GLET Georgia Leaders of Educational Technology COSN GA | K12 Cyber Forward

CATEGORY GUIDE · PROTECT · AREA 13 OF 22 · NIST CSF 2.0 PR.PS

Platform Security

This category asks whether the platforms themselves - servers, staff and student devices, network gear, and applications - are patched, securely configured, maintained on a documented schedule, and retired...

Why it matters

- Attackers scan the internet for firewalls, VPN appliances and servers missing known patches, and an unpatched internet-facing device can let them in without anyone in the district clicking anything.
- Chromebooks, Windows laptops and servers that pass their end-of-support date stop receiving security fixes, so planning refresh cycles in the budget avoids a forced, unfunded replacement in the middle of a school year.
- Maintenance and change records help a small team fix things faster after an outage, show auditors that patching actually happens, and support the patch window you report on a cyber insurance application.

Unpatched internet-facing devices and forgotten end-of-life servers are common ways ransomware gets into districts, and a missing patch-management process is a standard audit finding and cyber insurance red flag.

What good looks like at each level

Level	What you would see	Artifacts that show it
1 · Initial	Patches go on when someone has time, vendor technicians connect whenever they like, and there is no record of what changed or whether it still worked afterward. Moving up: Make maintenance repeatable: patch and maintain systems per vendor specifications on a consistent schedule, document the security controls in place, keep maintenance records every time, and name your go-to staff for each system.	• No written patch schedule; updates are applied after something breaks • Shared vendor remote access passwords with no session approval or log • Default passwords still set on printers, switches or the phone system
2 · Repeatable	Maintenance follows vendor specifications on a regular schedule, security controls are documented, and records are kept every time. Knowledge sits with a few go-to staff, and preventive maintenance is being written down. Moving up: Formalize control: approve, control, and test maintenance tools and activities, verify security controls after maintenance, retain detailed logs, and require approval and logging for every remote maintenance session.	• Monthly patch schedule for Windows and servers, with automatic updates on for Chrome devices and browsers • Maintenance entries in the ticket system for each piece of work • List naming the go-to person for each major system, such as the firewall, phone system and SIS integrations
3 · Defined	Maintenance tools and activities are approved, controlled and tested, security controls are checked after each change, detailed logs are kept, and every remote maintenance session is approved and logged. Moving up: Manage adherence: designated staff measure patch and refresh-cycle compliance, misses trigger corrective action, and leadership frees up resources when there is a risk of noncompliance or poor performance.	• Written patching standard with timelines for critical and actively exploited vulnerabilities, plus compliance reports from Intune, WSUS or the remote monitoring and management (RMM) tool • Change tickets recording approval and a post-change check, such as confirming the firewall still blocks inbound remote desktop • Vendor remote access log showing named accounts and approval for each session
4 · Managed	Designated staff measure patch and refresh-cycle compliance against targets, misses trigger corrective action, and leadership moves resources when compliance is at risk. Moving up: Shift to lifecycle thinking: strategically planned change management, proactive hardware and software refresh ahead of end-of-life, and continuous improvement of maintenance efficiency by staff trained deeply in security.	• Quarterly patch compliance report to the superintendent listing overdue items and owners • Device refresh plan tied to Chromebook Auto Update Expiration (AUE) dates and Windows end-of-support dates • Corrective action records, such as contractor hours approved to clear a patch backlog

Level	What you would see	Artifacts that show it
5 · Optimized	Systems are managed through a planned lifecycle from purchase to retirement, change management is planned strategically, and patching and configuration enforcement are largely automated, with trained staff focused on improvement.	• Multi-year lifecycle plan with refresh dates for servers, network gear and the device fleet • Automated patch rings and configuration baselines with reports of settings that drift • Post-change and post-incident reviews that lead to documented changes in the maintenance process

Quick wins

Quick win and how	Cost	Effort	Usual owner
Turn on automatic updates for Windows, browsers, and the Chrome fleet Set Windows Update for Business rings in Intune or a WSUS auto-approval rule for security updates, keep Chrome and Edge on automatic updates, and confirm in the Google Admin console that ChromeOS devices are allowed to update. If a testing vendor requires a version hold during state testing, give the hold an end date.	Free	Days	Network and systems administrator
Change default passwords on printers, access points, and appliances Work through printers, copiers, cameras, UPS management cards and wireless controllers, set a unique admin password for each in a password manager, and turn off web admin pages that are not needed. Record each change in the ticket system.	Free	Days	Network and systems administrator
Remove local admin rights from staff machines Use an Intune account protection policy or Group Policy restricted groups to remove staff from the local Administrators group, use Windows LAPS to rotate the built-in admin password, and deploy the software teachers need through Intune or Software Center. Pilot in one building and keep a short exception list with approvals and end dates.	Free	Weeks	Network and systems administrator
Join MS-ISAC and subscribe to CISA and vendor advisories Check current MS-ISAC membership terms and whether your state provides membership, and sign up for CISA alerts and Known Exploited Vulnerabilities catalog updates. Subscribe a shared IT mailbox to security advisories from your firewall, switch and SIS vendors.	Low cost	Hours	Technology director
Start logging every change in your existing ticket system Create a change ticket type with fields for what changed, who approved it, when, and how it was checked afterward, and require it for firewall rules, server updates and admin console settings. Review the week's changes in a short Monday check-in.	Free	Hours	Technology director

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

Common pitfalls

- Patching laptops but not the network edge. Firewalls, VPN appliances and remote access gateways face the internet directly and need firmware updates too; check vendor advisories and the CISA Known Exploited Vulnerabilities (KEV) catalog every week.
- Holding Chromebook or testing-device updates and forgetting to release them. Version pins set for state testing can leave devices far behind on security fixes, so put an end date on every hold.
- Keeping an old server running because one application still needs it. An unsupported server on the main network is an open door; isolate it on its own segment, restrict who can reach it, and set a retirement date with the application owner.
- Giving vendors standing remote access. Always-on support tools with shared passwords let anyone holding that password into district systems; require named accounts, MFA and approval for each session.
- Assuming a scheduled patch was installed. Updates fail quietly or get rolled back, so use compliance reports rather than the deployment schedule as proof.

Evidence that proves it

- Patch compliance dashboard from RMM, Intune, or WSUS showing percent current
- Change and maintenance log or ticket history with approvals and post-change verification
- Software inventory flagging unsupported or end-of-life items
- Chromebook AUE tracking sheet tied to a replacement budget
- Firewall and switch firmware update records
- Vendor remote-access approval and session logs

Who usually owns it

Technology director	Sets the patching and change standard, approves maintenance and remote access, and reports compliance to the superintendent.
Network and systems administrator	Applies patches and firmware, maintains secure configurations, and records each change with a post-change check.
Procurement and contracts lead	Writes supported lifecycle, patch delivery, secure remote support and breach notification terms into technology contracts.
Business and finance officer	Budgets device and infrastructure refresh ahead of end-of-support dates.

Insurance relevance · High

Underwriters ask how quickly you apply critical patches, whether unsupported systems are retired or isolated, and what protects endpoints and email, and some carriers scan your public addresses for known weaknesses before quoting.

- How many days does it take you to apply critical security patches, and how much faster for actively exploited ones?
- Is all software and firmware still supported by its vendor, and are any end-of-life systems isolated?
- Do all workstations and servers run endpoint detection and response (EDR) or next-generation antivirus?
- Do district email domains publish Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance (DMARC) records with an enforcing policy?

Tip: Report the patch window your compliance reports actually show rather than the policy target, and list any end-of-life system with its isolation and retirement date.

Funding and free help

Cloudflare Project Cybersafe Schools Rolling (2026 enrollment not separately confirmed)	Free email security and DNS filtering for small U.S. public school districts, announced in 2023 with no stated end date.
E-Rate Category Two (internal connections, including firewalls) Annual cycle · FY2027 window not yet announced	E-Rate discounts of 20–85% on equipment that carries broadband inside schools. Basic firewall services and components are the security-relevant Category Two items; requests count against a five-year, pre-discount budget per district.
CISA Cyber Hygiene Services (vulnerability and web application scanning) Rolling enrollment	Free, continuous external vulnerability scanning of a district's public IP addresses with weekly reports and urgent alerts; optional web application scanning is also 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.

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

Learn more

- Known Exploited Vulnerabilities Catalog (CISA) https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CIS Critical Security Controls Implementation Group 1 (CIS) https://www.cisecurity.org/controls/implementation-groups/ig1
- Cyber Hygiene Services (CISA) https://www.cisa.gov/cyber-hygiene-services
- SP 800-177 Rev. 1, Trustworthy Email (NIST) https://csrc.nist.gov/pubs/sp/800/177/r1/final
- The K12 SIX Essentials Series (K12 SIX) https://www.k12six.org/essentials-series