PASS
Partner Alliance for Safer Schools

Partner Alliance for Safer Schools

White Paper: Digital Infrastructure Security Guidelines

The volunteers who make up the Partnership Alliance for Safer Schools (PASS) bring together their research and expertise from the education, public safety, and industry communities to develop and support a coordinated approach to make effective use of proven security practices for schools. The PASS team is also dedicated to developing white papers on specific, school-safety topics.

The content in these white papers may point to specific products, brands, or organizations as illustrations of how certain safety and security measures are implemented. PASS does not endorse specific products or brands. Together, the volunteers and partners of the PASS share a single vision: Making all schools safer is both achievable and urgently needed.

AUTHORS

Main Author: Will Knehr

Contributors: Eric Daniels, Kacey Sensich

KEY TOPIC

Digital security layer for cybersecurity and protection of digital assets and information for K-12 schools

PROBLEM SOLVED

K–12 schools have long lacked a comprehensive framework for addressing digital and cybersecurity challenges. The newly introduced layer within the PASS Guidelines fills this gap by applying to digital security the same tiered methodology used for physical security — offering a holistic, scalable approach tailored to the unique needs of educational environments.

RELEVANT PASS GUIDELINES SECTION/S

- Digital Infrastructure Layer
    - Digital Infrastructure Layer Checklist

- Policies and Procedures Component
- People (Roles and Training) Component
- Architectural Component
- Communication Component
- Access Control Component

MOST RELEVANT FOR

- School administrators and safety officers
- CIO, CISO, IT Directors
- School board members and other governance stakeholders
- Systems integrators and consultants

TIME TO READ

Approximately 15 minutes

Introduction

School safety now depends as much on reliable networks, identity systems, and logging as it does on doors, radios, and cameras. The PASS digital infrastructure guidelines were created to give districts a practical, staged path to build and sustain that backbone. We grounded the work in NIST frameworks and controls, calibrated it with real constraints from K-12 staff, and organized it into maturity-based recommendations that districts can adopt without boiling the ocean. The result is a reference architecture, a set of control families with clear rationales, and an implementation roadmap focused on resilience, privacy, affordability, and interoperability.

How the Digital Infrastructure Layer Was Developed

We started with the NIST Cybersecurity Framework as the backbone for the digital infrastructure layer. We used control language, implementation details from NIST SP 800-53 and 800-171, and standard safeguards familiar to schools through the CIS Controls. We then pressure tested theory against practice through structured interviews and workshops with technology directors, network administrators, facilities leaders, and front office staff from districts of different sizes and funding levels. Conversations focused on what repeatedly breaks during incidents, where budget and staffing pinch, which requirements are demanding to meet on legacy equipment, and what “good” looks like when you have only a few people wearing many hats. The guidelines reflect that reality: simple where possible, staged by maturity, and always written so a small team can execute.

Why Digital Infrastructure Matters in K-12

Every modern safety outcome rides on digital networks. If identity is weak, an attacker can unlock doors in software even when the perimeter hardware is solid. A single phished account can cascade into video, PA, or access control outages if networks are flat. If logs are missing or time is unsynchronized, it becomes impossible to reconstruct events or prove compliance. This guidance aims to turn infrastructure from a hidden liability into a safety multiplier so that cameras stream when they must, doors lock when they should, and administrators respond with confidence under pressure.

The Digital Infrastructure Layer

Digital infrastructure in this context includes identity and access management, directory and authentication services, wired and wireless networks, routing and firewalls, certificate and time services, endpoint and device configuration baselines, logging and telemetry, vulnerability and patch processes, backup and recovery platforms, and the cloud and hybrid services that underpin safety systems. The scope explicitly covers the connective tissue for physical security technologies such as access control, video management, visitor management, intercom, and emergency notification, as well as the interfaces to building automation where they intersect with safety and security.

We organized all recommendations around a few principles: student safety and continuity of learning as the priority, least privilege and defense in depth for every system that can influence safety, privacy-preserving practices by default, usability for lean teams, open standards and interoperability to avoid lock-in, and lifecycle thinking so today's decisions remain supportable five years out. Affordability is addressed through a maturity model so districts can do the most important things first and expand when funding allows.

The reference design is identity-centric and has zero trust in posture – even when implemented incrementally – identity, and single sign-on anchor authorization for users, administrators, and service accounts. Networks are segmented into at least four zones separating safety systems, administrative IT, instructional IT, and guest access, with tightly controlled east-west pathways and restricted outbound egress for safety devices. Remote access for vendors and staff is brokered through managed gateways with strong authentication and session recording, where feasible. Time, certificate, and DNS services are treated as critical dependencies, with authenticated NTP, internal PKI or automated certificate management for devices, and protective DNS to reduce command-and-control and phishing risk. Logging is centralized; safety systems forward syslog and API telemetry to a district repository so alerts can correlate identity, network, and application events. The architecture supports hybrid operation because many districts will run a mix of on-premises controllers and cloud services for years.

Control Families and the Rationale Behind Them

Governance and risk management establish ownership for safety-relevant systems, assign data classification and retention responsibilities, and link technology choices to written policies so they survive personnel turnover. Asset management and inventory are emphasized because you cannot defend devices you cannot see; this includes discovering unmanaged cameras, controllers, and radios that often appear during construction projects. Identity, authentication, and access control focus on multifactor authentication for administrators, unique credentials and role-based access for operators, SSO for staff to reduce password fatigue, and proper handling of service accounts so automations do not become the weakest link. Network architecture and segmentation isolate safety systems from student and guest networks, restrict device-to-internet communications to only what is needed, and enforce ACLs to keep compromised classroom devices from reaching door controllers or video servers. Secure configuration and hardening call for baseline templates, removal of default passwords, turning off unused services, enforcing TLS where supported, and standardizing time and certificates so logs align during investigations. Vulnerability and patch management balance firmware realities with risk, recommending a test-then-deploy cadence, maintenance windows aligned to the school calendar, and explicit handling of end-of-support devices. Logging, monitoring, and detection require safety systems to generate actionable telemetry and districts to retain it long enough to support incident response and mandated reviews. Data protection and privacy translate FERPA-aligned expectations into technical controls such as encryption of data in transit and at rest, where supported, least-retention video policies, and confidentiality guarding for exports and evidence handling. Email and web security are included because most compromises begin there; stronger filtering upstream reduces the chance that compromised credentials are used to pivot into safety systems. Backup, recovery, and resilience prescribe 3-2-1-style backups with at least one offline or immutable copy, tested restores, and explicit recovery point and time objectives for safety-relevant systems that differ from general IT. Third-party and vendor management defines minimum contractual expectations such as vulnerability disclosure channels, patch support timelines, secure remote support methods, and interoperability commitments. Physical-digital convergence covers practicalities like locking network closets, labeling and documenting patching to safety gear, UPS coverage to ride through short outages, and change management that crosses facilities and IT. Incident response and continuity provide role-based playbooks, contact trees, and tabletops that blend safety and cybersecurity, including manual fallbacks for locking, paging, and reunification when systems are degraded. Training and culture close the loop with role-specific drills for front office staff, principals, facilities, and IT so that people are ready when technology is not.

To help districts sequence investments, recommendations are grouped into four tiers. The foundational tier establishes inventory, basic segmentation, MFA for administrators, removal of default passwords, centralized logging of safety systems, and working backups that have been tested. The standard tier expands segmentation depth, implements SSO for staff, enforces certificate-based device onboarding where available, and formalizes maintenance windows and change control. The enhanced tier adds adaptive monitoring, immutable backups, fine-grained role design for operators, vendor remote access brokering, and formal tabletop exercises that include safety leadership. The advanced tier rounds out zero-trust patterns with continuous verification for high-risk actions, automated certificate lifecycle for safety devices, rigorous egress filtering, and documented metrics with board-level reporting. The tiers are written so districts can pause at a stable plateau if budgets tighten, without undoing progress.

Districts asked for a clear order of operations that fits a school calendar. The recommended sequence begins with visibility and control: discovering assets, documenting data flows, and setting time and certificates, since those steps enable safe change later. Next, implement administrative MFA and remove default passwords on safety systems while carving out basic network segments and egress controls. Then, centralize logging and test backups so there is a safety net before making more changes. With those guardrails in place, move to SSO, role-based access, and deeper segmentation, followed by vendor access hardening, vulnerability and patch cadence, and formal incident response planning. Finally, advanced measures such as immutable backups, automated certificate management, and continuous monitoring should be adopted. Each phase is scoped to be executable by a small team during scheduled windows, with rollback plans and communication templates prepared in advance.

Measures of Effectiveness

We defined a few practical indicators that any district can track to keep the program honest and visible: time to restore a safety system from backup to a ready state, percentage of safety devices with unique credentials and current firmware according to policy, percentage of safety systems forwarding logs to a central repository with synchronized time, percentage of privileged accounts covered by MFA and reviewed each term, and number of vendor remote access sessions established through approved gateways. These measures are simple to gather and create a shared language for progress with leadership and the board.

Because schools replace systems slowly, procurement is the chief lever to improve security over time. The guidelines include language that districts can add to RFPs requiring support for role-based access and SSO, secure logging and APIs, documented patch timelines, export controls that respect privacy, certificate-based encryption where feasible, and clear remote support methods. Interoperability is emphasized so districts can mix systems without forfeiting security; protocols, schemas, and time and certificate standards are called out to avoid brittle, vendor-locked integrations.

The guidance keeps privacy front and center. Retention policies for video and access logs are tied to articulated safety and legal needs rather than convenience. Exports are controlled through chain-of-custody procedures that prevent uncontrolled duplication. Access to sensitive data is constrained by role and logged for audit. Where analytics are used, the guidelines recommend a documented use case, stakeholder notification consistent with district policy, and periodic review so features introduced for safety do not drift into inappropriate surveillance.

We framed resilience as maintaining critical safety functions even when the digital layer is degraded. That means planning for manual door overrides, fallback paging methods, and paper visitor management when systems are down. It also means designing power and network infrastructure to fail gracefully, using UPS and orderly shutdowns, and testing the ability to operate with limited bandwidth or cloud outages.

What Changed After Piloting and Stakeholder Review

Stakeholder feedback drove several essential shifts. We simplified the initial segmentation model so that smaller districts could implement it with existing switches. We replaced expensive SIEM assumptions with a “start where you are” logging approach that supports low-cost collectors and staged retention. We adjusted firmware guidance to reflect classroom calendar realities, favoring predictable windows over theoretical immediacy. We added specific identity patterns for service accounts because districts repeatedly cited automations as a blind spot. Finally, we elevated procurement language to the main body of the guidance after multiple districts noted that RFPs are their best leverage to improve posture without increasing headcount.

Summary

What does this mean for district leaders?

Leaders do not need to become network engineers to make progress. They can insist that safety-relevant systems have owners, that success is measured with a short set of meaningful indicators, and that purchases meet baseline security expectations. They can require that any safety exercise include a digital failure mode and that every planned change has a rollback and communication plan. Most importantly, they can protect the sequencing of work so technology staff are not forced into risky shortcuts.

Digital infrastructure is now inseparable from school safety. The PASS digital infrastructure guidelines give districts a pragmatic path to modernize that backbone, grounded in NIST and tempered by the lived experience of K-12 staff. Start with visibility and identity, separate what must never touch, log and back up what matters, and practice the response you hope you never need. Do those things in order, and schools will be safer, even on lean budgets and small teams.

References

https://www.nist.gov/cyberframework

https://www.cisa.gov/