

Technology Infrastructure Resilience

This category asks whether your infrastructure can absorb attacks and failures and keep schools operating: segmented networks, protected devices, powered and cooled server rooms, and enough...

Why it matters

- On a flat network, malware on one student or staff device can reach servers, the business office and building systems; segmentation keeps an incident inside one zone so the rest of the district keeps teaching.
- Phones, bells, door access, cameras and intercoms depend on the server room and wiring closets, so a failed uninterruptible power supply (UPS) or an overheated closet becomes a safety and operations problem, not just an IT outage.
- Capacity and failover planning keep online state testing, cloud-based instruction and family communication running on the days they matter most, and E-Rate can fund much of the network equipment involved.

Flat networks turn one infected machine into a district-wide ransomware outage measured in lost instructional days, and a failed UPS or a saturated internet link during state testing is its own crisis.

What good looks like at each level

Level	What you would see	Artifacts that show it
1 · Initial	<p>Device protection is uneven, security updates happen when time allows, nobody has time set aside to look at logs, and USB drives and network gear have no specific protections.</p> <p>Moving up: Start defining: write down device protection processes, research the protective technologies that close your gaps, designate qualified staff to own protection measures and security updates, and put resilience needs into the budget cycle.</p>	<ul style="list-style-type: none"> • No current network diagram; staff, student, guest and camera traffic share one network • Endpoint protection installed on some machines but not reporting to any console • No log review time on anyone's calendar and no record of the last UPS battery replacement
2 · Repeatable	<p>The district is defining device protection processes, researching protective technologies, assigning qualified staff and budgeting for the gaps, while rules for removable media and network equipment are being decided.</p> <p>Moving up: Implement and document: protective technologies deployed, security updates installed on time, audit logs reviewed under a defined practice, removable media restricted by policy, and communications and control networks protected.</p>	<ul style="list-style-type: none"> • Written list of protection gaps with options and costs placed in the budget cycle or E-Rate Category 2 plan • Named staff responsible for device protection and security updates • Draft standards for USB storage and for hardening network equipment
3 · Defined	<p>Device protection is documented and in place, security updates install on time, audit logs are reviewed on a defined schedule, removable media is restricted, and the network is segmented.</p> <p>Moving up: Eliminate gaps and monitor: routinely monitor communications and control networks, take corrective action when weaknesses surface, evaluate defenses against evolving threats, and add automated checks that avert attacks rather than just record them.</p>	<ul style="list-style-type: none"> • Current network diagram showing staff, student, guest and building-system virtual local area networks (VLANs) with firewall rules between them • Endpoint protection console showing every managed device reporting, and Chrome policy blocking USB storage on student devices • Weekly log review tickets covering firewall, content filter and admin console alerts
4 · Managed	<p>Protection is deployed without significant gaps, defenses are reviewed against changing attacker techniques, weaknesses get corrective action, and automated checks block attacks rather than just recording them.</p> <p>Moving up: Measure and standardize: track uptime and protection KPIs and let results guide improvement, standardize protective technologies across every building, and use automation to sustain availability targets through adverse events.</p>	<ul style="list-style-type: none"> • Protective domain name system (DNS) filtering and automated firewall blocking of known-bad domains and addresses • CISA Cyber Hygiene scan reports with remediation tickets closed • Monitoring alerts on building-system and core network segments, with records of follow-up

Level	What you would see	Artifacts that show it
5 · Optimized	Protection is measured with key indicators such as uptime and coverage, the same protective technology runs in every building, and automation keeps services available through failures and attacks.	<ul style="list-style-type: none"> Dashboard tracking uptime, endpoint coverage and blocked threats, reviewed with leadership Standard firewall, switching and wireless configuration used in every building Tested failover, such as a second internet path or cellular backup for critical sites, with results recorded

Quick wins

Quick win and how	Cost	Effort	Usual owner
Enroll in a protective DNS service such as MS-ISAC's MDBR Check current MDBR availability and terms with MS-ISAC or your state, or turn on the protective DNS feature in your firewall or content filter, then point your internal DNS forwarders at it. Keep the block reports as evidence.	Low cost	Hours	Network and systems administrator
Move guest Wi-Fi onto its own isolated network Create a guest VLAN with client isolation that reaches only the internet, block it from staff, server and building-system networks at the firewall, and apply the same CIPA content filtering. Test from a personal phone that internal addresses cannot be reached.	Free	Days	Network and systems administrator
Verify endpoint protection is enabled and reporting on every managed device Compare the device list in Microsoft Defender or your antivirus console with your asset inventory and Intune or Active Directory, and fix any device that is missing, disabled or out of date. Include servers and domain controllers, which are easy to overlook.	Free	Days	Network and systems administrator
Test every UPS and calendar the battery replacements Run each UPS self-test, note runtime and battery install date, and confirm the management card can shut servers down cleanly during a long outage. Put battery replacement dates on the shared IT calendar and order replacements before they are due.	Low cost	Days	Network and systems administrator
Sign up for CISA's free Cyber Hygiene external vulnerability scanning Request service through CISA's Cyber Hygiene page or by emailing vulnerability@cisa.dhs.gov , return the authorization form with the district's public IP address ranges, and route the weekly reports to a shared IT mailbox. Open a ticket for every critical or high finding.	Free	Hours	Technology director

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

Common pitfalls

- Creating VLANs but allowing all traffic between them. Separate networks only help if firewall rules stop student and guest networks from reaching servers and the business office, so test it from a student device.
- Leaving cameras, HVAC controllers and door systems on the staff network. Building systems often run old firmware and default passwords; give them their own segment and limit who can reach their management pages.
- Buying protective technology and never watching it. Endpoint alerts and firewall logs that nobody reads stop nothing; block a recurring weekly hour for log review and record what was found.
- Assuming the UPS works because the light is green. Batteries age without warning and fail under load, so run self-tests, track install dates and replace on schedule.
- Ignoring capacity until testing day. Online state testing, device updates and video can saturate a connection at the same moment; check bandwidth reports before testing windows and pause large updates during them.

Evidence that proves it

- Network diagram showing VLAN segmentation and firewall placement
- MDBR or protective DNS enrollment confirmation and block reports
- Endpoint protection coverage report showing all managed devices enrolled and reporting
- UPS test and battery replacement records
- Weekly log review notes or tickets
- CISA Cyber Hygiene report with remediation tickets
- Bandwidth utilization report from before a state testing window

Who usually owns it

Technology director	Owns the network design, protective technology choices and resilience budget requests, and reports gaps to leadership.
Network and systems administrator	Maintains segmentation, endpoint protection, UPS and server room monitoring, and performs the weekly log review.
Business and finance officer	Plans E-Rate Category 2 and local funding for network equipment, UPS replacement and redundant connections.
Emergency management lead	Makes sure door access, cameras and intercoms run on protected, powered infrastructure and are covered in continuity plans.

Insurance relevance · High

Carriers ask whether the network is segmented, whether remote desktop or other admin services are exposed to the internet and whether firewalls are current, and some scan your public addresses from outside before quoting, so the answer gets checked.

- Are student, guest, staff, server and building-system networks separated, with restricted traffic between them?
- Is remote desktop or any other administrative service reachable directly from the internet?
- Are firewalls at every internet connection kept on current firmware, with rule sets reviewed on a schedule?
- Are backups of critical systems protected from the rest of the network?

Tip: Run CISA Cyber Hygiene or another external scan before renewal so your answer about exposed services matches what the carrier's own scan will find.

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 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

- Malicious Domain Blocking and Reporting (MDBR) (CIS) <https://www.cisecurity.org/ms-isac/services/mdbr>
- Cyber Hygiene Services (CISA) <https://www.cisa.gov/cyber-hygiene-services>
- Best Practices for Event Logging and Threat Detection (CISA) <https://www.cisa.gov/resources-tools/resources/best-practices-event-logging-and-threat-detection>
- #StopRansomware Guide (CISA) <https://www.cisa.gov/resources-tools/resources/stopransomware-guide>
- Cross-Sector Cybersecurity Performance Goals (CISA) <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>