> • Admin console report showing MFA enforced for every staff organizational unit or group, with any exceptions documented • Quarterly access review log for the directory, SIS and finance system with reviewer sign-off • HR-to-IT separation tickets closed on or before each departure date
4 · Managed	<p>Access controls work the same way across the directory, SIS, finance system and building access, and the district tests whether its MFA methods and review processes still hold up and still meet state and federal requirements.</p> <p>Moving up: Close the remaining gaps and let data drive decisions: automate provisioning and deprovisioning from HR, review access analytics on a cycle, and leave no population - substitutes, vendors, service accounts - outside MFA and review.</p>	<ul style="list-style-type: none"> • Annual MFA review addressing push-approval fatigue and moving administrators to phishing-resistant methods such as security keys or passkeys • Account review results checked against FERPA and state requirements, with risk mitigation actions tracked to closure • MFA coverage and time-to-disable figures reported to the superintendent twice a year

Level	What you would see	Artifacts that show it
5 · Optimized	Access decisions are driven by data, and no group of users, including substitutes, coaches, vendors and service accounts, sits outside MFA and periodic review.	<ul style="list-style-type: none"> Accounts created, changed and disabled automatically from the HR or SIS system of record, with exceptions alerting IT Sign-in risk and access reports reviewed on a set cycle, with the resulting decisions logged Vendor and service account register with named owners, expiry dates and MFA or documented compensating controls

Quick wins

Quick win and how	Cost	Effort	Usual owner
Enforce MFA for all IT admin, business office, and HR accounts this week Put these users in their own organizational unit in Google or a group in Microsoft, give a few days' notice to enroll, then turn on 2-Step Verification enforcement or a Conditional Access policy requiring MFA (security defaults if your license lacks Conditional Access). Keep two emergency admin accounts with long random passwords stored offline so a misconfiguration cannot lock everyone out.	Free	Days	Technology director
Run a one-time sweep to disable accounts of departed staff and anything dormant 90+ days Export users with last sign-in dates from the Google Admin console or Microsoft Entra admin center, compare them with a current HR roster, and suspend rather than delete anything unmatched or idle for 90 days. Repeat the check in the SIS, finance system and vendor portals, and keep the exports as evidence.	Free	Days	Network and systems administrator
Create separate admin accounts for techs and strip admin rights from daily accounts Give each technician a second account used only for administration (for example jsmith-admin), move super admin or Global Administrator roles onto those accounts, and use narrower delegated roles such as password reset for everyday help desk work. Record the list of admin accounts and their owners.	Free	Days	Technology director
Set up a same-day HR-to-IT notification for every separation Add an IT step to the HR separation checklist: HR submits a help desk ticket or form on or before the last day listing the end date, buildings and systems, and IT disables access and records the time. Include coaches, long-term substitutes and contractors, who may not flow through the normal payroll process.	Free	Hours	HR director
Put locks on any open wiring closet and list who holds server room keys Walk every building with the head custodian, lock or re-key any open closet, and start a key and badge register showing holder, date issued and date returned. Add a vendor sign-in sheet at the main distribution frame (MDF) and server room door.	Low cost	Days	Technology director

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

Common pitfalls

- Exempting the superintendent, cabinet or board members from MFA after complaints. Leaders' mailboxes are attractive targets for payment and impersonation fraud, so enroll them first, in person, and let them set the example.
- Counting MFA as done when it is only available. Enrollment without enforcement leaves every unenrolled account open, and carriers and assessors look at the enforcement setting rather than how many people opted in.
- Relying on text-message codes or simple push approvals for administrator accounts. Codes can be intercepted through SIM swaps and a tired user can approve a push they did not start; use number matching or authenticator apps for staff and security keys or passkeys for administrators.
- Running the dormant-account sweep in July and disabling teachers who are simply on summer break. Time reviews against the school calendar, confirm departures with HR, and suspend before deleting so mail and Drive or OneDrive files can be recovered.
- Leaving shared and vendor accounts out of scope. Front-office shared logins, vendor support accounts and SIS integration accounts often hold broad rights with no owner; give each a named owner, the narrowest role that works and a review date.

Evidence that proves it

- MFA enforcement report from the Google or Microsoft admin console showing percent of staff enrolled
- Written access control procedure with onboarding/offboarding checklist
- Most recent quarterly account review with reviewer sign-off and date
- List of admin accounts with named owners, separate from daily-use accounts
- HR-to-IT termination workflow (form or ticket) with same-day disable timestamps
- Key and badge assignment log for server rooms and MDF/IDF closets
- Cyber insurance application MFA answers matching current console settings

Who usually owns it

Technology director	Owns the access control procedure, sets MFA and admin-account standards, and signs off on quarterly account reviews.
HR director	Sends every hire, role change and separation to IT on or before the effective date, including substitutes, coaches and contractors.
Network and systems administrator	Configures MFA enforcement, runs account exports and dormant-account sweeps, and maintains separate administrator accounts.
Principals	Approve role-based access for building staff and confirm their building's access list during each review.

Insurance relevance · High

Carriers probe identity closely, asking about MFA for email, remote access and privileged accounts as separate questions along with offboarding and dormant accounts, and some decline or surcharge applicants who cannot answer yes.

- Is MFA required, not just offered, for every staff member's email and cloud applications?
- Is MFA required for all remote access, including VPN, remote desktop and vendor support tools?
- Do all administrative and privileged accounts use MFA, and are they separate from everyday accounts?
- How quickly are accounts disabled when someone leaves, and how do you find dormant accounts?

Tip: Before signing the application, export the MFA enforcement report and admin role list from the console, answer from those screens, and describe any exceptions in writing instead of rounding up to yes.

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

- Multifactor Authentication (CISA) <https://www.cisa.gov/topics/cybersecurity-best-practices/multifactor-authentication>
- 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>
- Cross-Sector Cybersecurity Performance Goals (CISA) <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>