Introduction

Purpose

These Guidelines establish recommended operating standards for safety and communications technologies to be implemented in compliance with Alyssa's Law and serve as a model for future legislation. Alyssa's Law mandates the deployment of panic alert systems in schools to enable immediate notification of law enforcement, first responders, and campus occupants during emergencies. While the law establishes a critical requirement, there remains a pressing need to ensure that the tools used to meet its mandate are consistent, reliable, and capable of performing under the urgent demands of a crisis.

This document establishes clear Guidelines for qualifying technology solutions. By defining technical, operational, and performance recommendations, these Guidelines support school districts, technology providers, and public safety agencies in selecting and deploying tools that provide meaningful protection. It ensures that solutions are not only legally compliant but also effective in real-world emergency scenarios, minimizing response times, reducing confusion, and maximizing safety outcomes for students, staff, and first responders.

Ultimately, the goal is to create a standardized foundation that fosters innovation while safeguarding public trust and student lives. The Guidelines promote interoperability, accountability, and long-term sustainability across diverse educational environments and funding levels. These Guidelines also support policymakers in evaluating solutions fairly and consistently, helping states implement Alyssa's Law with integrity and impact.

Intended Use

This document highlights a cross-functional, multi-disciplinary approach to reviewing, analyzing, selecting, designing, deploying, operating, and maintaining systems, technology solutions, and supporting processes to enhance school safety. Achieving effective results requires coordinated collaboration among educational leaders, emergency responders, technology specialists, operational staff, and other stakeholders to ensure cohesive, reliable, and life-saving outcomes.

This guidance supports school districts, administrators, public safety partners, and technology providers (Purchasing Entity) in selecting and deploying solutions in compliance with Alyssa's Law. Its main goal is to maximize the safety benefits and operational value of emergency communication and alert systems by promoting best practices from design to implementation. In educational settings, technology and safety decisions are often made within isolated departments, such as IT, security, facilities, or school administration, which can inadvertently create blind spots, introduce vulnerabilities, and reduce system effectiveness.

While this document uses technical language to clarify requirements and ensure specificity for cross-functional teams, it is not intended to discourage participation by non-technical stakeholders. These details are included to remove ambiguity, prevent confusion, and support meaningful collaboration among all participants in the school safety ecosystem.

Scope

These Guidelines apply specifically to the alert activation and signaling apparatus used in K–12 educational environments as mandated by all permutations of Alyssa's Law. They are also recommended for higher education institutions seeking to enhance campus safety. The Guidelines cover the essential tools and technologies for initiating, transmitting, and managing emergency alerts intended to summon a law enforcement response and alert campus occupants during active threat situations. They serve as a baseline to ensure that all solutions deployed in educational settings meet fundamental operational and performance expectations.

The scope encompasses various activation and alerting modalities, including hardware-based solutions (e.g., fixed panic buttons and wearables) and software-based solutions (e.g., mobile apps, desktop alert systems, and cloud-based platforms). It includes proprietary systems that may use closed architectures, as well as traditional solutions that rely on more conventional communication methods. The intent is to be technology-agnostic while ensuring each solution meets minimum functional criteria and enables real-time, direct communication with first responders.

Also included in the scope are the supporting components necessary for the alert systems to operate effectively, such as network infrastructure, backup power, and integration with public safety access points (PSAPs), 911 centers, and on-campus security systems. These elements should be evaluated within the overall system to ensure continuous availability, failover resilience, and seamless interoperability across diverse operational environments.

It is important to note that while these recommendations provide guidance for alerting systems, they do not prescribe any single manufacturer, model, or platform. Instead, they establish performance and reliability thresholds that all compliant solutions must meet or exceed, enabling school districts and institutions of higher education to select technologies that fit their operational needs, physical layouts, staffing models, budget constraints, and emergency dispatch environment, without compromising effectiveness or safety.

Objective

The objective of these Guidelines is to establish a clear and consistent set of minimum requirements that technologies used to fulfill Alyssa's Law should meet to be considered effective, reliable, and suitable for

deployment in K–12 educational environments. These recommendations guide school districts, technology providers, and public safety agencies in evaluating, selecting, and implementing alert signaling systems that deliver immediate and actionable notifications to law enforcement during life-threatening emergencies.

By defining essential operational, technical, and integration benchmarks, these Guidelines aim to ensure that all compliant solutions provide measurable value in reducing response times, enhancing situational awareness, and improving outcomes during critical incidents. It further seeks to promote accountability, foster innovation, and support equitable access to effective school safety technologies, regardless of a school's size, location, or funding level.

Guiding Principles

The implementation of Alyssa's Law demands more than the presence of alerting systems—it requires that these systems perform reliably, inclusively, and with maximum impact in time-sensitive, high-stakes scenarios. The following guiding principles outline the core attributes that any alert signaling technology should demonstrate to ensure it serves its intended purpose: saving lives through faster, smarter, and more coordinated emergency response.

Time=Life℠ - Rapid Initiation and Dissemination of Alerts

In a life-threatening emergency, the speed of alert activation and transmission is the single most critical factor; time and urgency directly translate to saving lives. Alert systems should support near-instantaneous activation and feature clear, simple user interfaces that enable one-touch or one-step initiation. Once triggered, alerts should be disseminated throughout campus and to designated recipients, including on-site personnel, local law enforcement, and 911 Public Safety Answering Points (PSAPs), within seconds. The system should eliminate delays caused by user confusion, multi-step processes, or signal bottlenecks. The standard of speed ensures the fastest possible connection between a person in distress and those responsible for protecting them.

Rationale:
Emergencies escalate quickly. A system that minimizes activation steps and ensures rapid transmission can prevent delays that cost lives.

Reliability - High System Uptime and Fault Tolerance

An alert system is only effective if it works when needed. Systems should be engineered with reliability as a core function, including a documented 99.9% uptime, redundant power sources (e.g., battery or generator backup), and the ability to operate during network outages or infrastructure disruptions. Fault tolerance should be built into both hardware and software components to prevent single points of failure. System health should be continuously monitored, with automatic alerts generated for malfunctions or performance degradation.

Example: Resilience Table

Category Examples	Backup Examples
Internet Connectivity	Secondary Internet Line, Secondary Cellular Connection, Radio Communication Option
Power Supply	Battery Backup, Generator Backup, Uninterruptible Power Supply (UPS)
Hardware	Redundant Servers, Mirrored Storage, Hot Swappable Components
Software	Failover Clusters, Load Balancing, Automatic Rollbacks
Data Storage	Off-site Backups, Cloud Redundancy, Data Replication
Geographic Redundancy	Multiple Data Centers, Distributed Systems
Human Factors	Redundant Staffing, Cross-Training, Clear Communication Protocols

Rationale:
An alert system that fails during a crisis leaves schools vulnerable and erodes public trust. Built-in redundancy ensures dependability under adverse conditions.

Accessibility - Inclusive Design for All Users

All users, regardless of physical ability, role in the school, language proficiency, or level of technological comfort, should be able to operate the alert system effectively under stress. Interfaces should be designed to meet universal accessibility standards, including compliance with the Americans with Disabilities Act (ADA). This includes intuitive navigation and tactile or visual confirmations. Emergency protocols should not depend solely on complex software or on the availability of mobile devices, ensuring that all building occupants can use the system equally.

Rationale:
Any adult in a school, teacher, custodian, aide, guest, or administrator may need to activate an alert under stress. Accessibility ensures everyone can use the system effectively, regardless of role or ability.

Training & Preparedness - Regular Drills and Proficiency

Even the most advanced technology is ineffective without proper human integration. Comprehensive training for all faculty and staff is crucial to ensure that every individual who services school property is proficient in operating the alert system and understands emergency protocols. This includes regular reminders, access to key information, hands-on guidance, and routine simulations to build familiarity and confidence in high-stress

situations. Schools & Districts should conduct functional tests and coordinated responder drills; systems must include dashboards for health/status and tamper-proof activation logs for audits.

Rationale:
Even the best technology is ineffective if staff hesitate or make errors. Regular practice builds confidence and ensures quick, correct use during emergencies.

Interoperability - Integration with Safety and Emergency Systems

Alert systems should function as part of a broader safety ecosystem, not in isolation. Ideally, although not mandatory, the system should integrate with other essential communication tools. These tools may include public address and intercom systems, video surveillance, access control, fire alarms, mass notification platforms, and infrastructure for first-responder dispatch. Systems should support industry-standard protocols (such as CAP—Common Alerting Protocol) and provide APIs or data-exchange capabilities to ensure smooth communication across platforms. This interoperability enhances situational awareness and reduces delays caused by fragmented systems or manual information relay.

Rationale:
Fragmented systems create delays and miscommunication. Interoperability ensures coordinated response and real-time situational awareness.

Accountability - Logging, Auditing, and Review

The system should include a robust back-end for logging all activity to support transparency, effectiveness, and legal compliance. This includes timestamps for alert initiation, delivery confirmations, user actions, escalation events, and system health checks. These logs should be accessible through secure administrative dashboards and exportable for post-incident review or compliance reporting. The ability to audit system performance helps identify failure points, refine emergency protocols, and build trust among staff, families, and responders.

Rationale:
Audit trails improve transparency, support post-incident reviews, and help refine emergency protocols. This builds trust among staff, families, and responders.

False Positives - Managing Legitimate Events

Policies for addressing false positive security events are also essential. Schools should develop, maintain, and regularly test clear protocols for verifying alerts and, when appropriate, canceling false alarms without causing unnecessary panic or deploying emergency services. These policies should include steps for immediate internal verification, clear communication channels to responders, and processes for post-event review to

identify and mitigate causes of false positives. Such measures ensure that valuable resources are not diverted unnecessarily and that trust in the system remains high among staff and first responders.

Rationale:
False positives waste resources and undermine credibility. Clear, rehearsed procedures maintain trust and ensure readiness for real emergencies.

Scalability - Effective Across Diverse Environments

The technology should be scalable to serve institutions ranging from single-building elementary schools to sprawling high school campuses or multi-site districts. Whether the school is urban or rural, affluent or under-resourced, the system should maintain its core functionality without requiring excessive customization or resources. It should support phased implementation, enable modular expansion, and operate within modern and aging infrastructure environments. Affordability and adaptability are key to achieving equitable implementation across diverse educational settings.

Rationale:
Every school deserves reliable protection. Scalable systems promote equity, enabling districts to implement solutions sustainably across diverse contexts.

Privacy and Security - Protecting Data and Systems

Safeguarding student and staff information is paramount, necessitating robust privacy and cybersecurity measures for alert systems. Solution Manufacturers and Providers (vendors) should implement Cybersecurity Architecture best practices across the entire product and service lifecycle, incorporating Secure by Design and Secure by Default principles during development and manufacturing.

Systems should ensure data encryption at rest and in transit, utilize secure access controls for user authentication, and log all integrity events. Continuous monitoring for unauthorized or malicious activities and abnormalities is essential. Adherence to industry best practices is mandatory for Data Encryption, Identity Management, Role-Based Management, Least Privilege Access, Secure Access, and Patch Management. Vendors should also demonstrate compliance with federal laws like the Family Educational Rights and Privacy Act (FERPA) and the Children's Online Privacy Protection Act (COPPA).

Regular cybersecurity vulnerability testing is crucial, as is a documented incident response protocol for breaches. Customers (e.g., Schools) should understand and comply with their responsibilities under the Customer Shared Responsibility Model (CSRM) and apply Cybersecurity Architecture best practices for Defense-in-Depth, Identity Management, Role-Based Management, Least-Privilege Access, and Patch Management.

These guiding principles collectively establish recommended technology practices that not only fulfill the requirements of Alyssa's Law but also uphold the ethical and operational responsibilities of those tasked with protecting school communities.

Example: Cybersecurity Architecture Best Practice

Principle	Description
Defense in Depth	This principle involves using multiple layers of security controls to protect an organization's assets. It ensures that if one layer is compromised, the others remain intact, preventing unauthorized access. Examples include firewalls, encryption, and multi-factor authentication.
Least Privilege Access	This principle ensures that users are granted only the minimum level of access necessary to perform their job functions. This reduces the risk of insider threats and limits the potential damage from compromised accounts.
Security by Design and Default	"Secure by Design" means that security considerations are embedded from the outset of a project, from initial requirements and architecture design through development, testing, and deployment. "Secure by Default" means that the system's out-of-the-box configuration is the most secure state, with non-essential features and ports disabled.
Separation of Duties	This principle divides critical tasks among multiple individuals to prevent errors, fraud, and unauthorized actions. By ensuring no single person has end-to-end control over a sensitive process, SoD introduces a system of checks and balances that enhances accountability and reduces risk.
Zero Trust Architecture	This principle assumes that no user or device, whether inside or outside the network, should be automatically trusted. It requires strict identity verification for every user and device trying to access network resources, minimizing the risk of unauthorized access and lateral movement within the network.
Simplicity (KISS Principle)	This principle advocates simple, straightforward security solutions. Complex systems can introduce vulnerabilities, making it harder to manage and maintain security effectively. Simplicity helps reduce the attack surface and improve overall security.

Example: Customer Shared Responsibility Models

Vendors and Customers share control over technology; therefore, security is a shared responsibility. The following are examples of CSRMs based on the installation and hosting arrangements.

Type: SaaS

Description: Software as a Service model, cloud-hosted by the vendor

	Responsibility
Identity	Customer
App Configuration	Vendor
Data Confidentiality	
App SSDLC	
App Updates	
Data Security	
Cloud Security	
Network Security	
Infrastructure	
Physical	

Type: On-Prem

Description: On-Premise, self-hosted by the customer

	Responsibility
Identity	Customer
App Configuration	Vendor
Data Confidentiality	
App SSDLC	
App Updates	
Data Security	
Cloud Security	
Network Security	
Infrastructure	
Physical	

Rationale:
Alert systems hold sensitive information and form part of critical safety infrastructure. Strong cybersecurity safeguards protect privacy, maintain functionality, and reinforce trust.

Core Technology Recommendations

To fulfill the intent and statutory mandates of Alyssa's Law, panic alert systems deployed in educational environments should meet specific performance, design, and functional standards. These systems should enable immediate, reliable, and discreet signaling of emergencies, particularly active threats, to law enforcement and designated responders. This section defines the recommended technical and operational practices, along with enhancements that enhance safety and functionality.

Alert Initiation

Purpose and Functional Mandate

Alert initiation is the foundational capability of any emergency response system. It should allow any authorized user to instantly, discreetly, and confidently activate a panic alert under duress. The alert should notify on-site and off-site first responders and provide the user with confirmation that it has been triggered. The system should always alert law enforcement and fully support configurable silent, audible, and visual modalities to enable context-specific alert escalation within the campus.

Initiation Modalities

Depending on the Purchasing Entity's specific needs, the entity may wish to consider systems that offer multiple activation modes: fixed-position panic buttons, staff-wearable panic buttons, software-based desktop/mobile activation, and optional voice activation, each with anti-false-trigger safeguards to ensure redundancy, accessibility, and reliability. The following three initiation modalities are recommended for minimum compliance:

Building-Mounted Panic Buttons

- Deployment: Should be installed in all instructional spaces, administrative offices, cafeterias, gyms, libraries, health clinics, locker rooms, public spaces, and other designated areas.
- Design Requirements:
    - Hardwired or wireless with secure, tamper-resistant casings (minimum IP54).
    - Clearly identifiable but optionally concealable.
    - One-touch activation with tactile or visual confirmation.
- Performance:
    - Should initiate system recognition in <1 second and notify authorities in < 10 seconds.
    - Battery backup or alternate power is required

Rationale:
Outside organizations frequently use school buildings outside school hours, including for adult education programs, faith-based groups, and summer camps. Staff from these groups are not school employees and may not be issued wearable panic buttons. For this reason, installing fixed-position panic buttons should be considered so that all authorized campus occupants can activate the alert system during an emergency.

Wearable Panic Devices

- Design: Should be worn comfortably and unobtrusively as a lanyard, wristband, ID badge, or clip-on device.
- Build Standards:
  - Secure pairing to individual users or roles.
  - Minimum battery life of 12 months, or rechargeable, providing >24-hour operating time.
  - Wireless with secure, tamper-resistant casings (minimum IP65).
- Connectivity:
  - Should operate reliably throughout all indoor locations on campus and within 300+ feet of the exterior of each facility, using auto-mesh network extension where available and fallback to alternate wireless protocols where required.
- User Interface:
  - Different alerts can be activated in various ways, such as by pressing a specific designated button, utilizing a sequence of buttons, or pressing a button a specified number of times.
  - Feedback via vibration (tactile) and/or light
  - Should offer silent and audible/visual alert modalities, including the ability to escalate a silent alert to audible/visual.

Rationale:
Wearable panic buttons allow staff to initiate an alert immediately from any location without needing to reach a fixed-position device. Mobility is essential because emergencies are unpredictable and often unfold while staff are moving between classrooms, supervising common areas, or responding to students. Wearables may reduce activation time and provide a more immediately accessible way for staff to request assistance during an active threat.

Software-Based Activation (Mobile & PC)

- Compatibility: iOS, Android, Windows, macOS, browser-based platforms
- User Interface:
  - Simple, clearly marked panic button.
  - Single action (click/tap or keyboard shortcut).
  - Visual confirmation upon activation.
  - Should offer multiple silent and audible/visual alert modalities, including the ability to escalate a silent alert to audible/visual.

- Security:
  - Role-based access, SSO or MFA login, and end-to-end encryption.
  - Optional Voice Activation
- Capability: Users may trigger alerts using a customizable wake phrase (e.g., "trigger emergency alert").
- Controls: Requires anti-false activation logic (e.g., phrase + voice recognition, duration thresholds).

Rationale:
Mobile or desktop app activation provides an additional, low-cost layer of protection for individuals who are not school employees and therefore may not be issued wearable panic buttons. This includes after-hours staff, contractors, community groups, and other authorized building users. While not intended to be the primary activation method, app-based alerts provide an accessible option that can extend emergency activation to temporary or rotating personnel, enhancing overall coverage without incurring high costs or operational burdens.

Alert Modalities

The default action across all modalities for every system must be to immediately initiate a call to law enforcement. Furthermore, selected solutions should provide discreet, silent activation; simultaneous audible and visual activation; and the ability to escalate from a silent to an audible/visual state.

This alert should:

- Immediately and discreetly notify:
  - Local law enforcement or emergency dispatch (via 911 / PSAP).
  - Designated on-campus safety personnel.
  - District-level emergency operations, if applicable.
- Provide no local signal to the surrounding environment unless escalation is required.
- In addition to silent alerts, systems should include programmable audible and visual alert capabilities, such as:
  - Audible: Automated tones through intercom, desktop speakers, or dedicated alarms.
  - Visual: Flashing strobe lights, digital signage override, and full-screen desktop alerts.
  - These alerts should be optional, configurable by authorized personnel, and usable for broader lockdown or evacuation procedures where overt notification is necessary.

Rationale:
All systems should support multiple alert modalities to ensure the right response for different types of emergencies. A silent panic alert should be the default across all activation methods because it allows staff to discreetly notify law enforcement, on-campus safety personnel, and district emergency operations without signaling to the surrounding environment. This is essential in situations such as a suspected weapon, a hostage scenario, or any incident where audible or visual notification could escalate the threat. Silent activation enables responders to mobilize, coordinate, and take protective action before the situation intensifies.

Systems should also include configurable audible and visual alerts for scenarios requiring overt notification, such as an active assailant, a large-scale threat, or an immediate lockdown or evacuation. Audible tones, strobes, and desktop or signage overrides ensure that everyone on campus receives clear, rapid direction to take cover or move to safety. Together, this multimodal approach ensures alerts are matched to the specific emergency, maximizing safety for students, staff, and responders.

Engineering and Build Specifications

To ensure durability, effectiveness, and real-world reliability, all alert initiation components should meet the following standards:

- Environmental Resistance
  - Indoor devices: IP54 or higher for dust- and splash-resistance.
  - Outdoor devices: IP65 or higher
  - Wearable devices: IP65 or higher
- Activation Responsiveness:
  - Signal recognition within ≤1 second.
  - End-to-end 911/PSAP notification delivery within ≤10 seconds under normal network conditions.
- Power & Longevity:
  - All devices should include either direct power or a battery backup (with a minimum of 12 hours of operational capability).
  - Replaceable batteries should support at least 12 months of operation and provide low-battery warnings.
  - Rechargeable devices should fully charge within 2 hours and provide low-battery warnings.
- Durability:
  - Tested to withstand shock, vibration, and drop conditions per MIL-STD-810G or equivalent.
  - Panic buttons should function for at least 1,000 activations without failure.

Rationale:
Devices may be subject to stress, damage, or limited infrastructure during a crisis. Durable, responsive engineering ensures reliability when it matters most.

Redundancy and Failover

The alert initiation system should feature multiple communication paths to ensure signal delivery under adverse conditions. Required redundancy features include:

- Redundant Connectivity: The selection of primary, secondary, and even tertiary communications protocols, including Wi-Fi, LTE/5G, RF mesh, LoRaWAN, Bluetooth, or DECT, should be carefully aligned with the unique environment of each facility. This alignment is important for optimizing continuous failover capability and operational resilience.
- Offline mode: Systems should be designed to degrade safely and maintain essential life-safety functionality during partial or total loss of WAN, internet, or cloud connectivity. At a minimum, systems should support local survivability, allowing authorized users to initiate alerts and deliver on-campus notifications (including audible and visual alerts) in accordance with policy-configured escalation rules, even when cloud services are unavailable. During connectivity outages, local system components (e.g., gateways, controllers, endpoints, or applications) should continue to buffer and queue event logs, operational metrics, and fault conditions with accurate time-stamping, and should automatically synchronize stored data once connectivity is restored. Where available, systems should attempt external notification using any remaining communication pathways; when external connectivity is unavailable, local alerting and logging should continue to operate to support occupant safety and post-incident review.
- System health monitoring: Central dashboard for real-time device status, monthly performance testing, and alerts for unresponsive or failing components.
- Redundant mechanisms: If one modality (e.g., a wearable) fails or is inaccessible, others (e.g., a wall-mounted button or a software client) should remain functional.

Rationale:
Emergencies may include nefarious or incidental disruptions to power or networks. Redundancy ensures alerts still reach responders and warn campus occupants, even if one communications pathway fails.

Recommended Enhancements

While not required for compliance, the following features are recommended to increase system performance, versatility, and incident response quality:

- Geo-location tagging: Systems should support accurate identification of alert origin using appropriate location methods based on the activation modality. For wearable and mobile-device-initiated alerts, this may include GPS, BLE proximity, and wireless triangulation. For fixed or building-mounted panic buttons, the location should be derived from addressable or mapped IoT endpoints associated with known rooms or zones.

- Bi-directional communication: Allow school administrators or responders to send confirmation or guidance back to the initiator.
- Contextual escalation: Enable staff to choose between silent panic alert, lockdown, secure, evacuation, and possibly medical emergency alerts from a single interface.
- Duress activation: Coded inputs or sequential button presses for discreet activation under coercion.
- Role-based alert routing: Automatically notifies the appropriate response group (e.g., SRO, principal, district police) based on the incident type and location.
- Cloud-on-prem hybrid sync: Maintain localized failover operation with automatic cloud synchronization once external connectivity is restored.

Rationale:
These enhancements improve situational awareness, empower staff under stress, and streamline response coordination. They are not required, but add meaningful value where feasible.

Solution Guide Administration

Revision Cycle

To ensure this guidance remains aligned with evolving technology, industry best practices, and school safety needs, these Guidelines shall be reviewed and updated every 2 years.

The review process will include:

- Evaluation of advancements in school safety technologies and emergency communication systems
- Assessment of changes in federal, state, and local policy or funding related to school safety
- Review of implementation feedback and performance outcomes from schools and districts
- Consultation with subject-matter experts, safety professionals, emergency response agencies, and education stakeholders

At the conclusion of each review cycle, revisions may be issued to reflect current capabilities, emerging technologies, and lessons learned from real-world deployments. Interim updates may be published if significant technological, regulatory, or safety developments warrant accelerated action.

This structured, iterative approach ensures that the Guidelines remain evidence-based, relevant, and responsive as the safety technology landscape and education environment evolve.

Continuous Improvement Feedback Loop
A formal feedback mechanism will be made available to support this revision cycle and foster continuous improvement.

This mechanism will allow schools, districts, technology providers, and other stakeholders to submit suggestions, report challenges, and share best practices related to the implementation and effectiveness of these Guidelines.

Feedback Submission Process:

- **Online Portal:** A dedicated online portal will be provided for submitting structured feedback, including specific suggestions for Guideline revisions, reporting observed gaps or challenges, and sharing successful implementation strategies.
- **Annual Stakeholder Forum:** A forum will be convened annually to facilitate direct discussion and gather qualitative feedback from diverse stakeholders. This forum will also serve as a platform for sharing updates and discussing emerging trends.

All submitted feedback will be systematically categorized, analyzed, and considered during the biennial review. Key themes, identified challenges, and promising innovations will directly inform potential revisions and updates to ensure the Guidelines remain practical, effective, and responsive to the needs of the educational community.

Revision Categories

- Major Revision: Substantive updates, new requirements, structural changes
- Minor Revision: Clarifications, formatting changes, non-substantive edits
- Interim Update: Time-sensitive modification before scheduled review

Revision Log

This document is maintained as a living set of guidelines. Revisions reflect evolving best practices, technology capabilities, and stakeholder input. Version numbering distinguishes substantive changes from editorial updates. This document is maintained under a scheduled two-year review cycle with interim updates issued as needed. All revisions will be recorded in the log below.

Version:	Date:	Description of Changes:	Section(s) Impacted:
1.0	02/06/2026	Initial Release of Baseline Publication	All

Attribution and Contributing Expertise

This document was developed through the collaborative efforts of the Make Our Schools Safe (MOSS) Advisory Board Subcommittee on Alyssa's Law Legislation, Safety, and Technology. The guidance reflects input from a broad range of contributors across the school safety ecosystem, including subject-matter experts in emergency communications, school security, and public safety technology; emergency response professionals with experience in law enforcement, fire services, and 911/PSAP operations; education stakeholders such as district administrators, school security personnel, and instructional leaders; and technology and industry advisors specializing in safety infrastructure, communications systems, information security, and compliance.

The document was drafted and reviewed under the subcommittee's direction, with editorial oversight and contributions from members representing legislative, public safety, education, and technology disciplines. Policy and legislative advisors supporting the advancement of Alyssa's Law and related initiatives also provided insight. Collectively, these perspectives help ensure the guidance reflects current best practices, practical implementation considerations, and the evolving technology landscape supporting school safety and emergency response.

Plain-Language Notes

This guide explains key technology terms used in the Core Technology Recommendations section. The goal is to ensure every stakeholder, not just IT, can participate confidently in school safety planning and decision-making.

Alert Initiation

- Initiation Modalities - Ways to trigger an alert (button, wearable, app, voice)
- User Feedback - Confirmation that the alert was sent (vibration, tone, screen message)
- Silent Notification - Alert goes out quietly, so the threat is not alerted

System Reliability & Uptime

- 99.9% Uptime - System works virtually all the time (less than ~9 hours downtime per year)
- Redundancy - Backup communications, backup power, backup servers
- Failover - The system automatically switches to backup if something breaks

Accessibility

- Universal Access / ADA Compliance - All people must be able to use the system, including those with disabilities

Cybersecurity

- Encryption - Data is secured during storage and transmission
- Least Privilege - Users only get access they need, nothing more
- Audit Logs - System records who did what and when
- Zero Trust - Every access request is verified, no automatic trust
- Secure by Design / Default - System is secure from the start and ships with the safest settings enabled

Network & Infrastructure

- Cloud-Hosted (SaaS) - The system runs on secure online servers rather than on school servers.
- On-Premise System - System runs on school or district-owned hardware
- Patch Management - Regular security and performance updates are applied to keep the system safe

Performance Benchmarks

- <1 second latency - Alert processes instantly in under 1 second
- <10 seconds law-enforcement notification - Police receive an alert within 10 seconds

False-Trigger Management

- Verification Protocol - Steps to confirm false alarm without panic
- Post-Event Review - Quick debrief to improve future cases

Scalability & Compatibility

- Scalable - Term indicates that a system works similarly for one school or the entire district; this term may also describe a system whose capabilities may be expanded with additional functionalities and/or components.
- Interoperable - Works with other systems, including, but not limited to, radios, PA systems, cameras, access control, etc.

Glossary

Access Control System
A security system that manages and restricts access to buildings or rooms using devices such as keycards, badges, fobs, or biometric authentication.

Activation Device
A physical or digital tool used to trigger an emergency alert (e.g., button, wearable, app interface).

ADA Compliance
Meeting accessibility requirements under the Americans with Disabilities Act to ensure all staff can use safety systems.

Alert Escalation Path
The sequence of notifications and actions taken once an alert is triggered (e.g., internal team → 911 → district leadership).

Alert Latency
The time between alert triggering and its receipt by responders.

Alert Modalities
Different ways an alert can be triggered (e.g., via a wearable, desktop, wall button, mobile app, or voice command).

Audit Log
A secure record-keeping system for documenting system activity, such as alert triggers, logins, and configuration changes.

Chain of Custody (Digital)
Process for handling digital alert logs and evidence in a secure, traceable manner.

Cloud-Hosted / SaaS (Software as a Service)
A system hosted on secure off-site servers and accessed via the internet, managed by the vendor.

Cross-Functional Team
A group that includes school leaders, IT, emergency services, facilities, teachers, and safety staff working together on safety planning.

Cybersecurity
Technologies, processes, and practices designed to protect networks, systems, and data.

Defense in Depth
Security strategy using multiple layers of controls (e.g., firewalls, MFA, encryption, monitoring).

Direct-to-PSAP / Direct-to-911
System capability to send alerts directly to 911 dispatch centers without intermediary steps.

Drill Protocols
Standard procedures for practicing emergency response and testing systems.

Emergency Response Plan (ERP)
Formal plan outlining procedures for emergencies, including communications, evacuation, and law enforcement coordination.

Encryption (At Rest / In Transit)
A security process that converts data into an unreadable form while it is stored and during transmission.

Endpoint Device
Any device connected to the network that can trigger or receive alerts (e.g., wearable, tablet, intercom panel)

Failover
Automatic switch to a backup system, network, or power source if the primary system fails.

False Alarm Management
Procedures to identify, respond to, and document unintended activations.

First Responder
Police, fire, EMS, or emergency personnel who respond to school emergencies.

Geo-Location Services
Technology that identifies where an alert is triggered and provides precise location data to responders.

Grant Funding
Financial support is provided by public programs or private entities to support safety upgrades.

Incident Command System (ICS)
A standardized emergency management structure used by first responders to coordinate operations.

Interoperability
The ability of different systems (e.g., radios, PA systems, door locks, cameras) to work together.

IoT Device (Internet of Things)
An internet-connected device used in safety systems, including sensors, cameras, and alarms.

Least Privilege Access
Security principle limiting user access to only what is necessary for their role.

Local Notification
Alerts that notify internal staff or responders within the school or district.

Mass Notification System (MNS)
Platform for delivering messages to large groups during emergencies (staff, parents, students, responders).

Multimodal Alerting
Ability to activate and annunciate alerts in different formats based on the type of emergency. Activation: wearable panic button, building-mounted panic button, software-based alert activation; Annunciation: silent alerts, audible alerts, visual alerts, tactile alerts (vibration).

Multi-Factor Authentication (MFA)
Security that requires two or more credentials to verify identity.

Network Redundancy
Multiple network connections to prevent communication failure (e.g., wired + cellular backup).

NENA Standards
National Emergency Number Association guidelines for 911 communication systems.

On-Premises System
The system is hosted on local district servers and maintained by district personnel.

Operational Continuity
Ability to maintain school functions and communications during emergencies.

Panic Alert System
A system enabling immediate requests for emergency assistance.

PSAP (Public Safety Answering Point)
Official 911 call center that receives emergency alerts and dispatches responders.

Penetration Testing
Security testing that simulates cyberattacks to identify vulnerabilities.

Redundancy
Backup systems, networks, or power supplies that ensure operations continue if one component fails.

Role-Based Access Control (RBAC)
Permissions configured based on job role (e.g., teacher, admin, law enforcement).

Scalability
The system can expand from one school to an entire district without performance loss

Secure by Design / Default
Security is built into systems from the start and enabled by default.

Silent Alert
Discreet alert sent without audible or visible indicators.

Standard Operating Procedure (SOP)
Documented steps guiding emergency and system operations.

Tamper Alert
A notification is triggered if safety equipment is interfered with or disabled.

Threat Notification Protocol
Defined procedure for communicating emergency information to responders and staff.

Uptime
Percentage of time the system remains operational (target ≥ 99.9%).

Universal Accessibility
Ensuring emergency systems are accessible to all occupants, including those with disabilities.

Vendor Due Diligence
Evaluation process to ensure vendors meet safety, security, and legal requirements.

Voice-Activated Alert Triggering
Ability to trigger emergency alerts with specific spoken commands.

Zero Trust Architecture
The security model requires verification of every access request: "Trust nothing; verify everything."

