

PASS
Partner Alliance
for Safer Schools

Safety and Security GUIDELINES

for K-12 Schools

About PASS ***3***
Introducing The All-New 7th Edition 3
Scope 5
Structure Of The PASS Guidelines 6
Layered Security 6
Baseline Practices And Obligations 8
Recommended Uses 10
Risk Assessment - A Prerequisite 12
Layers Of Protection 15
Safety And Security Components 16
Using The PASS Guidelines To Formulate A Comprehensive Security Plan 18

District-Wide Layer ***21***
District-Wide Layer Checklist 22
Policies And Procedures Component 24
People (Roles And Training) 33
Architectural Component 33
Communication Component 35
Access Control Component 37
Video Surveillance Component 39
Detection And Alarms Component 44

Digital Infrastructure Layer ***49***
Digital Infrastructure Layer Checklist 50
Policies And Procedures Component 54
People (Roles And Training) Component 59
Architectural Component 65
Communication Component 71
Access Control Component 73

Campus Exterior Perimeter Layer ***78***
Campus Exterior Perimeter Layer Checklist 79
Policies And Procedures Component 80
Architectural Component 81
Communication Component 83
Video Surveillance Component 85
Detection And Alarms Component 89

Building Perimeter Layer ***90***
Building Perimeter Layer Checklist 91
Policies And Procedures Component 93
People (Roles And Training) Component 94
Architectural Component 94
Communication Component 104
Access Control Component 106
Video Surveillance Component 108
Detection And Alarms Component 111

Classroom/Interior Layer ***112***
Classroom Interior Layer Checklist 113
Policies And Procedures Component 115
People (Roles And Training) Component 116
Architectural Component 116
Communication Component 120
Access Control Component 123
Video Surveillance Component 127
Detection And Alarms Component 131

Additional Resources ***134***
Enhanced Technologies 135
Key Resources 139

DISCLAIMER: The Safety and Security Guidelines for K-12 Schools (the "Guidelines") are provided for informational purposes only. Under no circumstances do the contributors to this document and organizations participating in the Partner Alliance for Safer Schools (PASS) provide any related guarantees or accept liability for any loss or damage resulting from any person acting or refraining to act on this information. The Guidelines are not a substitute for legal, financial and other professional advice that may be required to address the specific facts and circumstances related to the implementation of a particular school safety security measure or program.

© 2025 Partner Alliance for Safer Schools

PASS
Partner Alliance for Safer Schools

About PASS

The Partner Alliance for Safer Schools (PASS) has a singular focus: To provide school administrators, school boards and public safety and security professionals with guidelines for implementing a layered and tiered approach to securing and enhancing the safety of school environments.

Established in 2014, PASS brings together expertise from the education community, law enforcement and the security industry to develop and support a coordinated approach that can assist school administrators in making effective use of proven security practices specific to K-12 environments and informed decisions on security investments.

In 2015, PASS first released the Safety and Security Guidelines for K-12 Schools (the "Guidelines"), which remains the most comprehensive information available on leading practices specifically for securing school facilities available. The seventh edition (2025) is greatly expanded to address the growing range of complex security challenges facing today's K-12 schools, providing a resource for school officials–and their solutions providers–to help achieve the most appropriate and cost-effective deployment of security solutions.

PASS has grown throughout the years, and the Guidelines reflect the time, expertise and passion of over 75 volunteers. It is those volunteers who make this work possible. For more information, visit passk12.org.

Introducing the All-New 7th Edition



The 7th Edition of the PASS Safety and Security Guidelines for K-12 Schools Represents two years of diligent work by our dedicated volunteers. If you've worked with the PASS Guidelines previously, here are some notable improvements from our previous edition.

- Introduction of the Digital Infrastructure Layer: This new layer recognizes the importance of cybersecurity and attentive management to digital systems and data. The addition of this layer takes a converged approach to security, dramatically expanding PASS beyond what was primarily a domain of physical security.
- Unifying the Property Perimeter and Parking Lot Layers into the new Campus Perimeter Layer: Our many volunteer school security experts recognized that these layers are commonly approached from a unified safety standpoint.
- Detailed Guidance on Visitor Entry: In addition to traffic-flow diagrams and example floor plans, this edition also extensively covers aspects like visitor management processes.
- Greater Content on Physical Hardening: From topics like door construction to security film and window glazings to reinforcement of classroom walls, the 7th Edition adds greater depth of content than before on aspects of physical hardening.
- Expanded Information on Panic Alarm Systems: As panic alarm systems have continued to prove valuable in school emergency situations, our newest edition increases guidance on this important solution.
- In-depth Coverage of Door Locks and Door Devices: Properly locking doors is an essential component within a school, and this version covers the complexities of school-specific lock requirements with great nuance.

There are many more areas where the PASS Guidelines have expanded for this new edition, released July 2025, and PASS welcomes feedback as we strive to continually improve our guidance, as we have done since founded in 2014. In addition to this resource, PASS regularly publishes articles and whitepapers on distinct school security topics via our website and circulates that content to our digital subscribers. Sign up at passk12.org to stay current with PASS.

© 2025 Partner Alliance for Safer Schools

Introduction

Today's school safety and security challenges are multifaceted and complex. There is no single action that will, by itself, make our schools safe. Protecting students and staff is a tremendous moral and legal responsibility that requires a comprehensive approach to these challenges.

Sadly, our nation's schools have increasingly become soft targets for mass violence. Since 2000, schools have been the second most frequent targets in active shooter incidents as defined by the FBI. The highly publicized mass murders at Columbine High School, Sandy Hook Elementary School and Marjory Stoneman Douglas High School and more recent mass shootings at other schools have led to reassessments of how we manage risk in the K-12 environment in the 21st century. In a nation where approximately 56 million students attend nearly 132,000 K-12 schools, a rate of 44 active shooter incidents from 2000 to 2019[1] is, thankfully, an extremely low one. While this low-probability/high-consequence threat cannot be ignored, it should always be considered within the full picture of K-12 safety and security challenges.

According to the FBI active shooter report of 2023, the rate of active shooter events in the last 5 years, in comparison to 2014-2018, has risen by 89%. While active shooter incidents are on the rise, only 12 of those events (between 2019-2023) occurred on a school campus. These updated statistics show that the changes in school safety and security are making a difference. Yet, there is still work to be done.[2]

Solutions to these challenges must be pursued across all areas of emergency preparedness: prevention, protection, mitigation, response and recovery; however, a modern and effective security infrastructure is a central component of any comprehensive school safety strategy. When other prevention efforts fail, facility security measures are critical to protection, mitigation and response.

Security management is a core responsibility of school administrators, who face daily pressure to ensure that students are protected, often without significant security expertise or the benefit of full-time safety/security staff. When it comes to security, administrators face two simple but difficult questions:

- What should we do?
- How do we prioritize?

The PASS Guidelines were developed to provide administrators with a means to effectively evaluate security infrastructure currently in place, prioritize investments and maximize security gained by leveraging available resources. The Guidelines identify and classify leading practices for securing K-12 facilities in response to urgent needs for information identified by the education community:

- Specific actions that can effectively raise the baseline of security
- Vetted security practices specific to K-12 environments
- Objective, reliable information on available safety and security technology
- Assessment of current security measures against nationwide best practices
- Multiple options for addressing security needs identified
- How to distinguish needed and effective solutions from sales pitches on unnecessary products

1 https://www.fbi.gov/file-repository/reports-and-publications/active-shooter-incidents-in-the-us-2019-042820.pdf/view
2 https://www.fbi.gov/file-repository/reports-and-publications/2023-active-shooter-report-062124.pdf/view

© 2025 Partner Alliance for Safer Schools

Scope

The primary focuses of the PASS Guidelines are physical security and life safety, and recommendations are limited to related policies, procedures, equipment and technology. The Guidelines do not address other aspects of prevention often associated with school safety, such as mental health, behavioral threat assessment[3] or policies related to firearms. Likewise, many areas of response and recovery are within the purview of law enforcement and other emergency responders. Great care has been taken to ensure consistency with and avoid unnecessary duplication of important recent work in these areas, such as the National Fire Protection Association's (NFPA's) NFPA 3000 Standard for an Active Shooter/Hostile Event Response (ASHER) *Program*,[4] released in 2018, which focuses in large part on response and recovery.

The Guidelines do not include best practices for the deployment of security personnel, school resource officers and school-based policing. While these individuals play a critical role in securing school facilities, organizations like the National Association of School Resource Officers (NASRO) provide excellent resources on the issues and best practices that are specific to personnel.[5]

While the safety and security of school facilities plays a key role in promoting safe and positive school climates, this should be part of a comprehensive school safety strategy that addresses other factors as well. For example, an assessment of targeted school violence by the U.S. Secret Service[6] found that while there is no profile for perpetrators, 80% of student attackers were bullied by their classmates, indicating the importance of processes and procedures to intervene when such behaviors are reported.

The Guidelines do not address every risk and every situation and, importantly, **do not include product-specific recommendations**. PASS does not endorse specific products, services or service providers. Further, the Guidelines do not address countermeasures such as tactical equipment or arming staff or security personnel, on which current practice and community viewpoints vary considerably among states and regions.

Common Acronyms in School Security

ACS – Access Control Systems

CPTED – Crime Prevention Through Environmental Design

DAS – Distributed Antenna System

EOP – Emergency Operations Plan

ICS – Incident Command Center

IDS – Intrusion Detection System

MNS – Mass Notification System

MOU- Memorandum of Understanding

NCS4 – National Center for Spectator Sports Safety and Security

NFPA A.S.H.E.R. – Active Shooter/Hostile Event Response

NRF- National Response Framework

NTAC – National Threat Assessment Center

PASS – Partner Alliance for Safer Schools

SOC – Security Operations Center

3 https://www.secretservice.gov/sites/default/files/reports/2020-10/USSS_NTAC_Enhancing_School_Safety_Guide.pdf
4 https://www.nfpa.org/codes-and-standards/nfpa-3000-standard-development/3000
5 https://www.nasro.org
6 https://www.secretservice.gov/data/protection/ntac/Protecting_Americas_Schools

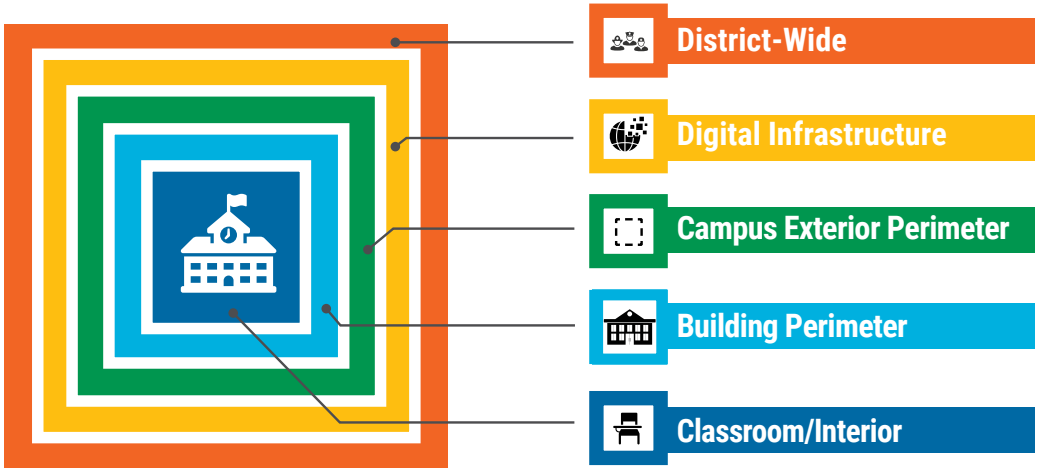
© 2025 Partner Alliance for Safer Schools

Structure of the PASS Guidelines

Layered Security

The security profession and industry have always recognized that the best approach to security is a layered approach. Consistent with the practice of implementing security in depth and the site security approach recommended by the U.S. Department of Homeland Security (DHS),[7] the Guidelines describe approaches within five physical **layers** for school facilities.

LAYERS OF PROTECTION



A layered approach is essential to addressing a broad range of threats, as each successive layer provides specific components to deter, detect or delay and respond to adversarial behaviors in the event that other layers are bypassed or breached. Each layer includes basic protective elements, or **components**, of security. Every layer does not necessarily include all seven of these common components, and a layer may include additional components unique to that layer.

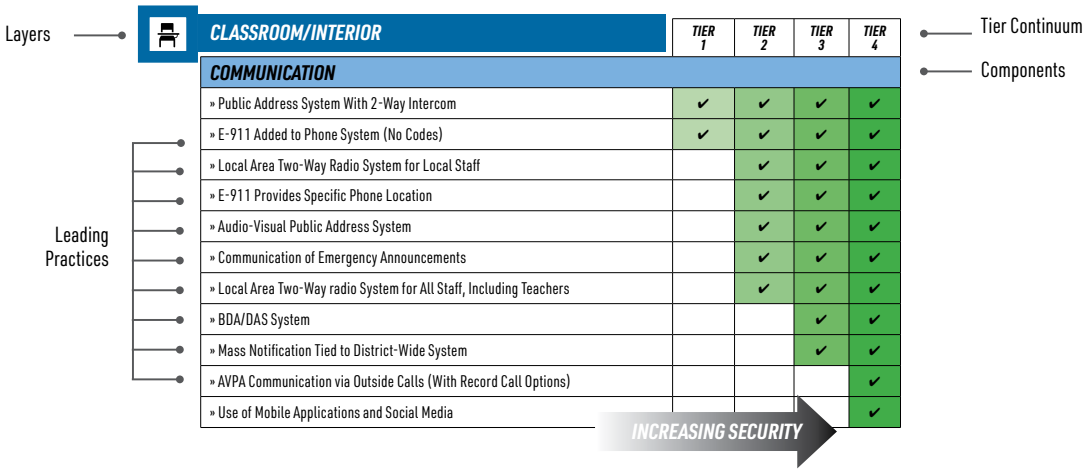
SAFETY AND SECURITY COMPONENTS

- **Policies and Procedures**
- **People (roles and training)**
- **Architectural**
- **Communication**
- **Access Control**
- **Video Surveillance**
- **Detection and Alarms**

While components are not listed in a priority order, three components included in all layers are policies and procedures, the roles and training of people and communication. These components often perform a function in every layer and every tier within each layer.

7 DHS Primer to Design Safe Schools Projects (2012), https://www.dhs.gov/xlibrary/assets/st/bips07_428_schools.pdf

© 2025 Partner Alliance for Safer Schools



Generally, each leading practice recommendation presented in this guide corresponds to one of these components within a layer or across multiple layers. Leading practice recommendations are further divided into TIERS along a "TIER Continuum" progressing from TIER 1, which provides a good baseline level of security, to TIER 4, which includes the most comprehensive approaches to securing a facility. It is often said, "If you have seen one school, you have seen one," meaning that every school and district is unique. Each building has its own culture as well as layout. The TIER Continuum helps address the uniqueness of schools and provides an approach that can be adapted to fit each school and district.

TIER DEFINITIONS

Tier One: Establishes a foundation that is a baseline layer of security. All schools should work towards adherence to Tier One measures. Some Tier One standards have a minimal budgetary impact, while others require funding and the development of an implementation plan.

Tier Two: Builds upon the foundation laid in Tier One. Tier Two recommendations can be phased in with available funding and as local culture shifts towards heightened levels of security. All schools – regardless of size, location or other specific factors – should work toward adherence to Tier Two measures if Tier One is complete.

Tier 3: An implementation step for a higher level of security developed after a documented assessment by the core security team. The team should consider threats, local conditions, and available technology solutions with budgetary and staffing resource allocation.

Tier 4: An implementation recommendation that is part of an overall strategic security plan detailed by the core security team. Tier 4 recommendations often require multi-year planning and district-level funding for full implementation.

Many schools will not be able to implement TIER 4 measures and may not have a need to do so. The general purpose of this guide and its TIERS is to provide school administrators with tools they can use to gauge their risk levels, identify their security needs and, after factoring in available resources, develop security plans tailored to their schools or districts that incorporate practices and procedures vetted by experts.

Each TIER includes all recommendations in the preceding TIERS, and in many cases, implementation of best practices at the lower TIER level lays the groundwork for moving to higher levels of security in the long term. Whether officials at a school or district determine that implementing TIER 1 best practices would be best for their situation or identify risk factors that compel a move to other TIERS, this guide can help to inform and provide a rationale for decision making.

© 2025 Partner Alliance for Safer Schools

Baseline Practices and Obligations

Some states have specific safety requirements applicable only to schools within their jurisdiction, such as Alyssa's Law which has been adopted in at least nine states so far that requires the installation of panic alarms linked to law enforcement. Another example would be some state laws requiring specific classroom locking mechanisms. At the same time, some safety measures–many procedural–are already required by federal law or regulation, or are commonly implemented throughout the U.S. Many (but not all) of the most relevant of these are highlighted here as "Baseline Practices and Obligations." It is assumed in the Guidelines that all such legal and/or regulatory obligations and common practices are being met. The "leading practice" recommendations across the Guidelines' layers and tiers are understood to extend beyond what is legally required already and that school and district staff are aware of and implementing any additional state-specific requirements in conjunction with recommended best practices found in the Tier Continuum.

- ***School and District Emergency Roles & Responsibilities Defined.*** Each school district adopts the NRF and NIMS developed by the Federal Emergency Management Agency (FEMA), which establishes an Incident Command System (ICS), collaborative planning teams, and emergency operations plans (EOPs) that include any elements that are required by state law and should detail the role of safety and security technologies during an emergency.

- ***All Staff Can Initiate Emergency Procedures.*** All school staff should be able to initiate lockdowns and other emergency procedures when appropriate. During an active threat incident where there is a danger to occupants of a school, staff need to know how to reduce risk and protect lives until help arrives.

- ***Empower Community to Share Concerns Through Anonymous Reporting.*** Most districts use communications tools allowing students and others in the community to anonymously report potential threats and other concerns has demonstrated success in preventing potential violence. Some states, such as Colorado, mandate that public schools implement tip line programs.[8]

- ***Staff and Volunteer Training on Mandated Reporting Requirements and Procedures.*** All states have laws requiring individuals serving in specific capacities to report suspected child abuse to an appropriate agency, such as child protective services or a law enforcement agency.

- ***Sharing Maps and Other Facility Information with Law Enforcement, Fire and EMS.*** As schools present unique challenges for emergency responders due to size, complexity and occupants, responders require extensive amounts of detailed yet easily understandable information in the event of an attack or other emergency.

- ***Security Plans Specific to Auxiliary Buildings.*** Safety and security are just as necessary and important at school district auxiliary buildings (transportation centers, educational centers, warehouses and other places in a school district that are not considered instructional facilities) as they are at main instructional buildings.

- ***Student Identification Badges (in secondary schools).*** Identification badges are a simple and secure way to easily determine who is supposed to be on campus as long as they are required to be worn visibly or presented to school staff upon request; this can be especially important to responders during emergency events, as they are not likely to be familiar with the students.

- ***Climate and Cultural Survey of Stakeholders.*** Conducting an anonymous climate and cultural survey allows a school district to obtain valuable information on the views of students, staff and parents that can inform planning teams on safety and security issues.

8 https://safe2tell.org/

© 2025 Partner Alliance for Safer Schools

- ***First Responder Training for School Personnel Based on Local Needs.*** School employees in school-based emergencies are the very first responders and should be provided with basic training in first aid protocols, including CPR and the use of automatic external defibrillators at a minimum. Many other first responder training programs are available that are relevant to trauma, mental health and other needs which arise during emergency situations.
- ***All-Hazard, Scenario-Based Drills with Community Partners on Recurring Basis.*** This type of exercise is intended to generate discussion of various issues regarding a hypothetical, simulated emergency and should foster an understanding of incident command and your district's capabilities.
- ***Video Data Use and Retention Policy.*** A video surveillance use and data retention policy is typically established at the district level to ensure consistency across all schools. The use policy provides clear instructions as to how video surveillance will be used in daily operations, while a data retention policy defines how long recorded video will be retained. Some states have produced guidelines and standards for school security that may address video data, so it is important to refer to them in your policy if applicable.
- ***Memorandums of Understanding (MOUs) with Emergency Responders.*** Districts establish MOUs with local police, fire and EMS in two primary areas relating to emergency communication, threat information sharing and building access in an emergency.
- ***MOUs With Law Enforcement for Sharing Video Data.*** Districts also establish MOUs with local law enforcement to provide for sharing recorded or live video of incidents when necessary for emergencies and investigations.
- ***MOUs With Hospitals, Religious Organizations, Community Centers and Red Cross.*** EOPs typically incorporate participation by local facilities and organizations for evacuation, trauma care, mass casualty response, family reunification, mental health recovery and other purposes if needed. These relationships with community organizations are governed by MOUs so that roles and responsibilities are clearly defined and all parties can be adequately prepared to act if needed.

© 2025 Partner Alliance for Safer Schools

Recommended Uses

There are several specific ways the PASS Guidelines can be used to assist school administrators and other officials.

- ***SUPPORT RISK ASSESSMENT AND DEVELOPMENT OF COMPREHENSIVE SECURITY PLANS.***
  The PASS Guidelines can be used by school officials, consultants and solutions providers to provide a common starting point for objective analysis and prioritization of school security needs. In this way, the Guidelines can be used as part of the risk assessment process or to define resulting recommendations (see Risk Assessment) or help initially formulate or update a comprehensive security plan to put recommendations into action.

  By identifying a given school or district's TIER levels, the Guidelines provide administrators with a frame of reference to communicate facility security status to school board members, parents and local officials as they seek support in advancing up the TIER Continuum as necessary to mitigate identified risk according to funding availability.

- ***GRANT PROPOSAL DEVELOPMENT.*** The federal government[9] and many states have provided significant funding for security improvements. The PASS Guidelines and best practices outlined here provide a framework for identifying the most critical needs and cost-effective solutions, information that can help strengthen and justify grant applications. For more information on funding sources, see the Security Industry Association's Guide to School Security Funding.[10]

- ***SCHOOL SAFETY/SECURITY STANDARDS.*** Unlike with fire detection and suppression, building codes do not generally guide the implementation of security practices as hard requirements. For the past 100 years, fire alarm systems have provided the communication mechanism used to alert students, staff and visitors to the presence of a fire threat inside a school. Fire alarms have long been required through adoption of NFPA 101, the life safety code, and NFPA 72, the fire alarm and signaling code, and as a result no students have lost their lives in a fire at a school since 1958.

  Several states have established baseline standards or guidance for securing school facilities, often to augment state grant programs, and there are many states in which such policies are under consideration. The PASS guidelines can help inform standards and guidance development efforts by policymakers or in the private sector.

- ***AVOIDING PITFALLS.*** Both administrators and providers benefit from being able to demonstrate effective use of technology and resources to meet specific security objectives, avoiding pitfalls that could result in the waste or underutilization of scarce resources in the pursuit of improved security.

  Not only can the information provided in the Guidelines help stakeholders stay informed on nationwide leading practices, it also provides a reference point for evaluating specific solutions and products that are offered. It is particularly important in today's climate that school officials be wary of aggressive marketing of any products that are unproven, inappropriate or even illegal for school use.

8 For example, the U.S. Department of Justice School Violence Prevention Program https://cops.usdoj.gov/svpp
9 https://www.securityindustry.org/report/sia-guide-to-school-security-funding/

© 2025 Partner Alliance for Safer Schools

TOP 10 K-12 SAFETY AND SECURITY PITFALLS:

1. Failure to assemble a planning team (see Policies and Procedures) that includes all appropriate and necessary stakeholders
2. Insufficient prioritization of security based on an "it won't happen here" mentality
3. Implementation of advanced technology and/or high-cost solutions without first ensuring baseline, proven security measures are in place (such as those found in TIER 1 in the PASS Guidelines)
4. Inconsistent implementation of disparate systems that do not meet security objectives identified in a comprehensive security plan or risk assessment
5. Short-sighted planning or products that respond only to the latest tragedy, as opposed to supporting a long-term, holistic approach
6. Choosing lowest-cost solutions above all other considerations, such as total life cycle costs
7. Reliance on technology for emergency communications that is not designed for such use
8. Overreliance on a single form of emergency communication or overdependence on a single type of solution or technology to address a broad range of safety and security challenges
9. Failure to appropriately balance external and internal risk mitigation–Based on risk assessment, different approaches may be more appropriate, depending on the facility. With active shooter events, for example, 100 percent of such incidents targeting elementary schools have been perpetrated by intruders from outside the school communities, while approximately 75 percent of incidents at secondary schools involved students or others associated with the schools.
10. Unnecessary products that can be solutions in search of a problem. The markteting of "barricade" or "secondary locking" devices is just one example. Offering no advantage over a lockset, such devices are typically offered as a lowest-cost lockdown solution. These devices can increase liability and risk and most violate fire and life safety codes as well as the Federal Law – Americans with Disabilities Act (ADA). For further information see *5 Reasons Schools Should Avoid Classroom Barricade Devices*[10] and the *PASS Whitepaper on Classroom Barricade Devices.*[11]



Examples of "barricade" or "door blocker" devices.

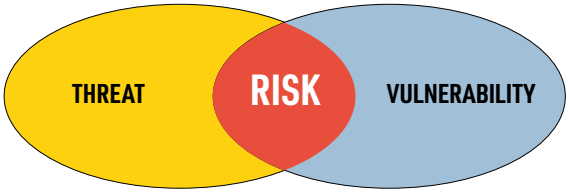
10 https://passk12.org/news/5-reasons-schools-should-avoid-classroom-barricade-devices/
11 https://passk12.org/wp-content/uploads/2019/04/PASS-WHITEPAPER-Classroom-Barricades-2019-04-10.pdf

© 2025 Partner Alliance for Safer Schools

Risk Assessment

Securing schools requires a risk mitigation mindset. What is risk? In everyday conversation, threat, vulnerability and risk are often used interchangeably to describe what we are trying to address with security; however, there are important distinctions between these terms.

- A threat is what we are trying to protect assets (people, property, etc.) against.
- A vulnerability is a gap in our protection efforts.
- A risk results where and when threats and vulnerabilities intersect.



Like any organization that invites people onto its property, schools have an obligation to provide a reasonable level of security to mitigate risks. In the commercial sector, protecting a facility and its occupants is viewed not as a reactive law enforcement function, but as a proactive security function. As mentioned earlier, the security objective is to deter, detect or delay, and respond to adversarial behavior through the use of people, processes and technology. The PASS components help mitigate risk by reducing vulnerability.

A risk assessment is the first step toward developing a comprehensive security plan and thus a prerequisite for decisions regarding deployment of security solutions. Several options for conducting risks assessments are available through:

- Local police and fire officials (ability varies by jurisdiction)
- DHS protective security advisors[12]
- Independent consultants
- Security design consultants/systems integrators
- Internal assessment using free assessment tools
- Assessment by local subject matter experts assembled by districts

A building assessment of physical security at individual facilities is part of the risk assessment process, either for each district facility or for a smaller representative sample of facilities. It is an inventory of existing components that are identified in the PASS Guidelines and helps document any potential gaps in a school's protection efforts. Under the PASS Guidelines, TIER 1 best practices are basic security measures that should be implemented by all schools and districts, while higher-TIER practices should be guided by recommendations resulting from an assessment process. PASS offers a summary of possible causes for school violence with appropriate resources that schools can use to educate themselves on these challenges and implement as part of the overall safety plan.

12 https://www.cisa.gov/about/regions/security-advisors

© 2025 Partner Alliance for Safer Schools

Risk assessments can cover a wide range of issues. Among these, there are many security-related threats facing schools in addition to other threats to safety, which is why an all-hazards approach is so important. These include but are not limited to:

- Theft
- Burglary
- Assault
- Sexual assault
- Kidnappers and sexual predators
- Workplace violence
- Active shooter/mass casualty attacks
- Homicide
- Suicide
- Gang activity
- Trespassing
- Bullying and harassment
- Parental custodial concerns
- Unsupervised visitors
- Vandalism/property destruction
- Compromise of confidential information

© 2025 Partner Alliance for Safer Schools

Risk assessment and mitigation can never eliminate risk; however, risks can be identified, measured and reduced. The best practices identified in the PASS Guidelines can be used for developing recommendations based on this process and formulating a plan to put them into action. The causes of school violence are complex. However, there are patterns that, if proper resources are utilized, schools can identify and work to resolve.

While many schools are prioritizing investment in high-tech security solutions over relational or systemic interventions, it is important to keep in mind that when it comes to school shootings, all schools operate within constraints that make it exceedingly difficult – sometimes impossible – to fully address the six root causes of these events:

1. ***Adverse Childhood Experiences (ACEs)*** often originate in the home, beyond school jurisdiction or reach.
2. ***Mental health services*** require licensed staff, funding, and long-term care that most schools are not equipped to provide.
3. ***Bullying and marginalization*** are social-cultural issues, deeply embedded in adolescent dynamics and sometimes reinforced by broader societal narratives.
4. ***Access to firearms*** is a political and legal issue schools cannot regulate.
5. ***Online radicalization*** occurs in digital spaces beyond school monitoring and often in secret.
6. ***Community and economic stressors*** are structural problems rooted in inequality, poverty, and lack of public services.

Many assessments are available and can provide a useful starting point for formulating a security plan, especially when resources for assessments are limited. PASS recommends that districts start with Schoolsafety.gov.[13] PASS also recommends using assessments provided by school safety centers in the many states where such centers have been established.

Similar free resources are also provided by state governments and the federal government. For building assessments, the NFPA 3000 Active Shooter and Hostile Event Response (ASHER) standard recommends the PASS Guidelines among other tools. See Annex of NFPA 3000 Chapter 5 (Risk Assessment).

13 https://www.schoolsafety.gov/foundational-elements-school-safety

© 2025 Partner Alliance for Safer Schools

Layers of Protection

District-Wide

Leadership and coordination at the district level are integral to the successful development and adoption of school safety processes, plans, technologies and procedures and for ensuring these measures are updated for consistency with leading practices as they evolve.

Most school safety measures have district-wide components or responsibilities. It is critical for districts to understand the fundamental link between readiness for day-to-day emergencies and disaster preparedness. School districts that are well prepared for individual emergencies involving students or staff members are more likely to be prepared for complex events like a community disaster or an active shooter incident. In the Guidelines, PASS outlines the components and best practices along the TIER Continuum at the district-wide level that schools and school districts can use in addressing a wide range of emergency situations that impact school safety, such as incidents of natural disasters, violence, mental health and medical emergencies.

Digital Infrastructure

The digital infrastructure layer encompasses the policies, technologies and operational safeguards implemented at both the district and school levels to mitigate risk, defend against cyber threats targeting the school community, and protect physical security systems from compromise through cyberattacks. It ensures that cybersecurity and physical security are integrated to provide a resilient defense posture across the educational environment.

Campus Exterior Perimeter

The campus exterior perimeter layer begins at the campus, school or facility property boundary and extends to the primary building(s). This area includes playgrounds, sporting fields and other facilities that are often used by the public after school business hours end. It also includes parking lots, where schools experience the most safety issues. Falls, car accidents, dangerous driving, theft, vandalism and assault are just some of the events that can take place in these areas. The physical security and safety of a school facility begins at the campus exterior perimeter, where the most outwardly visible security deterrents to an external threat can be implemented. Boundaries should be clear to the public and provide visible notice of the rules and responsibilities for individuals entering school property. This layer also takes the principles of crime prevention through environmental design (CPTED) into consideration so that the design of the campus and grounds enhances safety and security.

Building Perimeter

The building perimeter layer begins with school grounds adjacent to the exterior structure of a building and consists of the perimeter of a building itself, including the exterior doors and windows of a school. Securing a building perimeter can range from simple to complex, especially for middle schools or high schools with multiple buildings/open campuses. Key safety and security functions take place within this layer, as it encompasses all areas where people enter and exit a school building.

Classroom/Interior

The classroom/interior layer consists of a school's entire interior, including not only classrooms but also gymnasiums, cafeterias, media centers, etc. This is both the last layer of defense against external threats and, often, the first protection against internal threats to students, staff and visitors' safety.

© 2025 Partner Alliance for Safer Schools

Safety and Security Components

POLICIES AND PROCEDURES

The policies and procedures component involves a school or district's emergency operations plan (EOP) and security plans. Comprehensive security plans, and the policies and procedures created to implement them, form the foundation of school safety and security. Without proper policies and procedures in place, it is impossible to successfully use security technology and other security measures, regardless of how advanced they may be. Effective policies and procedures alone can mitigate risks, and there are often no costs associated with implementing them. Essential security-specific policies and processes relevant to each layer are categorized under TIER 1 as foundational leading practices.

PEOPLE (ROLES AND TRAINING)

Personnel (vigilant staff and students) make up the most important component of each layer. To individuals with criminal intent, such vigilance is an effective deterrent. ALL students and staff should be empowered to take effective action in emergencies and receive appropriate training and instructions relevant to a school or district's safety processes, plans, technologies and procedures.

ARCHITECTURAL

There are many architectural considerations that can enhance the security and safety plans for school buildings. Using Crime Prevention Through Environmental Design (CPTED) principles is critical to efforts by districts and their architects in designing buildings and grounds that enhance safety and security. Buildings should be designed to have natural surveillance (sight lines), territorial reinforcement (designated public, semi-private and private areas) and access control. The architectural component also includes collecting and sharing critical information about school facilities for mitigation and response to emergencies.

COMMUNICATION

Emergency communication is vital to the safety and security of the staff and students in our schools. It is important to distinguish between emergency and routine communication systems. An emergency communication system is defined by NFPA 72 (the national fire alarm and signaling code) as "a system for the protection of life by indicating the existence of an emergency situation and communicating information necessary to facilitate an appropriate response and action." Routine communication systems handle day-to-day communication on all matters outside this definition.

The use of dedicated emergency communication systems and technologies is essential. Normal business telephone, email and social media apps designed for routine communication are not adequate for critical communication during an emergency event unless they are specially configured for this purpose in a code-compliant manner. The 9/11 terrorist attacks and the 2011 tornado in Joplin, Missouri,[14] are two of many examples in which these routine communication technologies failed during emergency situations.

14 National Institute of Standards and Technology (NIST) Final Report, https://nvlpubs.nist.gov/nistpubs/NCSTAR/NIST.NCSTAR.3.pdff

© 2025 Partner Alliance for Safer Schools

ACCESS CONTROL

Controlling access to school property, buildings and classrooms is a basic security function and responsibility of school administrators. Mechanical locks have historically formed the base for any access control system, but there are other critical elements to consider. Many schools and districts have invested in electronic access control features that allow for enhanced security. Modern access control systems and procedures offer an effective solution to prevent unauthorized intruders from accessing a building during school hours and for monitoring access points for the various layers.

VIDEO SURVEILLANCE

A video surveillance system is a component of any school or district security program, providing deterrence and detection and, in more advanced implementations, enhancing response to a variety of daily challenges experienced at schools.

In the past, video recordings were used primarily in a forensic capacity to help determine the (who, what, when and where) of an incident after the fact. As video technology has advanced, so have capabilities that allow security professionals to leverage it as a proactive tool to help mitigate risks before and as incidents occur. Much of this capability has been enabled through the widespread use and increasing affordability of internet protocol (IP) cameras.

It is very important to note that, in video surveillance, there is no such thing as a "one-size-fits-all" approach. Designing a quality video surveillance system can be complicated and requires a collaborative approach involving multiple professionals.

DETECTION AND ALARMS

"Detection and alarms" refers to technology used to detect and/or report an emergency event. Traditional intrusion detection systems represent a key platform that has evolved beyond burglar alarms to provide the capability to report other types of emergencies and support an all-hazards approach to safety and security. The most important aspect of detection and alarm systems is that they provide the technological means to easily translate the detection of a security threat to a strategic notification that best fits with the processes and protocols put in place to respond to the threats that schools face.

A NOTE ON TESTING

All technologies within the safety and security components (Communication, Access Control, Video Surveillance and Detection and Alarms) should be tested yearly. These tests can be carried out during the summer to ensure that all technology is functioning appropriately. Additionally, it is recommended that all IP-based technologies should be checked for failures each week. For example, a process should be in place to ensure that all video surveillance cameras are online and functioning properly.

Routine maintenance should be considered for all technology that has IP-based equipment, firmware, and software. Many systems require firmware and/or software updates. Districts/Schools should have a process to ensure that the current firmware and software versions are installed.

© 2025 Partner Alliance for Safer Schools

Using the PASS Guidelines to Formulate a Comprehensive Security Plan

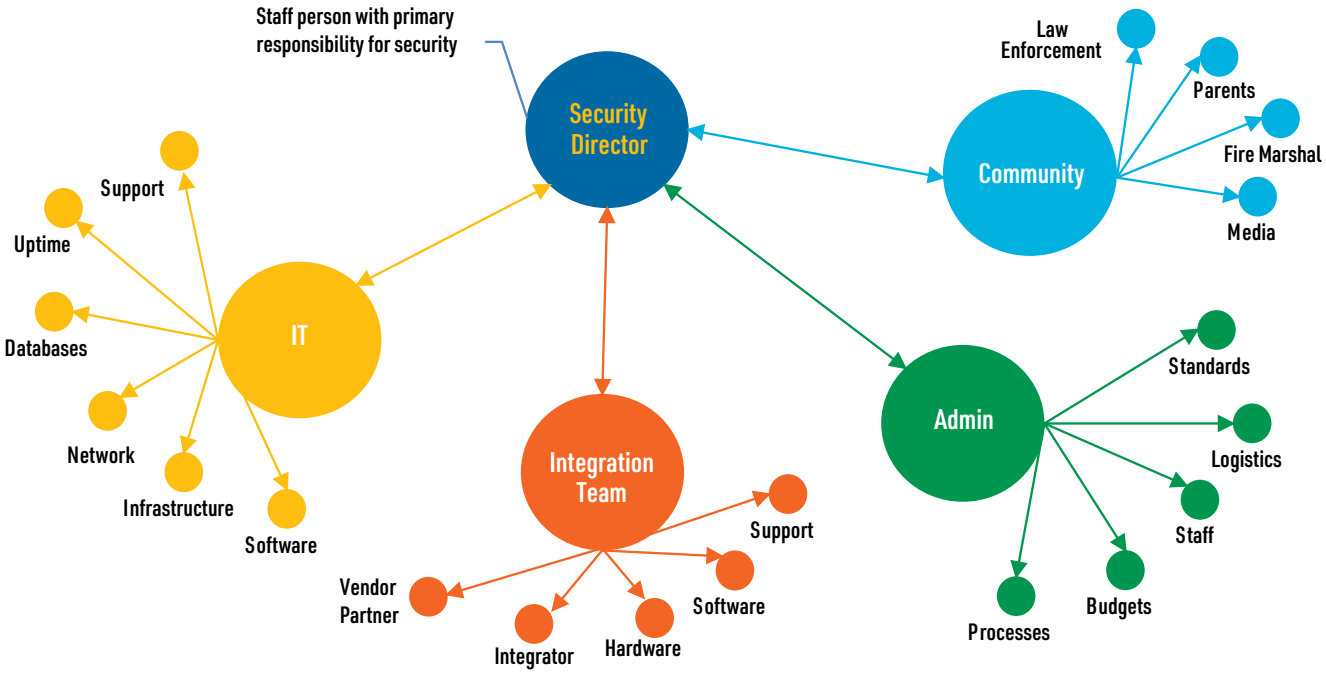
Here is a suggested roadmap for using the Guidelines to formulate a security management plan.

STEP 1–Assemble Team. Security planning teams should include key stakeholders in the K-12 environment. The process of forming a team should be led by an experienced security director, if a district is fortunate enough to have full-time staff in this position, or a staff member who has security as a primary responsibility. Start with a basic team including:

1. Security director
2. School administrator
3. Security/systems integrator and/or consultant
4. IT director
5. Local police and fire officials
6. School-based health care professional

In larger or more complex projects, it is also best to have a hardware consultant involved in the process.

Security...It takes a team.



© 2025 Partner Alliance for Safer Schools

STEP 2–Risk Assessment. Most school buildings across a district have unique risk profiles. Complete a risk assessment for each building followed by a building assessment (using the PASS Guidelines Checklist) and develop the plan and budget for the building.

STEP 3–Building Assessment Using Checklist by Layer. The Building Assessment can be completed using the PASS Guidelines Checklist. Complete this process by reviewing each layer within the Guidelines. The district-wide layer needs only to be completed once, as it is designed to cover best practices that should be implemented across the entire district. For each individual building, complete the balance of the layers, including:

- Campus Exterior Perimeter Layer
- Building Perimeter Layer
- Classroom/Interior Layer

LAYER/COMPONENTS/BEST PRACTICES	TIER 1	TIER 2	TIER 3	TIER 4	Status	Year	Notes
DISTRICT-WIDE							
DETECTION AND ALARMS							
» Panic Alarm System in Each Building	✔	✔	✔	✔			
» Panic Alarms Sent To Law Enforcement	✔	✔	✔	✔			
» Centrally Monitored Intrusion Systems	✔	✔	✔	✔			
» Fire Alarm Systems	✔	✔	✔	✔			
» Carbon Monoxide Detection	✔	✔	✔	✔			
» Panic Alarms Systems Unified with Access Control, Video Surveillance and Communication Systems		✔	✔	✔			
» Two Way Emergency Phones		✔	✔	✔			
» Graphical User Interface for Operators			✔	✔			
» Intrusion and Duress Alarms Monitored by a District-Wide SOC				✔			

STEP 4–Establish Documents and Budgets Based on Checklist Selections. Security component and best practices descriptions found in the guidelines can be used to assemble a detailed document of the building/district plan. Budgets can be established using an estimated cost range for each best practice.

The Goal: Unified Security and Life Safety Systems

All technology implementations should further build upon the unification of security and safety components and related systems by school districts. Unified systems address the difficulties of integrating technologies across different platforms and within the connected environment in which they reside. Properly implemented, a unified system eases integration of new components and allows a district to continue to evolve and expand. It is important for a school district to work with their integrator to ensure facility infrastructure can support any new technology as part of a unified system.

© 2025 Partner Alliance for Safer Schools

Trend: The Security Operation Center

A school Security Operations Center (SOC) is a centralized team that uses people, processes, and technology to monitor and improve an organization's overall security posture. SOCs can be staffed with both security and IT professionals who have expertise in both physical security and cybersecurity, and are responsible for preventing, detecting, analyzing and responding to a wide range of security incidents.

SOCs oversee physical security systems such as surveillance cameras, access control systems, intrusion detection systems and alarm monitoring. In addition to physical security, SOCs can also monitor servers, devices, databases, network applications, websites and other systems to uncover potential threats in real time. By integrating physical and cyber threat intelligence, SOC teams can respond more holistically to incidents that span both domains.

SOCs can identify and assess vulnerabilities within an organization's physical facilities and IT infrastructure, prioritizing and remediating risks to minimize the attack surface and reduce opportunities for exploitation. In the event of a successful attack or breach–whether physical, cyber, or a combination of both–the SOC is responsible for removing the threat, coordinating with emergency response or law enforcement if necessary, and restoring affected systems or facilities.

© 2025 Partner Alliance for Safer Schools

DISTRICT-WIDE LAYER



» QUICKFIND

District-Wide Layer Checklist 22
Policies And Procedures Component 24
People (Roles And Training) 33
Architectural Component 33
Communication Component 35
Access Control Component 37
Video Surveillance Component 39
Detection And Alarms Component 44

© 2025 Partner Alliance for Safer Schools



DISTRICT-WIDE LAYER

	TIER 1	TIER 2	TIER 3	TIER 4
POLICIES AND PROCEDURES				
» Dedicated Security Director/Department	✔	✔	✔	✔
» Establishment of Safety Policies and Procedures	✔	✔	✔	✔
» District-Wide Physical Security Standards	✔	✔	✔	✔
» Annual Physical Security Assessments Based on District-Wide Standards	✔	✔	✔	✔
» Ensure Maintenance of Security Technology Implementations	✔	✔	✔	✔
» Incident Reporting Documentation System	✔	✔	✔	✔
» Conduct Lockdown Drills	✔	✔	✔	✔
» Independent Security Assessment on 3-Year Cycle				✔
VISITOR MANAGEMENT SYSTEM				
» Visitor Badging System	✔	✔	✔	✔
» Electronic Visitor Management System		✔	✔	✔
» ID Scanning Technology		✔	✔	✔
» VMS-Assisted Background Checks				✔
STUDENT AND STAFF IDENTIFICATION				
» Volunteer Background Checks	✔	✔	✔	✔
» Smart Card Identification Badges		✔	✔	✔
PEOPLE (ROLES AND TRAINING)				
» Panic Alarm Activation	✔	✔	✔	✔
ARCHITECTURAL				
» Facility and Vicinity Mapping	✔	✔	✔	✔
» Entrances Marked With First Responder Numbering System	✔	✔	✔	✔
» Printed or Electronic Tactical Floor Plans		✔	✔	✔
» Zone Emergency Response System			✔	✔
» Virtual Response Plans and Implementation				✔
COMMUNICATION				
» Wide-Area Two-Way Radio System	✔	✔	✔	✔
» Bi-Directional Amplifier (BDA) or Distributed Antenna Systems (DAS)	✔	✔	✔	✔
» Trunked Radio System		✔	✔	✔
» Mass Notification Unified With Public Address/Audio-Visual PA		✔	✔	✔
» Unified of Access Control and Communication Systems		✔	✔	✔
» Unification of Detection and Alarm with Communication Systems		✔	✔	✔
» Unification of Video Surveillance with Communication Systems		✔	✔	✔
» Unification of Building Architecture		✔	✔	✔
WEATHER MONITORING				
» Monitor NOAA Local Weather Information	✔	✔	✔	✔
» Weather Monitoring Service		✔	✔	✔
» Weather Monitoring Station at Central School Facility				✔

© 2025 Partner Alliance for Safer Schools

DISTRICT-WIDE LAYER (cont.)

	TIER 1	TIER 2	TIER 3	TIER 4
ACCESS CONTROL				
» Emergency Site Building Access System for First Responders	✔	✔	✔	✔
» Access Control System Equipped with Remote Door Release and Lockdown Capability			✔	✔
» Electronic Access Control for IDF & MDF Rooms w/Key Override				✳
TRANSPORTATION				
» Interoperable Radio System for All Buses and School Vehicles	✔	✔	✔	✔
» Bus Video Surveillance/GPS System		✔	✔	✔
» Card-Based Check-In				✔
VIDEO SURVEILLANCE				
» Incorporation of Video Surveillance Into Emergency Response Plans	✔	✔	✔	✔
» Camera Standardization		✔	✔	✔
» Recording System Standardization		✔	✔	✔
» Recording System use of Video Analytics		✔	✔	✔
» Unification of Panic Systems with Video Surveillance System		✔	✔	✔
» Unification of Access Control with Video Surveillance System		✔	✔	✔
» Unification of Communication with Video Surveillance System		✔	✔	✔
» Video Verification of Panic Alarms to a Monitoring Service, Administrators and/or SOC			✔	✔
» Video Verification of Intrusion Alarms to Monitoring Service, Administrators and/or SOC			✔	✔
» Preventative use of Video Analytics				✔
» Brandished Weapons Analytics				✔
DETECTION AND ALARMS				
» Panic Alarm System in Each Building	✔	✔	✔	✔
» Panic Alarms Sent To Law Enforcement	✔	✔	✔	✔
» Centrally Monitored Intrusion Systems	✔	✔	✔	✔
» Fire Alarm Systems	✔	✔	✔	✔
» Carbon Monoxide Detection	✔	✔	✔	✔
» Panic Alarms Systems Unified with Access Control, Video Surveillance and Communication Systems		✔	✔	✔
» Two Way Emergency Phones		✔	✔	✔
» Graphical User Interface for Operators			✔	✔
» Intrusion and Duress Alarms Monitored by a District-Wide SOC				✔

© 2025 Partner Alliance for Safer Schools

POLICIES AND PROCEDURES COMPONENT:

Two national response models serve as the framework for local policies, procedures and response plans. For larger-scale emergencies and disasters, the National Response Framework (NRF)[1] offers guiding principles that enable all response partners to prepare for and provide a unified response to disasters and emergencies–from the smallest incident to the largest catastrophe. The term "response" (as defined by NRF) includes taking immediate action to save lives, protect property and the environment and meet basic human needs. Response also includes the execution of emergency plans and actions to support short-term recovery.

The NRF also describes how agencies, such as schools, can work together with communities, tribes, states, the federal government and private partners.

Secondly, the National Incident Management System (NIMS)[2]is a comprehensive national design for conducting incident management. NIMS provides the template, while the NRF provides the structure and mechanisms for incident management. A key component of NIMS is the Incident Command System (ICS),[3] which provides a standardized approach for incident management, regardless of cause, size, location or complexity. By using ICS during incidents, schools and districts will be able to more effectively work with the responders in their communities.

To maximize success, effective management of school emergencies requires training, preparation and planning. Schools are responsible for anticipating and preparing to respond to a variety of emergencies. The policies and procedures outlined below will help empower the students and staff to respond in an emergency, closely aligned with the phases of emergency management:

1 https://www.fema.gov/emergency-managers/national-preparedness/frameworks/response
2 https://www.fema.gov/emergency-managers/nims
3 https://training.fema.gov/emiweb/is/icsresource/

© 2025 Partner Alliance for Safer Schools

THE FIVE PHASES OF EMERGENCY MANAGEMENT



1. ***Prevention*** focuses on training, hazard response plans and exercises ahead of an event to prepare through proactive planning. The risk of loss of life and injury can be limited through good evacuation plans, environmental planning and design standards.
2. ***Mitigation*** is the effort to reduce loss of life and property by developing structural and non-structural measures that will mitigate the effects of a disaster.
3. ***Preparedness*** is a continuous cycle of planning, organizing, training, equipping, exercising, evaluating and taking corrective action. These elements are the cornerstones of preparedness and focus on readiness to respond to all-hazards incidents and emergencies.
4. ***Response*** is the management of resources including personnel, equipment and supplies and utilizes the incident command system in an all-hazards approach. The response phase is a reaction to the occurrence of the event.
5. ***Recovery*** activities continue beyond the emergency period and focus on restoring critical functions to stabilize operations and increase capacity to continue to serve their community after a disaster. The goal of the recovery phase is to bring the affected areas back to some degree of normalcy as soon as possible.

© 2025 Partner Alliance for Safer Schools

TIER 1

A. **Dedicated Security Director/Department.** Districts should designate a security director tasked with district-wide security management duties and responsible for the effective implementation of security policies and programs. Ideally this should be a full-time position with additional staff if needed as part of a security department; however, for many districts, staff tasked with security management will also perform additional functions.

B. **Establishment of Safety Policies and Procedures.** Each district should ensure that, within the policies and procedures established for staff and students, parents, volunteers and any others that interact with the school community, the following are covered:

- School safety/NIMS compliance
- All-hazards procedures
- Staff safety training
- Threat assessment
- Discipline
- Harassment and bullying
- Use of technology
- School engagement and truancy
- Pandemic procedures
- Food allergies and handling procedures
- Mail handling procedures
- Drug and alcohol prevention
- Student safety training
- Staff assignments for supervision of students within layers (see below)
- Violence prevention, awareness and reporting procedures
- Suicide prevention, response and reporting
- Mental health issues (e.g., depression)
- Child abuse
- Violence prevention, awareness and reporting procedures
- Plans and procedures for students, staff and community members with disabilities For further info see emergency procedures[4] and guidelines from Safe and Sound Schools.

C. **District-Wide Physical Security Standards.** Managing physical security resources includes strategic planning, identifying goals and performance objectives and justifying and applying a realistic budget. Every school district should establish and implement security standards for its facilities to guide this process. The PASS Guidelines provide a resource that may be used in the development of such standards and the prioritization of related security initiatives.

4 https://www.safeandsoundschools.org/resources

© 2025 Partner Alliance for Safer Schools

D. **Annual Physical Security Assessments Based on District-Wide Standards.** A proper school security assessment examines five safety areas: safety, security, climate, culture and emergency preparedness.

- **Safety**–the risk associated with the most common and most serious school safety incidents, such as parking lot and playground injuries and fatalities
- **Security**–an evaluation of access control, visitor management, video surveillance, locks, security policies and other approaches to reduce risks associated with the risk of school violence and other types of criminal activity
- **Climate**–assessing the perceptions of those within the school community
- **Culture**–the values and behavioral norms of students, parents and staff that relate to the other safety areas
- **Emergency Preparedness**–a thorough and holistic evaluation of emergency response preparedness provides the best opportunity to prevent death and serious injury once a crisis occurs

E. **Ensure Maintenance of Security Technology Implementations.** The implementation of security and life safety technology creates a district-wide responsibility to ensure this equipment is always properly maintained and operational; this is commonly accomplished through carrying out a program of periodic testing, either by staff or through built-in monitoring features or third-party monitoring services that can warn staff when electronic equipment is not functioning properly. One of the best ways to address equipment failures is to ensure that installation agreements provide for timely equipment replacement when necessary. Additionally, some school districts (especially larger districts) employ security technicians who can troubleshoot and repair problems immediately. It is important to note that many security equipment manufacturers offer training and certifications that technicians working with this equipment should obtain. At minimum, a yearly test should be conducted on all security technology implementations.

F. **Incident Report Documentation System.** To improve mitigation efforts and responses to future events, school districts should thoroughly document all safety- and security-related events or policy violations that take place within the district, no matter how minor; this documentation can be accomplished by assigning a staff member to document and maintain records of all incidents for the district. This system can be as simple as maintaining a basic electronic spreadsheet or using professional report documentation software. Incident data should be categorized as specifically as possible to better enable the most useful analysis possible, which can be used to educate stakeholders about factors influencing security operations.

G. **Conduct Lockdown Drills.** Creating a safe environment so children and educators can focus on learning is the goal of school security and safety professionals. Drills and exercises are part of a comprehensive approach to ensuring a safe learning environment, and best practices should reflect this.

Drills are common in the school environment, whether in language or math education, sports practice or safety. Exercises are common to improve skills in specific areas or disciplines.

School safety drills and exercises are no different. To ensure a safe environment during the school day, common drills repeated during the school year are the accepted practice. For years, the standard "fire drill" practice has been to line up, exit the classroom single file and march to a safe rally area, such as the schoolyard.

The need for "lockdown" drills has grown due to the unique circumstances of the active shooter or assailant. Whether in a school, business or other public space, best practices now dictate having a lockdown protocol as the major component of

© 2025 Partner Alliance for Safer Schools

an effective safety plan when escape is not possible. Other components may include methods to secure your area prior to sheltering notification and communication during an event.

In the school safety context, it is critical to distinguish between drills and exercises. Drills are educational opportunities to test processes, procedures and technologies. Exercises are mainly for first responders to test their training.

DESIGNING A DRILL

Lessons learned from decades of school fire drills may be employed here. What is an appropriate approach for schools to take as they plan, prepare and practice for protecting children and staff from danger that is inside the building?

Start with standardizing the term by calling these drills "lockdown" drills, as called for by the National Association of School Resources Officers (NASRO) and National Association of School Psychologists (NASP), and not "active shooter" drills or "active assailant" drills. PASS supports NASRO and NASP's position on designing drills. A lockdown should be looked at as an active threat situation, or a situation that presents an immediate and ongoing danger to the safety of students, staff and visitors. In addition to individuals using firearms (active shooters), other types of weapons and erratic behavior can also create active threat (lockdown) situations.

A NOTE OF CAUTION WHEN DESIGNING DRILLS

Some have called for making these drills realistic; however, schools are not set on fire to practice fire drills. Firefighters do not run through the building yelling at students and staff during fire drills. Firefighters use practice "exercises" to train in fighting fires. Schools have "drills" to educate/train students on how to evacuate the building in the event of a fire. Drills should be conducted in an educational way–there is no need for violent simulations.

WHAT SHOULD BE TAUGHT IN A DRILL?

Both staff and students should be educated about the options that can be used in an active threat situation. Realistically, students and staff are not always in their classrooms or behind closed doors as they go throughout their busy school days; because of this, students and staff should be taught additional strategies that go beyond just sheltering in a classroom. For example, there are other shelter options that should be taught, like what a staff member or student should do when in a bathroom, cafeteria, or hallway if an active threat arises. This is where evacuation (evade) or distraction (defend) strategies could come into play. Another critical option that staff and students can be educated on is care, which could be first aid or just being helpful to others in these situations.

When a lockdown drill occurs at an elementary school, it should be conducted when the majority of the school is sheltered inside and when some classes are outside at recess. The staff and students at recess could practice how to safely leave the school grounds to seek safety. Students in a secondary school can be taught what to do if they are caught in different locations inside and outside the school. Those at recess need to know what their options are outside the building, and they should be guided through the options. Age-appropriate strategies can also be offered as classroom lessons, wherein students are told about the different options that they may consider in an active threat situation.

Additional training, such as basic first aid, should also be considered when creating a lockdown drill. Many local emergency medical responders, the Red Cross and other organizations can provide age-appropriate training for students and staff.

© 2025 Partner Alliance for Safer Schools

8 PASS Recommendations for Conducting School Safety Drills

1. ***Purpose:*** Drills should be conducted in a way that is educational and involves the practice and testing of established processes, procedures and technologies. They should not involve violent simulations that could be traumatizing to participants.

2. ***Scheduling:*** Drills should be announced to staff, students and parents and include a scheduled time frame in which the drill will be conducted (e.g., Monday between 9 a.m. and noon). Drills should not be conducted in a "surprise" fashion.

3. ***Duration:*** Drills should be short and conducted as quickly and efficiently as possible.

4. ***Times and locations:*** Drills should be conducted at varying times throughout the school day–recess, passing periods and lunch time–and during after-hours activities such as child care and athletics.

5. ***Evaluation:*** Staff should be debriefed immediately following a drill where feedback can be exchanged. Drills should be run for other groups such as after-school child care and athletics.

6. ***Frequency:*** At least two lockdown drills should be conducted each school year. It is recommended to practice within the first 20 days of the start of the school year and within the first 20 days after winter break.

7. ***Drills vs. exercises:*** Any participants selected for "exercises" should be volunteers and be carefully selected, given the significant difference between a drill and an exercise. Drills involve all or most occupants of a school facility to test processes, procedures and technologies. Exercises are mainly for first responders to test their training.

8. ***Safety awareness levels:*** Drill design should be tailored to desired levels of safety awareness, which will vary depending on the developmental levels of students and the capabilities and training of staff involved. PASS recommends referring to Safe and Sound Schools' Developmental Levels of Safety Awareness resource[5] to help guide this process.

5 "Safe and Sound Schools' Developmental Levels of Safety Awareness, https://d12b1c87-439e-47fd-8767-5821f38c7b68.usrfiles.com/ugd/d12b1c_b2fb-99d2a0d1412ebf41fb713db7f2d1.pdf

© 2025 Partner Alliance for Safer Schools

TIER 4

A. **Independent Security Assessment on 3-Year Cycle.** Third-party assessments help school districts identify potential vulnerabilities and strengths relating to security and safety for students, staff and visitors. An evaluator should have considerable documented experience in conducting security and safety assessments for school systems.

Assessments should take a holistic look at a district's safety and security posture and include the following areas:

- Effectiveness of policies, plans and procedures
- Visitor screening procedures
- Use of CPTED
- Access points
- Analysis of surrounding neighborhoods
- Anti-terrorism measures
- Liability reduction opportunities
- Access control (building perimeter and interior)
- Video surveillance systems
- Alarm systems
- Student supervision
- School climate
- Bullying abatement strategies

VISITOR MANAGEMENT SYSTEM:

TIER 1

A. **Visitor Badging System.** Every school should have a visitor badging system. While these systems can range from basic to advanced, at a minimum, visitor badges should be issued to all individuals visiting schools who are not staff or students. A school should sign all visitors into a log using the visitors' government-issued identification cards and check the student information system to ensure that visitors are allowed on campus.

Each visitor should be issued a badge that includes:

- School name and logo
- Text that says "VISITOR" in large, bold font
- Name of visitor
- Expiration date and time
- Color code allowing staff to easily identify the type of visitor (e.g., parents are green, vendors are blue, volunteers are yellow)

© 2025 Partner Alliance for Safer Schools

TIER 2

A. **Electronic Visitor Management System.** Visitor management systems are technological solutions that streamline the visitor sign-in process and track specific visitor data such as who is entering the school and when, the reason for the visit and who was visited. Many systems record photos of the visitors or scan driver's licenses that are presented by visitors not only to help confirm the identity of the presenter, but also to check for persons that should not be permitted to enter for a variety of reasons, such as restraining orders or parental rights disputes. This usually involves checking the ID against the National Sex Offender Database but can also involve criminal background checks. Most solutions also have built-in volunteer tracking capabilities that allow school districts to track their hours, which is helpful to those that use these hours for property tax rebates and other purposes. Most systems also have built-in badging services.

ID Scanning Technology–A Key Element of Visitor Management Systems.

There are two primary scanning methods used by the industry which are 2D barcode scanning and optical character recognition (OCR). 2D barcoding offers the advantages of being less prone to misreading errors and the photo and scanning equipment tends to be less expensive. The OCR advantage is that the reading process happens in a single step. Generally, both processes should not take more than 30 seconds.

PASS recommends that visitor management systems utilize the National Sex Offender registry[6] for screening visitors. A prohibited person registry is a capability that your visitor management system should offer. Prohibited person registries are generally maintained by the school district and include information on people issues, like "no trespass" orders, domestic situations and other flagged persons.

PASS recommends when implementing a visitor management system that good policies and procedures are developed. Policy and procedures should address the alert notification process on when a positive hit is received. This should address the sending of alerts if a visitor appears to be on the sex offender registry, but how to verify (by photo) if the visitor and sex offender are the same person; how to handle "false" positives and how to include comments about the visitor for future handling at the campus or other campuses in the district.

PASS recommends that when a visitor management system is installed that it be monitored district wide as well. When a visitor enters a school, your front office staff should be able to see where they have been in the district and if appropriate, add notes that can be viewed by staff at other campuses. It is valuable to have a one-button report of everyone on campus in case of emergencies, but it can also be beneficial to see everywhere a visitor has been throughout the school year. If your district has a security operations center, they can help monitor this global process and clear positive and false positive matches.

6 https://www.nsopw.gov/

© 2025 Partner Alliance for Safer Schools

TIER 4

A. **Visitor Management System-assisted Background Checks.** The higher-tier visitor management system implementation provides the capability to run criminal background checks for all volunteers. This feature is typically done through a pre-enrollment process. Potential volunteers will pre-enroll through a web link set up by the district and provided by the visitor management company. As recommended in Tier 3, it is important for a district to have good policy and procedures in place that shows how a district will deal with someone with a record, what convictions limit a person from serving as a volunteer and who has the authority to decide whether a visitor will or will not be restricted from entering one or all schools. It is very common for a visitor management system to also report criminal records that have been sealed. Policies should be developed to address that scenario as well.

STUDENT AND STAFF IDENTIFICATION:

TIER 1

A. **Volunteer Background Checks**. Volunteers play an increasingly important role in the school community by providing many hours of their time to mentor, coach and tutor students and additionally supplement staff in many ways; however, volunteers also present a security vulnerability that many districts have struggled to address, requiring a balance between properly screening out unqualified individuals and encouraging participation from dedicated, privacy-conscious volunteers. School districts should screen volunteers to verify their identities and identify any potential problems, especially problems that could arise from an undisclosed criminal history. Some states require or facilitate school volunteer background checks, while others have no established screening requirements.

   Laws that require volunteer screening generally specify only that the individual undergo a criminal history check or a criminal history check plus a check of sex offender registries. Each school district should draft a policy regarding volunteers and what type of background check they should obtain. Failure to maintain trust can be devastating to an organization and lead to loss of community support, loss of funding or even a lawsuit for negligent selection of a volunteer. Even when faced with an incident involving a volunteer, a district will fare better by having made a good faith effort to conduct a background check before the incident occurred.

TIER 3

A. **Smart Card Identification Badges.** In more advanced implementations, smart cards with radio frequency identification (RFID) or near field communication (NFC) technology allow students and/or staff to check in electronically to the building, classrooms, buses and any other place where there is a need for documentation and accountability and provide a mechanism for secure payment in cafeterias. Since smart cards are coded with an electronic profile that is assigned to the card owner, additional functionality, including use across access control systems, can easily be added when necessary. In a phased implementation, school districts can start with a basic ID system and add other features later when budgets allow or needs change.

© 2025 Partner Alliance for Safer Schools

PEOPLE (ROLES AND TRAINING):

TIER 1

A. **Panic Alarm Activation.** Staff that are responsible for activating a panic alarm should be trained on what type of incidents require activation of the panic alarm system. The district/school should use an escalation tool, such as the escalation continuum by the Crisis Prevention Institute (CPI) or other evidence-based continuum models that address violence in schools. This training could assist in identifying at what point a panic alarm should be initiated.[7]

   Providers of panic alarm systems should at a minimum provide training and education to the school or district in regard to changes in policy and procedure. Examples of educational information include how the system will operate, when a panic alarm is to be pressed, why an alarm is activated and what happens upon alarm activation. In addition, system providers should provide training of all staff and/or students that may use the system.

ARCHITECTURAL COMPONENT:

TIER 1

A. **Facility and Vicinity Mapping.** As noted within the Policies and Procedures component, schools present unique challenges to emergency responders due to their size, complexity and occupants. Responders require extensive amounts of detailed, yet easily understandable information in the event of an attack or other emergency at a school. Districts should ensure that each facility can provide an overall floor plan, a roof plan, fire, HVAC, security systems and other emergency information useful to police, fire and other emergency partners.

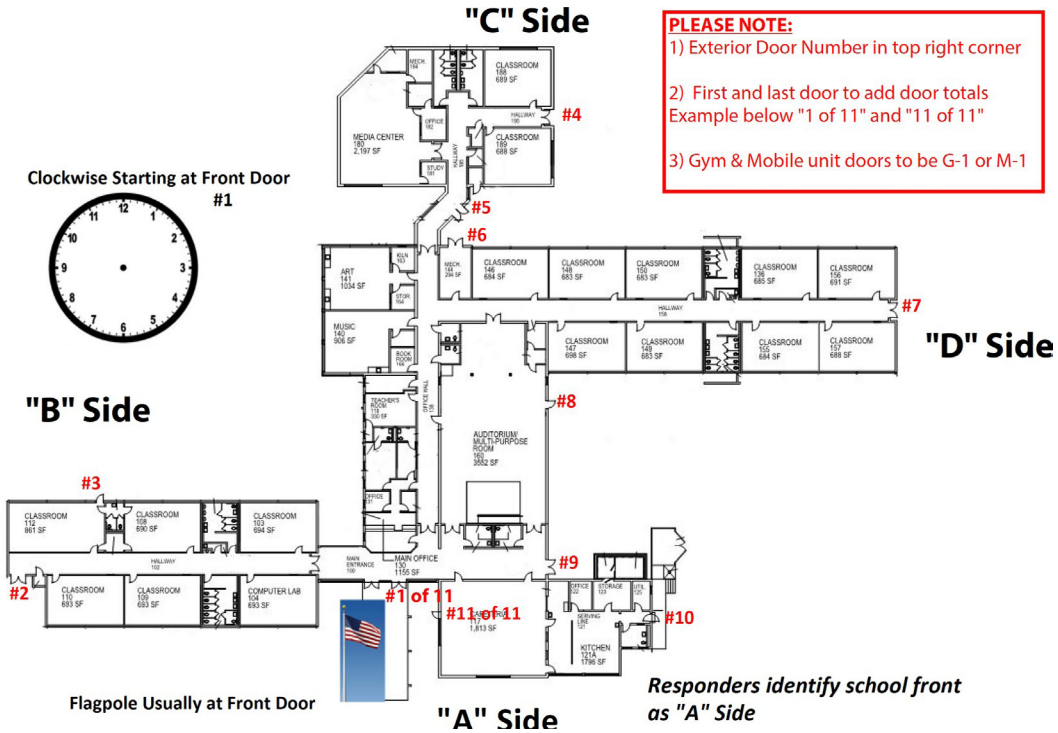
   At a minimum, this information should include:

   - Location of the rapid access security vault (RASV), a secure storage device where access credentials (keys, cards) are kept for emergency access.
   - Printed or electronic copy of "As-Built/Record Drawing" of facility. Plans should include all room names and associated numbers.
   - Printed or electronic copy of an aerial view of the subject facility. This should include a minimum five-block radius outside the campus perimeter.

B. **Entrances Marked with First Responder Numbering System**. All entry doors should be clearly marked with a first responder door numbering system, in coordination with local police and fire officials, to ease identification of entry points during emergency or tactical situations. Numbers should be made of reflective material like the numbers on a mailbox. The number system should be clear to the first responder as to where the door is within the relation to the layout of the school. While door numbering conventions in use share many similarities, PASS recommends adoption of the following convention (see figure) for greater consistency nationwide, which has been adopted by the Georgia Department of Education and is similar to the convention used by the Center for Safe Schools in Pennsylvania, the New Hampshire Department of Safety and others, where labeling begins at the main entrance and proceeds clockwise around the building.

7 https://www.crisisprevention.com)

© 2025 Partner Alliance for Safer Schools



TIER 2

A. **Printed or Electronic Tactical Floor Plans.** In addition to as-built/record drawings of the subject facility, "tactical floor plans" include basic room name/numbers and identification of security cameras and other access control devices.

TIER 3

A. **Zone Emergency Response System.** A zone emergency response system is an improved emergency response system and method for use in responding to emergencies and reducing the time it takes to get responders to the right location in a building or campus. An emergency dispatcher, or electronic equivalent, can reference designated directional zones to relay important directional information regarding a target location to first responders, regardless of whether additional premises-related information is immediately available. In addition, the zones can be displayed in a superimposed manner relative to mapped features of the local premises, such as satellite photos, site maps, architectural plans, etc.

TIER 4

A. **Virtual Response Plans and Implementation.** There are a number of products and resources available to create a digital, three-dimensional representation of a facility that allows users to virtually "walk through" the environment while accessing information about its features and toggling between a range of display views from "tactical" to "comprehensive strategic" features.

© 2025 Partner Alliance for Safer Schools

COMMUNICATION COMPONENT:

TIER 1

A. **Wide-Area Two-Way Radio System.** From a district-wide perspective, a two-way radio communication system is recommended to quickly and efficiently communicate threats to the district or to certain schools within the district. A wide area network radio system allows reliable voice communications with key district staff who would be the first to respond in an emergency. The system should allow all administrators, principals, security personnel and transportation staff to have two-way radios. Since public schools are government entities, commercial radio systems licensed under the Federal Communications Commission (FCC) Universal Licensing System[8] must be used by those entities, not off-the-shelf consumer products or radios designed for recreational use.

B. **Bi-Directional Amplifier (BDA) or Distributed Antenna Systems (DAS).** These technologies boost reception in and around buildings for emergency personnel radio networks on 700 MHz, 800 MHz and 900 MHz bands, as well as mobile phones and other devices if needed, where it would otherwise be inconsistent or unavailable due to surrounding construction materials or other factors. BDA systems use special cabling and boost all carrier networks, while distributed antenna systems use a series of antennas and typically cover larger areas for a single carrier network. Hybrid systems that combine these elements are also being implemented. PASS recommends consulting with a radio systems integrator and contacting both local law enforcement and fire departments that may have either a standard for such technologies or require the appropriate NFPA code, to coordinate the best plan to implement these technologies throughout a district.

TIER 2

A. **Trunked Radio System.** A trunked radio system allows organization of users into different groups and provides the capability to communicate on frequencies used by police, fire, EMS and other first responders in the community, whereas traditional two- way radio systems may be confined to a certain band (frequency) exclusive to the system.

B. **Mass Notification Unified With Public Address/Audio-Visual PA.** On a district level, AV/Public Address systems that are installed in each school should have the ability to be networked so that the district can use the mass notification system to provide district-wide communication to school facilities. There are several technologies currently available that allow for the individual communication systems to be unified. Some examples of unification can include:

    a. Integrating with the fire alarm/voice communication systems

    b. Legacy public address (PA) systems can be interfaced via IP technology to unify the communication system at a district level

    c. IP Phone systems can be interfaced to unify communication systems at a district level

    d. Interfacing to the trunked radio system

C. **Unification of Access Control and Communication Systems:** The unification of the access control and communication systems allow for automation of procedures for emergency events as well as the ability for one interface for initiation of an emergency procedure. For example, on an active threat event, the access control system can automate the simultaneous transmission of emergency

8 For a license example, see https://wireless2.fcc.gov/UlsApp/ApplicationSearch/applMain.jsp?applID=9075468

© 2025 Partner Alliance for Safer Schools

communication. Another example of unification is the ability to combine the audio from the door entry system to the communications system. PASS recommends reviewing the Access Control component in this section for other ways to automate activation of procedures for restricting access to appropriate first responders.

D. **Unification of Detection and Alarm with Communication Systems:** The unification of the detection and alarm systems with the communication system allows for automation of emergency procedures as well. For example, the activation of a panic alarm can automate the simultaneous transmission of emergency messages.

E. **Unification of Video Surveillance with Communication Systems:** The unification of video surveillance and communication systems provides an additional level of deterrence. The ability to use the real time video from the surveillance system can be coupled with ability to communicate potential threats as well as assist in confirming that appropriate doors are closed and building occupants are leaving evacuated areas.. See Video Surveillance component for information on audio recording.

F. **Unification of Building Architecture:** A site survey should be completed that includes assessment of audio levels, building/hall layout and ambient noise during class change to ensure its reach to cover all learning, administrative areas, and building exterior including parking lots and public space.

WEATHER MONITORING:

The most likely risk a school may face on any given day is a weather emergency. In their emergency preparedness protocols, school districts should practice for the types of weather emergencies that they may face.

TIER 1

A. **Monitor National Oceanic and Atmospheric Administration (NOAA) Local Weather Information.** One of the simplest means for weather monitoring is for each school to monitor the local NOAA weather feed[9] for their community and use a NOAA weather radio. A school district should ensure adequate pre-incident planning in monitoring the upcoming weather conditions to prepare for emergencies.

TIER 2

A. **Weather Monitoring Service.** Subscription-based services are available that provide specialized weather monitoring such as site-specific weather notifications as well as access to 24-hour meteorological consultation. This can play an important role in areas prone to weather dangers such as lighting and tornados. Site-specific warning technology typically includes lighting proximity and all-clear notifications that can help protect students and staff participation in outdoor events.

TIER 4

A. **Weather Monitoring Station at a Central School Facility.** The most effective way for a school district to address weather emergencies is to install a weather monitoring station at a centralized school facility location; this provides the most accurate information on the actual weather conditions in an area and helps ensure actions taken are not based on

9 https://www.noaa.gov/weather

© 2025 Partner Alliance for Safer Schools

inaccurate or incomplete information from other sources. Weather stations also benefit education programs by providing classes with access to weather data. The community can benefit in other ways as well, through incentives offered by the private sector to school districts to install weather stations at schools. This data is shared with and used by the community through various weather monitoring smartphone apps, including apps that provide information on live weather conditions and the threat from severe weather events such as lightning, hail, strong winds, heavy snow, hurricanes, flooding and other weather conditions that would impact school safety. Multiple weather stations may be required to achieve the same in-house functionality for a district that spans large geographic areas, with recommended placement every 10 miles for the most site-specific accuracy.

ACCESS CONTROL COMPONENT:

Controlling access to school buildings is fundamental to securing the school environment. Access control can consist of both mechanical and electronic systems. **Mechanical systems** are locking devices with mechanical keys, and **electronic systems** consist of electronically controlled locking mechanisms, card readers and cards.

A limited number of key operated openings should be provided to allow access to different areas of the property, parking lot and building from the exterior in the event alternate access to the building is required. Electronic access control is a preferred approach, as electronics allow control of access to specific openings at specific times. Emergency access through an RASV should be provided at multiple locations around the building, or at property and parking lot perimeters if secured, to ensure rapid access. Districts should provide access credentials to the RASV to all emergency responders.

TIER 1

A. **Emergency Site Building Access System for First Responders.** Mechanical keys or cards should be available to district and community emergency responders for all mechanically or electronically controlled openings to provide emergency access. Access credentials and other necessary keys should be placed in a designated lock box or other rapid access system (RAS) in use locally. While emergency access is critical, access to keys and cards should be tightly controlled and limited to key personnel and first responders.

   For electronically access controlled doors it is important for the district to work with the access control provider to determine how emergency access by first responders will be granted in an emergency situation.

TIER 3

A. **Access Control System Equipped with Remote Door Release and Lockdown Capability.** The control of an access system through a remote connection allows designated school personnel to open or lock any door that is part of an electronic access control system. This remote capability can typically be accomplished via an access control system smartphone app, a laptop connection to the school network, and designated computers at a dispatch or emergency operations center, and also provides emergency entry by law enforcement or other first responders. Additionally, schools should consider establishing system access rights that limit these capabilities only to those staff members responsible for responding to emergencies (SROs, safety personnel, and designated administrators).

© 2025 Partner Alliance for Safer Schools

TIER 4

A. **Electronic Access Control for MDF and IDF Rooms With Key Override.** Main Distribution Frame (MDF) and Intermediate Distribution Frame (IDF) rooms house and protect district network infrastructure.

TRANSPORTATION:

On any given day in America, millions of students ride school buses to and from school. Many of the same security technologies that have been deployed in schools are now deployed on buses. One of the most important practices is the deployment of advanced communications equipment that goes beyond traditional radio use. Bus communications platforms provide digital radio communications, GPS tracking, student accounting, text and email communications, engine diagnostics, driver behavior analysis and other data. Fully using these capabilities also provides the opportunity for school districts to streamline transportation costs.

TIER 1

A. **Interoperable Radio System for All Buses and School Vehicles.** All buses and other school vehicles should be equipped with interoperable radio systems, connecting administration, principals, teachers, security, maintenance, bus drivers, coaches and law enforcement agencies. By equipping staff and bus fleets with two-way radios and bridging software, schools can communicate directly with other responders when an emergency occurs. Whether providing care for an injured student, reporting weather conditions or situational information, this information can be shared instantly with responding agencies and other school personnel. To achieve radio interoperability, a district must coordinate with other community stakeholders, including local law enforcement agencies. Throughout the country most jurisdictions use the same two-way radio communication systems that allow users sharing the same range of frequency to communicate with the others in emergencies (trunked systems).

TIER 2

A. **Bus Video Surveillance/GPS System.** School bus surveillance systems provide an increasing number of safety and security benefits. Increases in both capability and affordability have led many districts to implement this technology. A typical school bus camera system consists of two to eight specialized mobile cameras and a mobile digital video recorder for each vehicle, with GPS. Camera systems can both monitor the inside of the vehicle, including driver/operator behaviors during routes, and record the external environment through outward-facing cameras. In addition to video data, the system can record signals from the vehicle, including braking, right and left turning, warning lights and stop-arm deployment; it can also record sensor events such as vehicle speed, alarms and idle time. Sensors can be integrated that measure any amount of force that was exerted on the vehicle during the route. For example, if the driver took a hard turn, or if there was a collision with another vehicle, the force of movement would be measured by the sensor, which can trigger an alarm event that can be quickly retrieved from the video. Importantly, school bus cameras can also capture student and driver behaviors, which could be vitally important in the review of an incident by school officials. GPS tracking allows a school district to know where buses and school vehicles are in real time, as well as possible integration with check-in systems. GPS features can be configured to record the location of the device at regular intervals (data loggers), report location and other vehicle data wirelessly in real time (data pushers) or allow users to remotely request and retrieve such information (data pullers) when connectivity or power is available intermittently and real-time data is not required.

© 2025 Partner Alliance for Safer Schools

TIER 4

A. **Card-Based Check-In.** School districts can deploy smart ID card systems to increase bus rider accountability and security. Such cards are embedded with RFID technology or NFC to log when and where a student boards and exits the bus. This information allows school officials to know whether students were on the right buses and if they got off at the right stops. These cards can also be used to alert parents of where their child's bus is and when their child has entered or exited the bus.

VIDEO SURVEILLANCE COMPONENT:

Video surveillance is an integral component of a school's physical security plan. It provides deterrence, detection and, in more advanced implementations, enhanced response to a variety of daily challenges experienced at schools.

Video surveillance uses include:

- Surveillance–Monitoring video in real time, either manually or through an automated process
- Assessment–Viewing recorded video to assess a situation that is currently happening or recently happened
- Forensics–Using recorded video data to provide a record of what actually happened during an event, including use as evidence of unlawful or impermissible activity
- Risk Mitigation–Using video analytics to proactively notify security or other personnel that an event is taking place

For decades, video recordings have been used in a forensic capacity to help determine the (who, what, when and where) of an incident after the fact. As video technology has advanced, so have the capabilities enabling security professionals to leverage video as a proactive tool that helps mitigate risks even as events unfold. Much of this capability has been enabled through the widespread use and increasing affordability of IP cameras. Harnessing these advances aligns with a tiered approach. While some analog video systems are still in use, new installations for K-12 should be specified with IP cameras as a fully networked system. Existing analog systems should be updated as funds become available, as the nature of video surveillance technology allows for updating functionality over time without replacing earlier investments.

IP camera systems evaluated should have the capabilities to provide for integrations such as video analytics and artificial intelligence-enabled functions.

Management of video surveillance assets and use policy at the district level will help ensure the most effective use of the technology to support safety and security across facilities and the most efficient use of resources.

Video Analytics

Video analytics generally have two different purposes: forensic and preventative. Forensic use of video analytics is using the analytics to "tag" recorded video for later forensic research. Preventative use of analytics is the use of analytics to generate an alert during the "live" event in order to respond to a potential threat.

Video analytics describes the process of observing and analyzing recorded video content to transform real-time information into intelligent and actionable insights. Smart video analytics for security systems use specialized artificial

© 2025 Partner Alliance for Safer Schools

intelligence (AI) and machine learning technologies to continuously observe video footage, with programs configured to automatically detect suspicious and anomalous events.

In operation, this enables active video security systems to identify and observe various objects and stimuli associated with security incidents without assistance from human operators. For example, video analytics systems can autonomously detect and observe vehicles, persons of interest, contraband items and unusual objects, warning staff of events that may require attention.

Choosing to deploy video analytics security tools removes the need for on-site personnel to manually observe video feeds continuously. Instead, AI programs ensure sites are well-observed by warning security staff of events that require their attention and response.

Types of Video Analytics

The business intelligence gathered through monitoring video surveillance streams in real-time using video analytics software, helps to identify patterns, attributes, and events of interest. Close human-based monitoring of many video feeds is simply not possible. With video analytics, the system can alert video operators of key events and automatically trigger specific actions or procedures.

Here are the most common types of video analytics:

Motion Detection

Video motion detection (VMD) is a feature that senses physical movement for a given area in real-time. Motion detection analytics are embedded in IP cameras, network video recorders, video analytics and video management software systems.

Automatic License Plate Recognition (ALPR)

Automatic license-plate recognition (ALPR) uses optical character recognition (OCR) technology on the captured video to identify and read vehicle license plates. Source videos can come from existing closed-circuit television (CCTV) or video cameras, law enforcement cameras, or high-speed ALPR cameras mounted on roadway infrastructures.

Facial Recognition

Face recognition (or more specifically, facial recognition) technology is capable of detecting and matching human faces from digital IP video. This data is typically compared against enrolled images, such as a database of authenticated users by matching unique facial features. Facial recognition video analytics can improve building and perimeter security and by alerting staff to the presence of a specific person, or quickly finding images of a person (such as a missing child) within vast amounts of video data. To prevent spoofing (such as holding a picture of a person up to the camera to impersonate an authenticated user), spatial recognition (ensuring the image is not generated from a two-dimensional source), as well as liveliness checks (the subtle movement of facial features), are typically deployed as additional features.

© 2025 Partner Alliance for Safer Schools

Crowd Detection

Crowd detection allows for the detection of crowd density to evaluate capacity or occupancy issues within a defined area. Applications of crowd detection include population counting, public event management, disaster management, safety monitoring, and suspicious activity detection (i.e. crowd of people in a prohibited area).

People Tracking

This feature shows the past or present movement of individuals within a defined area. Applications of people tracking include intrusion detection, wrong-way detection, people counting, physical distancing and customer behavior analysis.

Left and Removed Item Detection

Left and removed item detection is a video analytics technology based on monitoring the appearance and disappearance of static objects within a defined area. There is a vast range of beneficial applications. The technology is often deployed in public areas like airports or subways to detect potential bombs, although it can also be used to ensure fire escape areas remain clear and unobstructed.

Motion Tracking

Motion tracking in video surveillance is designed to detect objects moving within a predefined area of interest reliably. Motion tracking impacts a wide range of industries, including the military, critical infrastructures, entertainment, sports, healthcare, and robotics.

Object Tracking

Outdoor object tracking is a video analytic for detecting and monitoring the movement of vehicles and people in outdoor environments. Applications of object tracking include traffic control, visual surveillance, forensics, human-object interaction, gesture recognition and augmented reality. AI-based object tracking analytics can identify the type of object, such as vehicle or person.

People Counting

People counters are video analytics optimized for indoor usage that count the number of people passing through a specified area. Benefits can include occupancy control, capacity evaluation, sales and conversion metrics, personalized visitor experiences and measuring operational effectiveness.

PTZ Auto-Tracking

Pan-tilt-zoom (PTZ) auto-tracking video analytics enable video surveillance cameras to follow and zoom in on people and vehicles within a field of view. Some benefits of PTZ auto-tracking include a larger field of view with fewer blind spots, motion tracking, and cost savings. Auto PTZ also enables an operator to monitor an event while leaving his or her hands-free to perform other tasks, such as using a telephone or engaging in other deterrent activities.

© 2025 Partner Alliance for Safer Schools

TIER 1

A. **Incorporation of Video Surveillance into Emergency Response Plans.** Use of video surveillance to provide remote situational awareness during incidents should be incorporated into emergency response plans. Valuable information can be relayed to law enforcement responders who are enroute to or, in the case of EMS, waiting to enter a facility. Law enforcement may use video surveillance to determine the threat level of a given area. For example, under the NFPA 3000 standard for responding to active shooter events, control zones are established that define the threat level of an area and the personnel or competencies that are needed to operate in that area. Defined as hot, warm and cold, assignment of these areas is the responsibility of law enforcement. Information from the video surveillance system may provide key information necessary for making this determination, which could mean the difference between EMS entering an area or not.

   The plan should also document who is responsible for operating the video surveillance system during an emergency and how they will communicate with law enforcement. In many cases, law enforcement may have access to the video directly or may request access to the video surveillance on site. In either case, schools should still assign someone to this role so that they can assist law enforcement if needed. This person should be trained in the use of the system and included in emergency drills and have a backup in case that person is not on site or incapacitated.

TIER 2

A. **Camera Standardization**. Equipment standardization provides better life cycle management options and shortens downtime when devices fail or are damaged. At the district level, schools should consider standardizing on specific camera models based on intended use, such as "hallway cameras," "parking lot pan-tilt-zoom (PTZ)" or "entrance/exit cameras." This does not necessarily mean standardizing one manufacturer's products district-wide; rather, it means making consistent decisions on devices that meet operational requirements for given types of locations. It is not uncommon to have equipment produced by multiple manufacturers recording to the same video management system, but by limiting the number of different models installed, districts can keep on hand spare equipment that can be rapidly deployed if needed.

   As IP cameras have advanced, all new cameras purchased by the district should consider having audio capabilities. The ability to record audio in certain areas can be an asset for districts. Areas of the building such as the main office, secure visitor entry center and known areas of bullying can assist in alerting the district to potential threats. Audio analytics are now available to detect audio aggression and have keywords that prompt an alert and/or recording of an event. Districts should investigate the potential issues with audio recording with the district's general counsel before implementing audio analytics.

B. **Recording System Standardization.** The standardization of video surveillance recording devices should be considered to provide a consistent user interface and experience across all schools in the district. This will decrease operational training costs by having only one system with which security personnel need to be proficient. Standardization enables the assignment of backup personnel for staff across different schools in the district to be integrated into emergency response plans; it also provides better life cycle management options for the district.

© 2025 Partner Alliance for Safer Schools

Most importantly, standardizing on a specific video management system provides a district with the ability for a centralized security operations center (SOC) to help manage video surveillance at schools throughout the district. Many districts have multiple recording platforms that have been deployed over the years at different schools. If the upfront cost to bring these systems under one platform is prohibitive, a planned migration can be established that defines the decision criteria for bringing schools into the new system as budgets allow.

C. **Recording System Use of Video Analytics.** Certain video analytics should be used for recording purposes to assist in reacting to emergencies or to speed up forensic investigation of events that have occurred. Common video analytics enabling a reactive approach include motion detection, perimeter detection and object detection.

D. **Unification of Panic Systems with Video Surveillance System:** The panic alarm system should provide an automated "alert" to the video surveillance system that will activate functions of the video surveillance system that are critical to live event information. Video surveillance systems have the ability to take information from the panic alarm system so that video from appropriate cameras is automatically provided to the SOC, provide an alert to persons monitoring the video surveillance system, in addition to providing real time information to first responders.

   Further, with the use of video analytics and AI, video surveillance systems can provide real time detection of specific anomalies in actions or movements inside and outside the building.

E. **Unification of Access Control with Video Surveillance System:** The advantage of a unified access control and video surveillance systems is a key building block to a unified safety and security platform. Unified platforms provide the ability for command and control during emergency situations without going to separate platforms. This strategy saves time and simplifies response.

F. **Unification of Communication with Video Surveillance Systems:** The unification of video surveillance and communication systems provide an additional level of deterrence. The ability to use the real time video from the surveillance system can be coupled with ability to communicate potential threats as well as assist in confirming that appropriate doors are closed, and that building occupants are leaving evacuated areas.

TIER 3

A. **Video Verification of Panic Alarms to a Monitoring Service, Administrators and/or SOC.** An emergency panic system should be integrated with the existing camera system and video available to designated response personnel. Live video access is critical because it provides real-time intelligence for first responders and other staff members responsible for emergency coordination and support. Another option for a school district is to develop their own SOC that replaces the need to hire a third-party organization to monitor alarms. There are staffing, capital and ongoing operational costs associated with this approach to be considered.

B. **Video Verification of Intrusion Alarms to Monitoring Service, Administrators and/or SOC.** Many schools use intrusion detection systems that are monitored by offsite, central station companies that will dispatch law enforcement, EMS, fire or district security personnel based on the nature of the alarm. To reduce false alarms, some locations require alarms to be "verified" before these first responders can be called or dispatched. In the past, this typically meant calling or sending someone to the site of the alarm to verify the alarm. Today, video verification capability provides central

© 2025 Partner Alliance for Safer Schools

station monitoring services with the ability to verify alarms remotely in cases where there is camera coverage of the affected space.

TIER 4

A. **Preventative Use of Video Analytics.** Certain video analytics should be used for creating alerts "real time" to assist in preventing a security incident. Analytics such as loitering, wrong way detection, crowd detection, line-crossing detection and facial recognition can assist in immediately identifying a situation that may have the potential to lead to a security incident.

B. **Brandished Weapons Analytics.** Brandished weapon analytics can provide a way to detect firearms entering in shown (brandished) in a building. The use of brandished weapons technology should be thoroughly investigated before implementation. See PASS Whitepaper[10] on Weapons Detection for more information.

DETECTION AND ALARMS COMPONENT:

Detection and alarm systems use sensors or devices that are generally either hardwired or wireless or a combination of both. A hard-wired system uses devices (e.g., door position switches, latch bolt monitors, motions sensors, glass break detectors) that are physically wired to a control panel that sends an alert to a central monitoring facility. Monitoring can be done via a telephone line, a broadband connection or cellular communications or a combination of these. A wireless system uses similar devices; however, the devices are battery powered and use radio signals to communicate to the control panel rather than a wire. Alerts are transmitted via the same communication mechanisms provided for the hardwired design.

The advantage of a wireless system is the ability to place a sensor or communications device in any location, including a device that staff can carry on their persons. The disadvantage is that radio signals can be affected by the building structure and additional radio communications infrastructure may be required to ensure signals can be transmitted and received from all areas of a school.

Districts should consider both designs when examining the implementation of intrusion detection and panic alarm systems. The type of design (hardwired vs. wireless) and monitoring (centralized vs. decentralized) should be based on the risk assessment and specific MOU established with first responders.

Another important aspect of detection and alarm systems is their ability to be configured as "decentralized" (standalone) or "centralized" (unified) systems. A decentralized system is specific to an individual property and reports alarm events separately, while a centralized system can monitor multiple buildings, alerts and technologies as one unified system. School and district officials should work with local law enforcement and first responders to determine the best system type to use for a facility or facilities. A centralized system allows for advanced features like immediate notification to first responders via two-radio and mobile- and PC-based technologies, while decentralized systems typically rely on a third-party central monitoring station to provide alerts and notifications to first responders.

10 https://passk12.org/whitepapers/what-is-weapons-detection/

© 2025 Partner Alliance for Safer Schools

When evaluating a panic alert solution (such as required under Alyssa's Law where applicable), the type of connectivity must be considered–both existing connectivity inside buildings and outside across the entire school campus including athletic fields, playgrounds, agricultural education areas, driving ranges, bus loops, parking lots, etc.

Depending on the type of system, connectivity capabilities can range from but are not limited to those found in hardwired systems. This may include mobile phone systems that connect through cellular or Wi-Fi, wearable wireless solutions using Bluetooth Low Energy (BLE) that connect directly to the school's secure network, or a combination of methods with redundancies that will automatically switch over to a secondary connection if the primary connection should fail.

School districts should establish a regular test schedule to evaluate the functionality and coverage capacity of all emergency communication systems, not just law enforcement radios, to determine if adequate signal strength is available in all areas of the school's campus.

A mobile panic alert solution should provide a capability that fills those identified connectivity deficiencies. In other words, if the solution is dependent on the same connections that your communications evaluation has identified as having gaps on your campus, then the solution will have gaps in coverage as well.

A top tier solution will include secure network connectivity that is segregated from general use communications which may become vulnerable to overload (does not rely on wi-fi or cellular service), can be tested regularly, has functionality is not limited to a single location or area on campus (only functioning inside a classroom), and has redundancy in connectivity capabilities.

When it comes to panic alarm systems, consider the guidelines below as a place to start:

- Trust your experts, both your current security professionals and those responsible for responding to emergencies at your schools.
- Understand regulatory standards, including Alyssa's Law, United Laboratories (UL), NFPA and IBC.
- Consider the importance of location as it relates to the size of the schools within your district and the need for responders to know where to go inside and outside of the facility.
- Ensure that any panic solution you consider is fit for a life-safety application.
- Know what you can afford in terms of upfront and recurring costs and utilize pilot programs when appropriate.

© 2025 Partner Alliance for Safer Schools

TIER 1

A. **Panic Alarm System in Each Building.** Each building should have a panic alarm system that sends automatic signals to local law enforcement for immediate response. The buttons should automatically notify law enforcement through a 24/7 monitoring station and/or 911 call center. The initiation of a panic alarm system should be in accordance with the local and state law. At minimum, physical panic buttons should be located in the common areas of each building, including but not limited to:

- Front/Main Office
- Counseling Office
- Cafeteria
- Library
- One Per Hallway

Panic alarms, also known as duress alarms, are safety measures that school employees can use to call for immediate help in emergencies. They can be used in a variety of situations, including medical emergencies, active assailant incidents, inclement weather and intruders.

Panic alarms can help schools respond more effectively to emergencies by summoning police or campus staff. In the case of active assailants, the sooner law enforcement is notified, the sooner they can respond and potentially save lives. Duress buttons can also help teachers alert other staff to an emergency so that students and staff can get to safety as quickly as possible.

Panic alarms are typically small and easy to push, so they can be activated without anyone noticing. They can be installed in a variety of places, such as under a desk, on a keyboard, or as a foot pedal on the floor. Some duress alarms can also be worn as a watch or on a lanyard.

PASS recommends that schools consult local law enforcement, security professionals and the district's safety and security team to determine whether the primary areas are enough or additional locations are needed. In addition to the primary locations, secondary locations for panic buttons should also be installed. Secondary locations could include other areas based on our risk assessment and recommendations of the district's safety and security team, local law enforcement and emergency first responders.

B. **Panic Alarms Sent to Law Enforcement.** Once a panic alarm system is in place, it is important to define certain types of security threats that should be immediately sent to local law enforcement. Panic alarms should ideally be sent immediately both to appropriate district staff and to local law enforcement under a MOU governing this process.

. The vast majority of situations in which a panic alarm is triggered will not be an active assailant event. It would be prudent, however, for a district to create a MOU with local law enforcement agencies that all panic alarms should be responded to as though the threat is a worst-case scenario. Not only does this response ensure that local law

© 2025 Partner Alliance for Safer Schools

. enforcement is notified of a threat immediately; it also allows for the accumulation of data to better understand what threats are facing schools in the district and the effectiveness of the policies, procedures and technology involved. The data accumulated should be reviewed with local law enforcement in an effort to make adjustments to the policies, procedures and technology to maximize response efficiency and effectiveness.

C. **Centrally Monitored Intrusion Systems** Intrusion detection provides a significant barrier against threats through deterrence. From a district-wide standpoint, intrusion detection systems are used to mitigate threats to facilities when unoccupied. Preventing unauthorized access to school buildings after hours helps mitigate common threats such as vandalism and theft, but intrusion detection also plays a broader security role, as such access could also enable a range of more serious safety and security concerns. Securing the building through intrusion detection can be as simple as monitoring each exterior doorway through door position sensors and latch bolt sensors that are monitored by a central source. The central source can be a monitoring service, such as one that monitors for fire detection, a local law enforcement emergency operation center or a district security operations center.

   From a district perspective, all school buildings should be monitored for whether an exterior door or window is breached while the building is unoccupied. The technology used to accomplish this can incorporate hard-wired or wireless solutions that are readily available. [11]

   Intrusion detection systems and emergency communication and fire detection systems allow for an easy expansion of panic buttons or similar technology to the system. These duress buttons can be used for active threats, weather emergencies, medical emergencies and other security threats. Like intrusion detection, panic alarms should be monitored by a central source. Additionally, fire alarm systems can have panic buttons added to most addressable systems; districts should work with the local Authority Having Jurisdiction (AHJ) when investigating using the fire alarm for panic alarms.

D. **Fire Alarm Systems.** Fire alarm systems typically work independently of school security systems, due to pre-existing codes by the International Building Code (IBC), National Fire Protection Association (NFPA) and do not have much to do in regard to securing a school building. However, Codes are changing in which fire alarm systems with voice evacuation are being used to communicate additional threats to schools other than fire. PASS recommends that districts work with the local Authority Having Jurisdiction (AHJ) on what is required for each building within the district.

E. **Carbon Monoxide Detection.** Recent changes in IBC and NFPA Code requirements include having carbon monoxide detection in school buildings. Any school building that has gas fired appliances (boilers, HVAC units that use gas for heating, gas water heaters, etc.) need carbon monoxide detection. PASS recommends that the district work with the local Authority Having Jurisdiction to determine whether and how carbon monoxide detection should be installed in each building. Some vape detection technologies can also be used for carbon monoxide detection; however, these devices do NOT meet the requirements of NFPA. See the Enhanced and Emerging Technologies section of the guideline for more information on vape detection.

11 https://passk12.org/duress-alarm/how-to-evaluate-your-duress-alarm-options/

© 2025 Partner Alliance for Safer Schools

TIER 2

A. **Panic Alarms Systems Unified with Access Control, Video Surveillance and Communication Systems.** Panic alarm systems should integrate with the access control system to automatically initiate procedures to secure (lockdown) the building. In addition, the panic alarm system should have an interface to the video surveillance system to alert security personnel that the panic alarm has been initiated as well as show the camera views of the area.

   The emergency communication system should alert building occupants that a panic alert has been initiated. For more information on interfacing the emergency communication system with the Panic Alarm system, see the Communications Component in the Interior/Classroom Layer of this guideline.

B. **Two-Way Emergency Phones.** Depending on the size of the school campus, a parking lot area can encompass a vast amount of space that is difficult to monitor, providing a setting susceptible to threats. It is important to have some sort of two-way communication allowing the persons in the parking lot space to quickly communicate with the security team of the district.

   Two-way emergency phones provide locations from which a person can communicate with the security team of the district. These emergency phones are normally placed strategically and in sufficient numbers so that one is accessible within 200 feet of any location within a parking lot.

   These devices also have the capability to integrate with the video surveillance system to allow for audio and visual communication with security personnel. Use of this technology is particularly important within large campuses that have multiple parking areas.

TIER 3

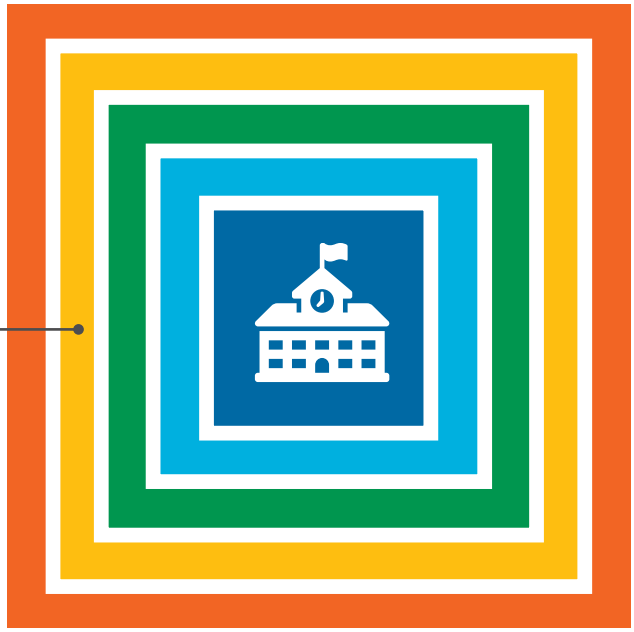
A. **Graphical User Interface for Operators.** School districts should consider providing graphical maps and interfaces that allow users to interact with and monitor unified security system technology in real time. Many school districts utilize a digitized map of a school that displays where the security devices are laid out in their exact locations. Information from camera feeds, card readers and other devices can be easily accessed and monitored in such a manner. For example, motion detectors, latch position and door contacts can be indicated on the map to change color when a change is detected. This real-time information provides staff with instant situational awareness during emergencies.

TIER 4

A. **Intrusion and Duress Alarms Monitored by a District-Wide SOC.** District security personnel that know the facilities, students and staff are in the best position to quickly determine the nature and appropriate response to alarms, managing other security systems and emergency communications from a centralized location. Intrusion and duress alarms monitored by a district SOC is the most desirable implementation because it adds a holistic layer to augment local responders. The advantage of having a SOC is that a district can use technology to further enhance the all-hazards approach, as it can be configured to allow for alarm communications to the SOC for a wider variety of events than those where fire, EMS or law enforcement response would be required.

© 2025 Partner Alliance for Safer Schools

DIGITAL INFRASTRUCTURE LAYER



» QUICKFIND

Digital Infrastructure Layer Checklist 50
Policies And Procedures Component 54
People (Roles And Training) Component 59
Architectural Component 65
Communication Component 71
Access Control Component 73

© 2025 Partner Alliance for Safer Schools

	TIER 1	TIER 2	TIER 3	TIER 4
DIGITAL INFRASTRUCTURE LAYER				
POLICIES AND PROCEDURES				
» Develop and Maintain a Data Privacy Plan	✔	✔	✔	✔
» Vendor Assessment for All New Products	✔	✔	✔	✔
» Supply Chain Risk Management Plan	✔	✔	✔	✔
» Develop and Maintain a System Security Plan		✔	✔	✔
» Hardware and Software Provenance		✔	✔	✔
» Supplier Assessments and Reviews		✔	✔	✔
PII PROCESSING AND TRANSPARENCY				
» Develop a Personally Identifiable Information (PII) Plan	✔	✔	✔	✔
» Identify All PII Stored on the Network	✔	✔	✔	✔
» Do Not Store PII That Is Not Absolutely Necessary	✔	✔	✔	✔
» Privacy Notice Should Be Available To All Personnel at the Time and Location of Collection	✔	✔	✔	✔
IDENTIFICATION AND AUTHENTICATION				
» Access to Physical and Logical Systems	✔	✔	✔	✔
» Removal of Accounts Policy	✔	✔	✔	✔
» Review of Data Before Public Release	✔	✔	✔	✔
» Have a Portable Media Policy	✔	✔	✔	✔
» Wi-Fi Hotspot Policy	✔	✔	✔	✔
» Bring Your Own Device (BYOD) Policy	✔	✔	✔	✔
» Password Requirements	✔	✔	✔	✔
» Ensure That System and Security Logs Are Enabled on All Devices	✔	✔	✔	✔
» Maintain Plan of Actions and Milestones (PO&M) for All Security Controls That Cannot Be Met	✔	✔	✔	✔
» Vendor and Third-Party Services Policy	✔	✔	✔	✔
» Avoid Using Shared Accounts So All Activity Can Be Tied to a Specific User		✔	✔	✔
» Ensure System and Security Logs Are Retained in Accordance With Local, State and Federal Guidance		✔	✔	✔
» Ensure Records Are Stored in a Secure and Encrypted Environment		✔	✔	✔
» Conduct Continuous Monitoring and Audits of Security Controls		✔	✔	✔
» Hire Security Auditors to Verify Security Controls		✔	✔	✔
» Change Control Board and Review Changes to Connections, Systems, Architecture and Settings		✔	✔	✔
» Ensure System and Security Logs are Audited for Malicious or Anomalous Behavior			✔	✔
» Hire Penetration Testers to Verify Environment Security			✔	✔
» Impact Analysis Performed for CBB			✔	✔
» Utilize Data Classification and Tracking Tools to Identify and Stop the Transmission of Sensitive Data			✔	✔
» Conduct Routine Risk Assessments			✔	✔
INCIDENT RESPONSE				
» Develop an Incident Response Plan	✔	✔	✔	✔
» Develop Incident Reporting Procedures and Plan	✔	✔	✔	✔
» Business Continuity Plan			✔	✔
» Disaster Recovery Plan			✔	✔

© 2025 Partner Alliance for Safer Schools

	TIER 1	TIER 2	TIER 3	TIER 4
DIGITAL INFRASTRUCTURE LAYER				
PEOPLE (ROLES AND TRAINING)				
» Maintain a List of Personnel With Access to the Facility	✔	✔	✔	✔
» Security Screenings for All Employees and Visitors	✔	✔	✔	✔
» Access Agreements for Visitors	✔	✔	✔	✔
» Ensure All Visitors Sign in on the Visitor Request Log	✔	✔	✔	✔
» Personnel Transfer Process	✔	✔	✔	✔
» Personnel Termination Process	✔	✔	✔	✔
» Have All Employees Wear Identification Badges		✔	✔	✔
» Set up a Visitor Management System		✔	✔	✔
» Escort Visitors as Required		✔	✔	✔
AWARENESS AND TRAINING				
» Conduct Annual Cybersecurity Training	✔	✔	✔	✔
» Maintain Records of Cybersecurity Training and Exercises	✔	✔	✔	✔
» Ensure That Privileged Users Receive Additional Cybersecurity Training	✔	✔	✔	✔
» Conduct Phishing Simulation Training	✔	✔	✔	✔
» Conduct Remedial Training After Security Incidents	✔	✔	✔	✔
» Conduct Annual Tabletop Exercises	✔	✔	✔	✔
» Conduct Business Continuity Plan (BCP) Training		✔	✔	✔
» Conduct Disaster Recovery Plan (DRP) Training		✔	✔	✔
PII PROCESSING AND TRANSPARENCY				
» User consent to PII Collection and Storage	✔	✔	✔	✔
INCIDENT RESPONSE				
» Ensure Staff Are Trained on Incident Response	✔	✔	✔	✔
» Conduct Incident Response Simulations	✔	✔	✔	✔
» Conduct BCP and DRP Testing and Exercises	✔	✔	✔	✔
SYSTEM AND SERVICES ACQUISITION				
» Developer Required and Optional Training	✔	✔	✔	✔
» Developer Support for Vulnerabilities	✔	✔	✔	✔
» Developer Security Design and Architecture Review	✔	✔	✔	✔
IDENTIFICATION AND SERVICES AUTHENTICATION				
» Identify and Authenticate All Users	✔	✔	✔	✔
» Require Multi-factor Authentication for Users	✔	✔	✔	✔
» Require Multi-factor Authentication for Single Sign-On (SSO)	✔	✔	✔	✔
» Use a Centralized Identification and Authentication Service	✔	✔	✔	✔
» Require Re-authentication After Periods of Inactivity	✔	✔	✔	✔
» Verify Geographic Location of Authentication Request			✔	✔
CONTINGENCY PLANNING AND MAINTENANCE				
» Ensure Maintenance Personnel Are Properly Screened and Vetted	✔	✔	✔	✔
» Ensure Maintenance Personnel Sign the Visitor Log and Are Escorted as Required	✔	✔	✔	✔

© 2025 Partner Alliance for Safer Schools

DIGITAL INFRASTRUCTURE LAYER

	TIER 1	TIER 2	TIER 3	TIER 4
ARCHITECTURAL				
CONFIGURATION MANAGEMENT				
» Maintain Current System Architecture Drawings and Diagrams	✔	✔	✔	✔
» Baseline Configuration for All Systems and Network Devices	✔	✔	✔	✔
» Secure Storage of All Baselines and Configurations	✔	✔	✔	✔
» Disable Any Ports, Services or Configurations Not Required for System Functionality	✔	✔	✔	✔
» Software Evaluation and Restriction	✔	✔	✔	✔
» Ensure Installed Software Is Signed and Verified.	✔	✔	✔	✔
» Supply Chain Management – Component Verification	✔	✔	✔	✔
» System, Software and Configuration Changes Require Privileged Access		✔	✔	✔
» Identify and Authenticate All Devices		✔	✔	✔
» Keep an Inventory of All Physical Assets			✔	✔
» Track and Inventory All Physical Assets			✔	✔
» Configuration Management Plan				✔
COMMUNICATIONS AND INFORMATION INTEGRITY PROTECTION				
» Denial of Service Protection	✔	✔	✔	✔
» Boundary Protection (DMZ	✔	✔	✔	✔
» Transmission Confidentiality and Protection	✔	✔	✔	✔
» Malicious Code Protection – Signature-Based Code Analysis	✔	✔	✔	✔
» System Monitoring – EDR	✔	✔	✔	✔
» Spam Protection	✔	✔	✔	✔
» Phishing Protection	✔	✔	✔	✔
» Issue Public Key Certificates From Approved Service Provider		✔	✔	✔
» Security Information and Event Management (SIEM) System		✔	✔	✔
» Secure Failover			✔	✔
» Living off the Land Attack Detection - User Behavior Detection			✔	✔
CONTINGENCY PLANNING AND MAINTENANCE				
» Schedule, Document and Maintain Equipment in Accordance With Manufacturer Recommendations	✔	✔	✔	✔
» Product Maintenance Through Entire Lifecycle	✔	✔	✔	✔
» Register All Risks in the Risk Register	✔	✔	✔	✔
» System Backups Conducted on a Routine Basis		✔	✔	✔
» Test Backups Regularly to Make Sure They Work		✔	✔	✔
» Develop a Risk Categorization Program		✔	✔	✔
» Vulnerability Monitoring and Scanning		✔	✔	✔
» Maintain an Inventory of All System Hardware Components			✔	✔
» Maintain an Inventory of All System Software Components			✔	✔
» Alternate Storage Site for Backups			✔	✔
» Alternate Processing Site (Cold, Warm, Hot)			✔	✔
» Conduct Threat Hunting				✔
COMMUNICATION				
» Communication Plan (Email, Phone, Contacts, etc.)	✔	✔	✔	✔
» Communicate With Key Stakeholders When Performing Maintenance on Network Systems	✔	✔	✔	✔
» Vulnerability Reporting Program			✔	✔

© 2025 Partner Alliance for Safer Schools

DIGITAL INFRASTRUCTURE LAYER	TIER 1	TIER 2	TIER 3	TIER 4
INCIDENT RESPONSE				
» Subscribe to Threat Warning Services	✔	✔	✔	✔
» Track and Monitor Incidents	✔	✔	✔	✔
» Conduct Post Incident Reviews and Update IRP as Needed	✔	✔	✔	✔
» Draft Media, Customer and Partner Incident Notification Templates	✔	✔	✔	✔
ACCESS CONTROL				
» Data Privacy Policy Login Banner	✔	✔	✔	✔
» Session Termination After a Period of Inactivity	✔	✔	✔	✔
» Locking a Device Upon 5 Unsuccessful Login Attempts	✔	✔	✔	✔
» Enforce Least Privilege	✔	✔	✔	✔
» Require Organization Approval for Privileged Accounts	✔	✔	✔	✔
» Remove and/or Deactivate Access Accounts When No Longer Required	✔	✔	✔	✔
» Audit Accounts for Anomalous Behavior	✔	✔	✔	✔
» Require Multi-Factor Authentication (MFA)	✔	✔	✔	✔
» Networking Equipment and Servers Are in Locked Cabinets or Rooms	✔	✔	✔	✔
» Monitor Remote Access Sessions	✔	✔	✔	✔
» Require Devices to Use a Cryptographic Module (TPM, Secure Element, etc.)	✔	✔	✔	✔
MEDIA PROTECTION				
» Restrict Access to Digital and Physical Media	✔	✔	✔	✔
» Encrypt All Sensitive Stored Digital Media	✔	✔	✔	✔
» Secure Physical and Digital Media in Transport	✔	✔	✔	✔
» Review All Media Prior to Release and Sanitize	✔	✔	✔	✔
» Appropriately Mark and Classify Media		✔	✔	✔
PII PROCESSNG AND TRANSPARENCY				
» Fixed Camera, Wide Area Coverage	✔	✔	✔	✔
» Infrared (IR) Cameras or Lighting		✔	✔	✔
» Wireless Video Data Transmission		✔	✔	✔
CONTINGENCY PLANNING AND MAINTENANCE				
» Ensure Old Media Is Properly Destroyed	✔	✔	✔	✔
» Keep a Record of All Media That Is Destroyed»	✔	✔	✔	✔
» Destruction of Old Equipment	✔	✔	✔	✔
» Enforce Separation of Duties		✔	✔	✔
» Protect Wireless Access Points With Strong Passwords and Encryption		✔	✔	✔
» Monitor Privileged Accounts		✔	✔	✔
» Limit the Number of Devices That a Person Is Logged Into (User Sessions)		✔	✔	✔
» Data Classification and Tagging		✔	✔	✔
» Limit the Use of Removable Media		✔	✔	✔
» Segmentation of VLANS		✔	✔	✔
» Password Manager With MFA		✔	✔	✔
» Automate the Removal and/or Deactivation of Accounts When Access Is No Longer Required			✔	✔
» Detect Rogue Hotspots			✔	✔
» Record Remote Access Sessions				✔

© 2025 Partner Alliance for Safer Schools

POLICIES AND PROCEDURES COMPONENT:

TIER 1

A. **Develop and Maintain a Data Privacy Plan:** Develop a data privacy plan that details how the school will protect sensitive information, such as student records, personal identification information (PII) and health data. This plan should outline how data is collected, stored, shared and protected. Regularly review the plan to ensure compliance with data privacy regulations such as Family Educational Rights and Privacy Act (FERPA). For example, if a new data-sharing agreement is established with a third-party vendor, update the plan to reflect how data will be securely handled.

   By maintaining a strong Data Privacy Plan, the school ensures that personal information is handled safely and legally.

B. **Vendor Assessment for All New Products:** Conduct a thorough vendor assessment to ensure that the product meets the school's security and privacy requirements before purchasing new software or hardware. This could include reviewing the vendor's security practices, data protection measures, and reputation in the industry. Ask the vendor for documentation about their data encryption practices, compliance with relevant laws (like FERPA), and recent third-party security audits.

   There are free resources available for vendor assessments such as the North Carolina Department of Public Instruction's Third Party Vendor Integration Checklist[1] and the department's guide to third party data integration[2]. Additionally, CISA has published its Secure By Demand Guide[3].

C. **Supply Chain Risk Management Plan:** Develop a supply chain risk management plan that outlines how the school will assess and mitigate risks associated with suppliers, vendors and third-party services. This plan helps protect against vulnerabilities that could be introduced through third-party vendors, such as compromised hardware or software. Include procedures for vetting new suppliers, regularly reviewing existing ones and identifying potential risks, such as reliance on single suppliers for critical systems or sourcing from regions prone to cyber threats. The plan should also include contingency measures, such as alternative suppliers, in case a vendor fails to meet security or performance requirements.

TIER 2

A. **Develop and Maintain a System Security Plan**: Create a system security plan (SSP) that outlines the security controls, policies, and procedures used to protect the school's IT systems. This plan should include details about access control, network security, data protection and incident response. Regularly review and update the plan to reflect changes in technology or security requirements. For example, if new software is introduced or the network architecture changes, update the plan to include how it will be secured.

1 https://www.dpi.nc.gov/third-party-vendor-integration-checklist/open
2 https://www.dpi.nc.gov/about-dpi/technology-services/third-party-data-integration
3 https://www.cisa.gov/resources-tools/resources/secure-demand-guide

© 2025 Partner Alliance for Safer Schools

B. **Hardware and Software Provenance:** Implement a process for documenting and verifying the provenance of all hardware and software used by the school, including creating a software bill of materials (SBOM) for any software purchased or developed in-house. Provenance refers to tracking the origin and history of hardware and software used by the school. This could include requiring vendors to provide an SBOM that lists all components, libraries, and dependencies included in the software. Track this information to ensure that every component is from a trusted source and has not been tampered with. Periodically audit both hardware and software to confirm that the products are consistent with their documented provenance.

C. **Supplier Assessments and Reviews:** Establish a formal process for evaluating suppliers before entering into agreements and conducting periodic reviews of existing suppliers. For new suppliers, assess their security practices, financial stability, and reputation by requesting information on their data protection protocols, compliance certifications, and customer references. For example, evaluate a potential cloud service provider by reviewing their encryption practices and uptime reliability. For ongoing relationships, conduct annual reviews to ensure they continue to meet the school's security, privacy, and performance standards.

PII PROCESSING AND TRANSPARENCY

TIER 1

A. **Develop a Personally Identifiable Information (PII) Plan:** Create a PII plan that outlines how the school collects, stores, uses, and protects personal information, such as student and staff records. This plan should detail the policies and procedures for handling sensitive information, including roles and responsibilities. For example, it may include policies for data retention, encryption, and access control. Review the plan regularly to ensure it aligns with legal requirements like FERPA.

B. **Identify All PII Stored on the Network:** Conduct an inventory of all PII stored on school systems, including student records, employee data and health records. Use data discovery tools to scan the network and identify where PII is stored, such as in databases, shared drives, or individual devices. Document this inventory and ensure that all PII locations are properly secured and monitored.

C. **Do Not Store PII That Is Not Absolutely Necessary:** Implement a policy that limits the collection and storage of PII to only what is necessary for school operations. For example, avoid collecting sensitive information like social security numbers unless absolutely required by law or policy. Regularly review the data stored and delete any unnecessary PII to reduce the risk of data breaches.

D. **Privacy Notice Should Be Available to All Personnel at the Time and Location of Collection:** Provide a clear privacy notice whenever PII is collected, explaining what data is being collected, why it's needed, how it will be used and how it will be protected. Include a privacy notice on digital enrollment forms or post it at the front office where paper forms are collected. Ensure that staff, students, and parents can easily access and understand the noticereplace by adding to previous sentence:, for example by adding it to teacher and student handbooks.

© 2025 Partner Alliance for Safer Schools

IDENTIFICATION AND AUTHENTICATION

TIER 1

A. **Access to Physical and Logical Systems:** A policy should be in place limiting access rights to the physical hardware of data infrastructure and access to software applications. Establishing user-based roles for software and physical hardware access is key to accomplishing this.

B. **Removal of Accounts Policy:** Create a formal policy for when and how user accounts should be removed. Roll out by documenting the policy and training staff to follow it. The policy should outline the timeframe for removing inactive accounts (e.g., accounts that haven't been used for 90 days). This policy ensures that old accounts are not left active and potentially misused.

C. **Review of Data Before Public Release:** Districts should have a policy requiring a data review process before any public sharing to ensure sensitive data is not mistakenly shared. Implement a process where data is reviewed by multiple staff members before it's made public.

D. **Have a Portable Media Policy:** Establish a policy on the use of portable media like USB drives to reduce the risk of malware or data loss. This policy should restrict the use of portable storage devices and require encryption for any data stored on them. This reduces the risk of data loss if devices are lost or stolen.

E. **Wi-Fi Hotspot Policy:** Regulate the use of personal or unsecured Wi-Fi hotspots to protect data from being intercepted. Implement a policy that restricts the use of personal mobile hotspots on school grounds to prevent students or staff from bypassing school network security. Allow only approved hotspot use for specific needs.

F. **Bring Your Own Device (BYOD) Policy:** Require personal devices used for schoolwork to meet specific security standards, such as having up-to-date antivirus software and using a secure password. Ensure students and staff are informed of these requirements before connecting to the school network.

G. **Password Requirements:** Set strong password rules, including length and complexity, to ensure users create secure passwords. Implement by enforcing these rules during password creation and change intervals. Passwords should include special characters and have a minimum length of 8 characters or should adopt passphrases.

H. **Ensure That System and Security Logs Are Enabled on All Devices:** Event logs should capture the (who, what, where, when, source, and identity) associated with an event. Configure all school devices (such as laptops, desktops and network equipment) to automatically generate system and security logs. This can be done by enabling logging features in the device's settings or through centralized logging tools. Logs should track key events like user logins, software installations and system errors.

I. **Maintain Plan of Actions and Milestones (POA&M) for All Security Controls That Cannot Be Met:** Create a document that lists any security controls the school cannot meet immediately. For each control, outline the action steps that will be taken to meet it in the future, assign responsible staff, and set deadlines (milestones). Review and update this document regularly to ensure progress is being made and involve school leadership in reviewing high-priority items.

© 2025 Partner Alliance for Safer Schools

J. **Vendor and Third-Party Services Policy:** Districts should establish policies for vendors and third-party service providers (e.g. cloud services) to ensure that the digital controls and policy of the district are applied to vendors and third-party services.

TIER 2

A. **Avoid Using Shared Accounts So All Activity Can Be Tied to a Specific User:** Eliminate shared accounts to ensure that every action on the system is tied to a specific individual, increasing accountability. Implement by enforcing unique user credentials for all staff. Assign individual user accounts for each staff member and student instead of using shared accounts. This ensures that all actions taken on school systems (such as accessing files or changing settings) can be traced back to a specific user, improving accountability and security.

B. **Ensure System and Security Logs Are Retained in Accordance With Local, State and Federal Guidance:** Set up a log retention policy that keeps all system and security logs for at least 180 days. Use a centralized logging system to store these logs in an organized manner, allowing IT staff to review historical data if needed for audits or investigations. Retaining system and security logs for at least 180 days to provide a sufficient window for investigation and auditing. Implement by setting retention policies within your logging systems.

C. **Ensure Records Are Stored in a Secure and Encrypted Environment:** Store logs and records in a secure location, such as an encrypted server or cloud storage solution. Encryption ensures that even if someone gains unauthorized access to the storage location, they cannot read or tamper with the logs. Ensure that only authorized personnel have access to this secure environment.

D. **Conduct Continuous Monitoring and Audits of Security Controls:** Use automated security tools that continuously monitor the school's systems for compliance with security controls, such as intrusion detection systems and vulnerability scanners. Set a regular audit schedule (e.g., quarterly) where IT staff manually review the effectiveness of these controls. Document any findings and make necessary adjustments to maintain security. Continuous monitoring helps you catch and fix issues before they turn into bigger problems.

E. **Hire Security Auditors to Verify Security Controls:** Bring in external security auditors to review the school's compliance with cybersecurity standards and best practices. These auditors will check that all security controls are correctly implemented and functioning as intended. The auditors' reports can help identify areas where the school's security policies may need improvement.

   Security auditors review your security policies and practices to make sure everything is being done correctly and securely. They check that all controls are in place and functioning as expected. This independent review helps ensure that your school is staying safe and compliant with regulations. Ideally this should be done annually.

F. **Change Control Board and Review Changes to Connections, Systems, Architecture and Settings:** Set up a change control board (CCB) consisting of key IT and administrative staff. Any proposed changes to the school's technology infrastructure (e.g., adding new systems or updating configurations) must go through the CCB for approval. This ensures that changes are well-planned and do not inadvertently introduce new security vulnerabilities.

© 2025 Partner Alliance for Safer Schools

TIER 3

A. **Ensure System and Security Logs Are Audited for Malicious or Anomalous Behavior:** Regularly audit system and security logs to detect malicious or unusual behavior, such as multiple failed login attempts or access from unexpected locations. Implement by using automated tools to flag anomalies and by scheduling regular reviews by IT staff. Investigate any anomalies to identify potential security incidents early. Typically, this is done by feeding logs into a SIEM system.

B. **Hire Penetration Testers to Verify Environment Security:** Contract with a third-party cybersecurity firm to perform penetration testing on the school's systems. Penetration testers simulate attacks on the network to identify vulnerabilities before malicious actors can exploit them. It's like having someone check the locks and windows of a house to make sure it's secure. Review the tester's findings and implement recommended security improvements to close any gaps. Ideally, this should be done annually. CISA has some valuable information on penetration testing.[4]

C. **Impact Analysis Performed for CCB:** As part of the change control board process, require an impact analysis for each proposed change. This analysis should assess the potential security risks of the change, such as how it may affect network security or data protection. The analysis helps the CCB decide whether the change is safe to implement or if additional security measures are needed.

D. **Utilize Data Classification and Tracking Tools to Identify and Stop the Transmission of Sensitive Data:** Implement data classification and tracking software that can automatically identify sensitive data, such as social security numbers or personal health information, and prevent it from being transmitted inappropriately. For instance, the software could block emails that attempt to send sensitive data to unauthorized recipients or alert IT staff when sensitive files are accessed or shared. This helps protect against accidental data leaks or breaches. These tools help ensure that sensitive data doesn't leave the school's network or fall into unauthorized hands.

E. **Conduct Routine Risk Assessments:** Schedule regular risk assessments, such as annually or quarterly, to identify new risks and evaluate the effectiveness of existing controls. During a risk assessment, the IT team might assess the school's network security, data protection measures, and compliance with regulations. Document the findings and determine if any new controls need to be implemented or existing ones adjusted to reduce vulnerabilities. This process should also be a part of the CCB. A monthly frequency is ideal, quarterly is acceptable, and less often puts the organization at risk.

4 https://www.cisa.gov/resources-tools/services/penetration-testing.

© 2025 Partner Alliance for Safer Schools

INCIDENT RESPONSE

TIER 1

A. **Develop an Incident Response Plan:** Develop an incident response plan (IRP) that outlines step-by-step procedures to follow in the event of a cybersecurity incident, such as a data breach, ransomware or malware attack. This plan should detail who is responsible for specific actions, how to contain and mitigate the incident, and how to recover systems. Store the plan in a secure, easily accessible location and review it annually to ensure it remains current. Having this plan ensures that the school can quickly and effectively address security issues, minimizing damage and disruption. CISA has examples of IRPs for Schools.[5]

B. **Develop Incident Reporting Procedures and Plans:** Create clear procedures for reporting cybersecurity incidents. This should include how staff should report suspicious activity or breaches, who to contact and what information to provide. Having a clear reporting plan ensures that incidents are detected and addressed quickly. For example, develop a reporting template that includes key details like the type of incident, the systems affected and any immediate actions taken. This ensures that incidents are reported promptly and handled effectively.

TIER 3

A. **Business Continuity Plan:** Develop a business continuity plan (BCP) that outlines how the school will continue operations during a disruption to technology systems, such as a natural disaster or cyberattack. This plan should include steps for keeping critical functions running, such as communication with staff and parents, remote learning, and maintaining access to student records. Store the plan in a central, easily accessible location, and review it annually to keep it up to date. Some districts include the operations for DRP (see below) as well.

B. **Disaster Recovery Plan:** Create a disaster recovery plan that details how the school will restore technology systems and data after a major incident, such as a data breach, server crash or flood. Include specific procedures for restoring data from backups, bringing systems back online, and communicating progress to stakeholders. Ensure IT staff and administrators are familiar with the DRP and that it's reviewed regularly. This plan helps the school quickly return to normal operations after an incident.

PEOPLE (ROLES AND TRAINING) COMPONENT:

TIER 1

A. **Maintain a List of Personnel With Access to the Facility:** Keep an up-to-date list of all staff members and contractors who have access to the school's facility, including keys or access cards. Use access control software to manage and regularly review the list, ensuring that only currently authorized individuals have access. Remove access for individuals who no longer need it, such as former employees or vendors.

5 https://www.cisa.gov/resources-tools/resources/federal-government-cybersecurity-incident-and-vulnerability-response-playbooks

© 2025 Partner Alliance for Safer Schools

B. Security Screenings for All Employees and Visitors: Conduct background checks and security screenings for all employees and visitors to ensure that only trustworthy individuals have access to the school's facilities and systems. These screenings help protect students, staff and sensitive information by verifying that everyone allowed into the school or onto the network is properly vetted.

Background checks should be implemented for all employees during the hiring process and for visitors who will have regular access to sensitive areas (e.g., contractors or long-term volunteers). For example, conduct criminal background checks, verify references, and check for any past security incidents. For visitors, require them to sign in, present identification, and undergo screening if they are accessing restricted areas, such as IT rooms or student records offices.

C. Access Agreements for Visitors: Require visitors to sign an access agreement before being granted entry to sensitive areas or systems areas (such as IT infrastructure, student records or secured facilities). This agreement outlines the rules for accessing the school's facilities and systems, ensuring that visitors understand their responsibilities and limitations while on-site. This helps protect the school from potential security breaches caused by unauthorized or careless behavior.

D. Ensure All Visitors Sign in on the Visitor Request Log: Require all visitors to sign in at a designated check-in point, such as the front office or security desk. The log should include their name, reason for the visit, time of arrival, and the staff member they are visiting. This practice ensures there is a record of who is on the premises at any given time and can be used for security audits or emergency evacuations.

E. Personnel Transfer Process: Establish a formal process for transferring employees between roles within the school. When an employee is transferred to a new role or department, update their access to match their new responsibilities. This ensures that they have the right level of access for their new position and prevents them from retaining access to areas or systems they no longer need. This reduces the risk of unauthorized access. Track and document these changes to ensure proper access control is maintained.

For example, when an employee moves from one department to another, update their access rights and permissions to reflect their new responsibilities. For instance, if a teacher transitions to an administrative role, remove their access to classroom management software and grant them access to administrative systems.

F. Personnel Termination Process: Establish a clear process for when employees leave the school, ensuring that their access to systems, facilities and sensitive information is promptly revoked. This process includes collecting badges, keys and equipment and removes their digital access to school systems. It helps prevent unauthorized access after someone leaves the school.

For example, on the employee's last day, collect their identification badge, keys and any school-issued devices. Immediately disable their access to digital systems (such as email and network accounts) through the IT department to prevent unauthorized access. Document the steps taken during the termination to ensure all security measures have been followed.

© 2025 Partner Alliance for Safer Schools

TIER 2

A. **Have All Employees Wear Identification Badges:** Issue identification badges to all staff members and require them to wear their badges while on school premises. Badges should display the employee's name and photo to make it easy to identify who belongs on campus. This helps ensure that only authorized personnel have access to sensitive areas like classrooms, IT rooms or administrative offices.

B. **Set up a Visitor Management System:** Implement a visitor management system (see also Electronic Visitor Management System under the District-Wide Layer) that tracks anyone who comes onto the school grounds who isn't a regular employee, such as parents, contractors or delivery personnel. For example, use visitor check-in software that records visitor details and prints temporary badges. The system can notify staff when visitors arrive, ensuring that they are appropriately monitored.

C. **Escort Visitors as Required:** For visitors who need access to sensitive areas or are unfamiliar with the building, assign an escort to accompany them. This ensures that visitors are monitored while on campus, reducing the risk of unauthorized access to restricted areas. Implement a policy where visitors to sensitive areas (such as server rooms or staff-only areas) must be escorted by a staff member at all times.

AWARENESS AND TRAINING

TIER 1

A. **Conduct Annual Cybersecurity Training:** This should be done yearly at a minimum, and preferably more if possible. All security controls and preventive measures are in vain if a staff member falls for a phishing attack and grants the attack full access to the systems. PASS recommends that all new hires and substitute staff are provided with cybersecurity training when onboarded.

B. **Maintain Records of Cybersecurity Training and Exercises:** Keep detailed records of all cybersecurity training and exercises to track participation and ensure compliance. Implement by using a learning management system or maintaining logs. Use a learning management system (LMS) or spreadsheet to track who has completed cybersecurity training and exercises. Maintain records that include the employee's name, date of training, and the type of training completed. This ensures you have a clear record for audits or compliance purposes.

C. **Ensure That Privileged Users Receive Additional Cybersecurity Training:** To help maintain the principle of least trust, ensure that privileged users only receive access to necessary rights and privileges and not beyond what they need for their job. Provide additional, specialized cybersecurity training for privileged users who have access to critical systems. This training should cover topics such as secure system configuration, recognizing advanced threats, and managing user permissions securely. Ensure this training is completed annually and logged.

D. **Conduct Phishing Simulation Training:** Quarterly testing is recommended to determine staff awareness of cyber threats and ability to recognize scams and phishing attempts. Run phishing simulation exercises to teach staff how to recognize and respond to phishing attempts. Implement by using phishing simulation tools and analyzing the results.

© 2025 Partner Alliance for Safer Schools

Example implementation: Implement phishing simulations that send fake phishing emails to staff as a test. Monitor how many staff members click on the links and use the results to offer targeted follow-up training for those who fall for the simulation. This helps staff recognize and avoid real phishing attacks in the future.

E. **Conduct Remedial Training After Security Incidents:** Offer remedial cybersecurity training to employees involved in security incidents to prevent future breaches. Implement by conducting a review after incidents and providing follow-up training. This remedial training ensures the employee understands what went wrong and how to avoid it in the future.

F. **Conduct Annual Tabletop Exercises:** Hold annual tabletop exercises to simulate cybersecurity incidents and test the effectiveness of policies and procedures. Implement by organizing drills with key staff and reviewing outcomes. Organize a tabletop exercise where key staff members discuss a simulated cybersecurity incident, such as a data breach or ransomware attack. The exercise walks through the school's response plan, testing policies and procedures, and identifying areas for improvement. Document lessons learned and update response plans accordingly. Resources for conducting and planning tabletop exercises are available from CISA.[6]

TIER 2

A. **Conduct Business Continuity Plan (BCP) Training:** Provide training to staff on the business continuity plan, explaining their roles during a disruption. Ensure that new employees are trained on these plans during onboarding and hold refresher sessions annually. This ensures that everyone knows their role and what to do if a disruption occurs. Training prepares staff to respond calmly and effectively, reducing confusion during a crisis.

B. **Conduct Disaster Recovery Plan (DRP) Training:** Provide training to staff on the disaster recovery plan, explaining their roles during a disruption. This can include training IT staff on how to restore data from backups, and train administrators on how to manage communication with parents and staff. Ensure that new employees are trained on these plans during onboarding and hold refresher sessions annually.

PII PROCESSING AND TRANSPARENCY

TIER 1

A. **User Consent to PII Collection and Storage:** Make sure students, parents, and staff provide their consent before the school collects and stores their PII. This includes informing them why the data is needed, how it will be used, and obtaining their permission. Consent ensures that data collection is transparent and in line with privacy requirements.

Districts should require students, parents, and staff to provide informed consent before collecting and storing their PII. This can be done through consent forms that explain what data is being collected, why it is needed, how it will be used and how it will be protected. For example, when parents enroll their children, have them sign a consent form that outlines the school's data collection practices.

6 https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

© 2025 Partner Alliance for Safer Schools

INCIDENT RESPONSE

TIER 1

A. **Ensure Staff Are Trained on Incident Response:** Provide training sessions for staff on the incident response plan, ensuring that everyone understands their role in case of an incident. This training helps them know exactly what to do in the event of a cybersecurity incident, ensuring that everyone responds quickly and effectively to contain and resolve the issue. Train IT staff on containing and mitigating threats, while training administrators on communication protocols. This training can be part of onboarding and refresher sessions can be held annually to keep everyone up to date.

TIER 2

A. **Conduct Incident Response Simulations:** Schedule regular incident response simulations, where staff practice responding to a simulated cybersecurity incident. These simulations should mimic real-world scenarios, such as a phishing attack or ransomware infection, and test the effectiveness of the incident response plan. After each simulation, gather feedback and identify areas for improvement.

TIER 3

A. **Conduct BCP and DRP Testing and Exercises:** Hold annual drills that simulate different disruption scenarios (e.g., power outage, cyber-attack, or building closure) to test the effectiveness of the business continuity plan and disaster recovery plan. These tests/drills/exercises help identify weaknesses in the plans and improve staff readiness. After each exercise, debrief with the participants and update and improve the plans as needed. Testing not only ensures that the plans will work when needed but also helps improve the plans and makes sure staff are ready to respond to actual incidents.

SYSTEM AND SERVICES ACQUISITION

TIER 1

A. **Developer Required and Optional Training:** Provide mandatory security training for developers who create or maintain the school's software and systems. Required training should cover secure coding practices, data protection, and identifying vulnerabilities. Optional training can also be offered to help developers stay up to date with the latest security best practices and technologies.

B. **Developer Support for Vulnerabilities:** Require developers to provide ongoing support for their products by identifying and fixing any security vulnerabilities that arise. This ensures that the software is kept up to date and secure, even after it's been deployed. This includes providing updates and patches to address newly discovered vulnerabilities. Developer support helps the school quickly address any security issues that could affect its systems.

C. **Developer Security Design and Architecture Review:** Implement a process where developers must conduct a security design and architecture review before any new system or feature is deployed. This review should assess the security implications

© 2025 Partner Alliance for Safer Schools

of the system's design, identify potential weaknesses, and ensure that security controls are built into the system from the start, rather than added later. By reviewing the design and architecture, developers can catch and fix potential security weaknesses early, reducing risks for the school.

IDENTIFICATION AND AUTHENTICATION

TIER I

A. **Identify and Authenticate All Users:** Ensure that every user who accesses school systems is identified by requiring a unique username and password for each individual. This ensures that only authorized staff, students, and administrators can access the school's technology resources, such as student records and online learning platforms. Implement user directories to manage and track identities.

B. **Require Multi-factor Authentication for Users:** Implement multi-factor authentication (MFA) for all users accessing critical systems, such as email, student records, or financial systems. MFA adds an extra layer of security by requiring users to provide not only a password but also a second factor, such as a code sent to their phone or an authentication app, to verify their identity. This helps protect against unauthorized access, even if a password is compromised. As part of defense in depth it's another way of verifying who is accessing the network/system. Keep in mind that not all MFA is created equal (phishing resistant) and that many of these systems natively support MFA.

C. **Require Multi-factor Authentication for Single Sign-On (SSO):** As SSO is an authentication process for users to access multiple applications with one sign on process, it is extremely important to enforce MFA for any SSO.

D. **Use a Centralized Identification and Authentication Service:** Implement a centralized authentication service, such as the lightweight directory access protocol (LDAP), to manage user identities and access across the entire school network. With LDAP, user accounts are managed centrally, ensuring consistent authentication policies across all systems and devices, and making it easier to add or remove users as needed. It simplifies user management and enhances security by centralizing control.

E. **Require Re-authentication After Periods of Inactivity:** Configure systems to require users to re-authenticate (enter their password or provide a second authentication factor) after periods of inactivity, such as 15 minutes. This helps ensure that if a device is left unattended, it cannot be accessed by unauthorized individuals without re-entering credentials.

TIER 3

A. **Verify Geographic Location of Authentication Request:** Implement geographic verification for authentication requests to prevent unauthorized access from unexpected locations. For example, if a staff member typically logs in from the school campus but a login attempt is detected from another country, the system can block the attempt or require additional verification. This helps prevent potential security breaches from remote attackers.

© 2025 Partner Alliance for Safer Schools

CONTINGENCY PLANNING AND MAINTENANCE

TIER 1

A. **Ensure Maintenance Personnel Are Properly Screened and Vetted:** Maintenance personnel that work on critical systems, should be properly screened and vetted, such as undergoing background checks before allowing personnel to work on sensitive equipment. Require maintenance contractors to provide references and undergo criminal background checks, especially if they will be working on sensitive systems like security cameras or servers. This ensures that only trustworthy individuals are given access to sensitive equipment, reducing the risk of security breaches or intentional damage.

B. **Ensure Maintenance Personnel Sign the Visitor Log and Are Escorted as Required:** Require all maintenance personnel to sign in at the front desk or a designated visitor check-in point before beginning their work. This includes logging their name, the company they represent, and the purpose of their visit. If they are working in secure areas (such as server rooms or access control areas), ensure they are accompanied by authorized staff at all times. This ensures that visitors are monitored and reduces the risk of unauthorized access to sensitive areas.

ARCHITECTURAL COMPONENT:

CONFIGURATION MANAGEMENT

TIER 1

A. **Maintain Current System Architecture Drawings and Diagrams:** The district should keep updated diagrams that map out the school's entire IT infrastructure, including networks, devices, servers, and security tools. Update these diagrams whenever new equipment is added, removed, or reconfigured. Store these documents in a secure, easily accessible location (e.g., a shared drive or documentation management system) so that IT staff can refer to them for troubleshooting and planning. Keeping these updated makes it easier to troubleshoot issues and ensures that everyone has a clear picture of the system for future improvements or security changes.

B. **Baseline Configuration for All Systems and Network Devices:** Establish standard, secure configurations for all school devices and network equipment (such as laptops, servers, and routers). These configurations should include settings like password policies, security features, and approved software. Once a baseline is set, ensure that all new devices are configured accordingly before being deployed, and regularly review these baselines to incorporate security updates.

C. **Secure Storage of All Baselines and Configurations:** Store baseline configurations and documentation in a secure location, such as encrypted cloud storage or a password-protected internal server. Limit access to these configurations to only authorized personnel, ensuring they are protected from unauthorized changes or tampering.

D. **Disable Any Ports, Services or Configurations Not Required for System Functionality:** Turn off or disable any unnecessary ports, services, or configurations on devices. This reduces the attack surface and limits potential entry points for hackers. For example, disable Bluetooth and USB ports if they are not needed for the system's operation.

© 2025 Partner Alliance for Safer Schools

E. **Software Evaluation and Restriction:** Review software for security vulnerabilities, data privacy, data residency, and conduct a full vender assessment. Also, review data privacy and residency policies to ensure student and staff data is safe, and conduct a full assessment of the vendor to ensure they meet security standards. This includes checking for known vulnerabilities, ensuring it complies with data privacy laws, verifying where data is stored, and assessing the vendor's reputation. Only approve software that passes these checks. Templates for assessing software risk are available from CISA.[7]

F. **Ensure Installed Software Is Signed and Verified**: When installing software, make sure it is "signed" (has a digital certificate) and verified to confirm it comes from a trusted source. This prevents the installation of fake or harmful software that could compromise your system.

G. **Supply Chain Management – Component Verification:** Verify the components of products and equipment in the supply chain to ensure they are secure and free from tampering. This process ensures that the parts and software coming into the school are trustworthy and haven't been compromised. Component verification helps protect against hidden vulnerabilities or malicious alterations in the products you rely on. This can be done by working with vendors who provide certifications for their products and conducting spot checks to ensure no unauthorized or counterfeit parts are introduced into the network infrastructure.

TIER 2

A. **System, Software and Configuration Changes Require Privileged Access:** Restrict the ability to make system, software, or configuration changes to IT staff with privileged accounts. This limits the potential for unauthorized or accidental changes that could compromise security. For example, only network administrators should have the ability to change firewall rules or install new software.

B. **Identify and Authenticate All Devices:** Set up device management tools that identify and authenticate all devices (such as laptops, tablets, and smartphones) before they are allowed to connect to the school network. Devices can be identified using unique identifiers, like MAC addresses or digital certificates, to ensure only trusted devices can access school resources. This helps prevent unauthorized or unknown devices from accessing the network, reducing the risk of security breaches from unapproved devices.

TIER 3

A. **Keep an Inventory of All Physical Assets:** Maintain an inventory of all physical assets, such as computers, projectors, and other valuable equipment. Use asset management software to track items by type, location and assigned user. Update the inventory regularly when new equipment is purchased or old equipment is retired. This helps prevent loss or theft and ensures accountability as well as keep track of what is owned, where it is located, and its condition. An inventory also helps with budgeting, repairs, and ensuring that nothing is lost or stolen.

7 https://www.cisa.gov/sites/default/files/publications/ICTSCRMTF_Vendor-SCRM-Template_508.pdf

© 2025 Partner Alliance for Safer Schools

B. **Track and Inventory All Physical Assets:** Conduct regular audits of physical assets to verify their location and condition. For example, once a semester, have IT staff or designated personnel check that all laptops, tablets, and other devices are accounted for and in working condition. Track changes, such as if a device is reassigned to a different staff member or if equipment is moved to a new classroom. This practice ensures that all assets are being properly managed and reduces the risk of missing or unaccounted-for equipment.

TIER 4

A. **Configuration Management Plan:** Develop a configuration management plan that outlines the procedures for managing and controlling system configurations. This plan should include how baselines are set, how changes are approved and documented, and how systems are maintained over time. The plan ensures consistency in configuration management and helps protect the school's systems from misconfigurations or vulnerabilities.

COMMUNICATIONS AND INFORMATION INTEGRITY PROTECTION

TIER 1

A. **Denial of Service Protection:** Denial of service (DoS) protection prevents attacks that try to overwhelm the school's network or systems with too much traffic, causing them to slow down or stop working. Use tools and services that detect and block these attacks before they disrupt normal operations. DoS protection helps keep the school's systems running smoothly even when under attack. For example, deploy a firewall with built-in DoS protection features that monitors traffic and blocks malicious requests targeting the school's web services. Regularly review network logs for signs of attempted DoS attacks and update protection settings as needed.

B. **Boundary Protection (DMZ):** Boundary protection refers to securing the "borders" of the school's network, such as the connection between the school's internal systems and the internet. This protection uses firewalls, filters and other tools to monitor and control what enters or leaves the network, keeping out unauthorized access and harmful traffic. It helps prevent attacks from reaching the school's systems.

   Set up boundary protection to monitor and control the flow of data between internal and external networks. Use firewalls, routers, and gateways to enforce security rules at the network's perimeter. This could include configuring the firewall to block unauthorized incoming traffic while allowing legitimate communication, such as remote access for teachers using the school's VPN. Segment internal networks using VLANs to limit the movement of threats across different areas of the school's network.

   A demilitarized zone (DMZ) is a separate network segment acting as a buffer between an organization's internal network and the external, untrusted network (like the internet). It's like a semi-secure area where public-facing services, such as web servers, email servers and DNS servers, are hosted, isolating them from the organization's sensitive internal systems

C. **Transmission Confidentiality and Protection:** Ensure that data sent across the network, like emails or files, is protected and kept private. Use encryption to secure data during transmission so that even if someone intercepts it, they can't read or use it. This helps protect sensitive information as it moves between systems, both inside and outside the school. Implement VPNs

© 2025 Partner Alliance for Safer Schools

for remote access to guarantee that data transmitted over external networks remains secure. For example, use protocols like SSL/TLS to secure web traffic, ensuring that any communication between the school's servers and external websites (such as cloud services) is encrypted.

D. **Malicious Code Protection – Signature-Based Code Analysis:** Deploy antivirus and anti-malware software that uses signature-based detection (looking for known malware patterns) to protect the school's systems. For example, install antivirus software on all school computers that checks for known threats using signature updates and also watches for abnormal behavior, such as unauthorized software installations or unusual network activity. Regularly update the software to include the latest signatures and algorithms for behavior analysis.

E. **System Monitoring – EDR:** Deploy an endpoint detection and response (EDR) solution to continuously monitor endpoints, such as laptops, desktops and mobile devices, for malicious activity. For example, if an attacker tries to execute a malicious script on a teacher's laptop, the EDR system will detect the behavior, quarantine the file, and alert the IT team. Regularly review the EDR logs and reports to stay ahead of emerging threats and adjust security configurations as needed.

F. **Spam Protection:** Use email filtering solutions to block spam and potentially harmful emails from reaching staff and students. This could include configuring email filters to detect and block emails containing suspicious attachments, phishing links, or language commonly used in scams. This reduces the risk of staff and students falling victim to email-based threats such as malware or phishing attempts.

G. **Phishing Protection:** Implement an email protection system that specifically targets phishing threats. Phishing protection tools detect and block emails or websites that attempt to trick users into revealing personal information, such as passwords or financial details. This includes the use of an advanced email security solution that detects phishing emails by scanning for red flags such as fake domain names, malicious links, or social engineering tactics. Provide users with a reporting tool to flag suspected phishing attempts and implement automated responses that block or quarantine phishing emails before they reach inboxes.

TIER 2

A. **Issue Public Key Certificates From Approved Service Provider:** Obtain and issue public key certificates from a trusted, approved certificate authority (CA) to secure web services, email servers, and other network resources. For example, the school's website can use an SSL certificate from an approved CA to enable HTTPS, ensuring that visitors' data is encrypted and their connection is secure.

It is necessary to verify the authenticity of email and other communications and to digitally verify who sent information between two parties while encrypting information to protect unauthorized interception of data. Public key certificates are digital certificates that verify the identity of users or devices. Make sure these certificates are issued by a trusted and approved service provider. This helps ensure that secure connections, like those used for websites or email, are properly authenticated and protected from impersonation or fraud.

8 https://www.cisa.gov/cyber-hygiene-services

© 2025 Partner Alliance for Safer Schools

B. **Security Information and Event Management (SIEM) System:** Implement a SIEM system to collect and analyze security data from across the school's network in real time. The SIEM tool can gather logs from firewalls, servers, and endpoints, correlating this data to detect patterns of suspicious activity, such as multiple failed login attempts or data exfiltration. Configure the SIEM to send alerts to IT staff when potential threats are detected, allowing for timely investigation and response. These services can be hosted internally, or by hiring a Security Operations Center as a Service (SOCaaS) depending on budget.

TIER 3

A. **Secure Failover:** Establish a secure failover process that ensures continuity of critical systems in case of failure. Set up a backup server that automatically takes over if the main server goes down, ensuring that important services, such as email and online learning platforms, remain available. Implement failover mechanisms with strong security controls, such as encrypted connections and regular security audits, to prevent unauthorized access during a failover event. This keeps critical services running securely while the primary system is restored.

B. **Living off the Land Attack Detection - User Behavior Detection:** Use user behavior analytics (UBA) tools to detect living off the land (LotL) attacks, where attackers use legitimate tools and processes already present on the system to carry out their activities. Configure UBA to monitor for unusual user behavior, such as accessing files they normally don't or running system commands outside their role. If an anomaly is detected, such as a non-IT staff member executing PowerShell scripts, the system can alert IT staff to investigate the potential attack.

CONTINGENCY PLANNING AND MAINTENANCE

TIER 1

A. **Schedule, Document and Maintain Equipment in Accordance With Manufacturer Recommendations:** Develop a maintenance schedule based on the manufacturer's guidelines for all critical equipment, such as computers, network devices, and security systems. Regularly perform maintenance on school equipment (such as computers, servers, and security systems) following the manufacturer's instructions. Documenting the maintenance ensures that there is a record of when work was done, which helps track the equipment's condition and compliance with recommendations. This ensures that all equipment remains in good working order and reduces the risk of unexpected failures.

B. **Product Maintenance Through Entire Lifecycle:** Implement a policy for maintaining all products, such as software, hardware, and systems, throughout their entire lifecycle. This includes regularly applying security patches, updating software, and conducting routine maintenance to ensure continued functionality and security.

C. **Register All Risks in the Risk Register:** Keep a risk register, which is a list of all identified risks that could affect the school's cybersecurity or operations. For each risk, include details like how likely it is to happen and what the potential impact would be. This register helps track and monitor risks, making it easier to manage and reduce them over time. The register helps track progress in addressing risks and provides a central record for audit purposes.

© 2025 Partner Alliance for Safer Schools

TIER 2

A. **System Backups Conducted on a Routine Basis:** Schedule regular backups of critical systems and data, such as student records, financial information, and lesson plans to prevent data loss in case of a problem, like a system crash or cyberattack. This could include configuring automated daily backups to a secure cloud storage solution and store copies locally as well. Ensure that backups are set to occur outside of regular school hours to avoid disruption.

B. **Test Backups Regularly to Make Sure They Work:** Regularly test the backups by restoring data from them to ensure that they work as expected. Schedule quarterly tests where IT staff restore specific files or systems to verify the integrity of the backup process. Document the results of these tests and address any issues immediately. Testing ensures that backups are reliable, so they'll be effective in a real emergency when you need to recover lost or damaged data.

C. **Develop a Risk Categorization Program:** Create a risk categorization program that assigns each identified risk a category based on its impact and likelihood. For example, categorize risks as "High," "Medium," or "Low" depending on how critical the risk is to the school's operations and security. Risks could include things like unauthorized access to student data, network failures, or malware infections. This helps prioritize which risks need the most attention and resources to mitigate.

D. **Vulnerability Monitoring and Scanning:** Use automated vulnerability scanning tools to regularly scan the school's network and systems for potential vulnerabilities, such as unpatched software or misconfigured settings. For example, schedule weekly scans that identify weaknesses in firewalls, servers, or devices. Ensure that any vulnerabilities found are promptly addressed through patching or reconfiguration to prevent exploitation. Regular scanning helps find and fix security gaps before they can be taken advantage of. This proactive approach reduces the likelihood of cyber incidents by addressing issues as soon as they are discovered.

   There are many open-source tools such as CISA's Cyber Hygiene Services, which offers free, vulnerability and web app scanning[8]. In addition to CISA's resources, there are many third-party services that can conduct vulnerability scanning as well.

TIER 3

A. **Maintain an Inventory of All System Hardware Components:** Use inventory management software to track all hardware (like computers, routers, and printers) in use at the school. Regularly update this inventory whenever new items are added or removed. This ensures that the school knows exactly what assets it has, making it easier to manage maintenance, updates, and security.

B. **Maintain an Inventory of All System Software Components:** Use inventory management software to track all software in use at the school. Regularly update this inventory whenever new items are added or removed. This ensures that the school knows exactly what assets it has, making it easier to manage maintenance, updates, and security. This inventory also helps the district track what needs to be protected, updated, or replaced, and ensures that everything is accounted for in the district cybersecurity plans.

© 2025 Partner Alliance for Safer Schools

C. **Alternate Storage Site for Backups:** Store backup copies of critical data at an alternate site, away from the main location. This protects your data in case something happens to the main site, like a fire or flood. The alternate storage site ensures you still have access to backups even if the primary location is compromised. Consider the location of the alternate site. The alternate site should be outside a 100-mile range. States and counties may have residency requirements, so check with local authorities before setting up an alternate location.

D. **Alternate Processing Site (Cold, Warm, Hot):** Identify an alternate location where critical systems can be operated in case the primary site becomes unavailable. Depending on the level of preparedness, this could be a cold site (an empty facility where equipment could be moved), a warm site (a location with some equipment that requires setup), or a hot site (fully operational and ready to take over immediately). For example, a hot site could be a cloud-based platform that mirrors critical systems and can be activated instantly if the school's network fails.

   This approach ensures that even if the main site goes down, the school can keep critical systems running. For cloud-hosted schools, this will be easy to implement. For on-prem hosted schools (schools where systems are hosted on the school's premises), this will be much more difficult and require a more significant investment.

TIER 4

A. **Conduct Threat Hunting:** Implement a proactive threat-hunting program where IT staff actively search for signs of potential threats or malicious activity within the school's systems. Conduct regular reviews of system logs to identify unusual behavior, such as repeated failed login attempts or unexpected network traffic patterns. Use specialized tools to investigate and address any threats before they result in a security incident.

   Threat hunting involves actively searching through systems and networks for signs of cyber threats or suspicious activity, even before an attack has been detected. This is a more proactive approach than simply waiting for alerts from security tools. By hunting for threats, the school can identify potential dangers early and take action to prevent them from causing harm.

COMMUNICATION COMPONENT:

TIER 1

A. **Communication Plan (Email, Phone, Contacts, etc.):** Develop a communication plan that includes up-to-date contact lists for staff, students, parents and emergency services. Identify multiple communication methods, such as email, phone trees or messaging apps, which can be used to notify people of an incident and provide updates. This plan ensures that everyone stays informed during a crisis, even if one communication method fails.

B. **Communicate With Key Stakeholders When Performing Maintenance on Network Systems:** Before performing maintenance on critical systems like power sources, access control, security systems, servers, or networks, coordinate with key stakeholders (such as IT staff, school administration, or security personnel). This helps ensure that everyone is aware of the work being done, minimizing disruption to school operations and ensuring that any potential risks are managed. For instance,

© 2025 Partner Alliance for Safer Schools

schedule the work during non-school hours to minimize disruption. Ensure that stakeholders are informed of the progress and any potential impacts on school operations.

TIER 3

A. **Vulnerability Reporting Program:** Establish a vulnerability reporting program that allows staff, students, or external parties to report potential security vulnerabilities or weaknesses in the school's systems. For example, provide an email address or an online form for reporting issues, such as suspicious emails, outdated software, or unsecured devices. Ensure that reports are reviewed by the IT team, who will assess and prioritize the vulnerabilities for remediation. Publicize the program so everyone knows how to report concerns and establish a process for acknowledging and responding to reported issues before they can be exploited by cybercriminals, helping the school fix problems quickly and stay secure.

INCIDENT RESPONSE

TIER 1

A. **Subscribe to Threat Warning Services:** Subscribe to threat warning services, such as those offered by CISA (Cybersecurity and Infrastructure Security Agency), to receive alerts about new or emerging cyber threats. These updates help the school stay informed about potential risks and take action to protect against them. CISA has a free threat warning service[9].

B. **Track and Monitor Incidents:** Keep a record of all cybersecurity incidents, including what happened, how it was handled, and the outcome. This helps the school identify patterns, track the effectiveness of response efforts, and ensure that all incidents are properly documented for future reference.

C. **Conduct Post Incident Reviews and Update IRP as Needed:** After a cybersecurity incident is resolved, conduct a review to understand what happened, what worked well, and what could be improved. Use these insights to update the Incident Response Plan so that the school is better prepared for future incidents.

D. **Draft Media, Customer and Partner Incident Notification Templates:** Prepare pre-written templates for communicating with the media, customers (e.g., parents), and partners (e.g., vendors) in case of a cybersecurity incident. These templates should include clear messaging about what happened, what steps are being taken to address the incident, and how it may affect stakeholders. Having these templates ready allows the school to respond quickly and consistently when communicating during a crisis.

9 https://public.govdelivery.com/accounts/USDHSCISA/subscriber/new?qsp=CODE_RED

© 2025 Partner Alliance for Safer Schools

ACCESS CONTROL COMPONENT:

TIER 1

A. **Data Privacy Policy Login Banner:** Display a message when users log into the system, informing them that their actions may be monitored. Implement by setting up a notification that appears during logon across all systems. Schools can configure a message that appears when someone logs into school systems, reminding users of school policies (e.g., "Unauthorized use of this system is prohibited").

B. **Session Termination After a Period of Inactivity:** Automatically log out users after a set period of inactivity to reduce unauthorized access risks. Implement by adjusting system settings for time-based session termination. NIST recommends that session termination for inactivity be 20 minutes and 15 minutes for moderate risk environments.

C. **Locking a Device Upon 5 Unsuccessful Login Attempts:** District issued device should be locked after 5 failed attempts. It is recommended that the devices be capable of remotely wiping the device. Automatically lock devices after multiple failed login attempts to prevent unauthorized access. IT staff can configure this in the system settings, ensuring devices are secure from unauthorized users trying to guess passwords.

D. **Enforce Least Privilege:** Assign system access based on roles, tasks, and needs to ensure users only have the minimum access required to do their jobs. Implement by setting up role-based access control (RBAC) and regularly reviewing user permissions. For example, teachers only access student management systems, while IT staff access network configurations. Limit each group's access to only what is necessary for their role.

E. **Require Organization Approval for Privileged Accounts:** Any access to critical systems or data should have an approval process. At minimum, there should be a role-based approval process by a governance team. The district should require management approval before creating or assigning privileged accounts.

F. **Remove and/or Deactivate Access Accounts When No Longer Required:** Districts should manually deactivate accounts for users who leave, transfer, or no longer need access. In establishing this process, it is important for HR and IT to collaborate on deactivation. Also, have a checklist for IT staff to follow when an employee leaves or changes roles. This includes manually deactivating their user accounts across systems like email, student information systems, and network access.

G. **Audit Accounts for Anomalous Behavior:** Regularly review user account activities to detect suspicious behavior. Set up monitoring tools that look for unusual activity, such as logins from unexpected locations or times. IT staff should review these logs regularly to detect any potential security threats.

H. **Require Multi-Factor Authentication (MFA):** Require multi-factor authentication (MFA) for all accounts to add an extra layer of security. MFA verifies something you are, something you know and/or something you own. Biometrics, such as a fingerprint, is something you are; something you know is commonly a password; and something you own would be a cell phone or email account. MFA should be integrated with your login systems and requiring users to enroll. Implement MFA for all staff when logging into critical systems, such as email or student management platforms. This can be done by requiring a secondary code sent via text or email in addition to their password.

© 2025 Partner Alliance for Safer Schools

I. **Networking Equipment and Servers Are in Locked Cabinets or Rooms:** Physically secure networking equipment and servers by storing them in locked areas. Implement by using secure rooms or cabinets and limiting access to authorized personnel**.** PASS recommends network routers, switches, and servers in secure rooms or locked cabinets that only IT staff can access. This physical protection prevents unauthorized personnel from tampering with equipment.

J. **Monitor Remote Access Sessions:** Track remote access sessions to detect unauthorized activity. Implement by enabling logging and recording tools in your remote access systems. These logs should record when users connect, what they do, and when they disconnect, providing a record for auditing.

K. **Require Devices to Use a Cryptographic Module (TPM, Secure Element, etc.):** Ensure that devices used by staff and students have a trusted platform module (TPM) or other cryptographic module installed. These modules securely store encryption keys and ensure that sensitive data (such as login credentials) is protected on the device itself. For example, require devices to have TPM chips activated to enhance data security on school-owned computers.

MEDIA PROTECTION

TIER 1

A. **Restrict Access to Digital and Physical Media:** Limit who can access digital and physical media (such as hard drives, USB drives or paper records) to only authorized staff. This reduces the risk of sensitive information falling into the wrong hands, whether it's stored digitally or physically. Store physical media in locked cabinets and restrict access to digital files by setting permissions that only allow approved staff to access them. Implement role-based access control to ensure that only staff members with the appropriate clearance can access confidential information.

B. **Encrypt All Sensitive Stored Digital Media:** Encrypt all sensitive digital media when it is stored on devices or servers. Configure computers and network storage systems to automatically encrypt files containing personal or confidential information. This ensures that even if the media is stolen or accessed without authorization, the data remains protected and unreadable. Use industry-standard encryption algorithms

C. **Secure Physical and Digital Media in Transport:** Secure physical and digital media when it is being transported between locations. For physical media, use locked containers or courier services that specialize in secure transport. For digital media, use encrypted channels, such as VPNs or encrypted email, to send files securely over the internet. This helps prevent unauthorized access or interception during transport.

D. **Review All Media Prior to Release and Sanitize**: Before releasing media, review it to ensure it doesn't contain sensitive or unnecessary information as required based on District or other applicable policies. If possible, sanitize the media by removing or redacting sensitive data. This reduces the risk of accidentally sharing confidential information.

© 2025 Partner Alliance for Safer Schools

TIER 2

A. **Appropriately Mark and Classify Media:** Label physical and digital media according to its level of sensitivity, using terms like "confidential," "internal use only," or "public." For instance, student records could be marked as "confidential," while general newsletters may be labeled "public." Clearly marking media ensures that staff handle it appropriately and follow proper security protocols based on the classification. This helps staff understand how to handle each type of information properly, ensuring that sensitive data is treated with extra care.

PII PROCESSING AND TRANSPARENCY

TIER 1

A. **PII Should Be Encrypted in Storage:** Districts should configure databases and file storage systems to automatically encrypt records containing PII, such as student names, addresses and grades. Encryption converts the information into a secure code, so even if someone gains unauthorized access to the data, they won't be able to read or use it.

B. **PII Is Only Accessible by Personnel Who Require Access:** Restrict access to PII based on job roles and responsibilities. Limit access to PII to only those employees who need it to perform their job duties, such as administrators or school nurses. Restricting access minimizes the risk of unauthorized use or exposure of sensitive personal information. Use role-based access control (RBAC) to ensure that only personnel with a legitimate need to access PII are granted permission.

C. **Ensure PII Is Encrypted When Transmitted:** Encrypt all PII when it is being transmitted over the network, such as when sending student records between schools or to external service providers. Use secure protocols like HTTPS, SSL/TLS, or VPNs to ensure data is protected during transmission and cannot be intercepted by unauthorized parties.

CONTINGENCY PLANNING AND MAINTENANCE

TIER 1

A. **Ensure Old Media Is Properly Destroyed:** Establish a policy and process for securely destroying old media that is no longer needed. For digital media, use data-wiping software to permanently erase files from hard drives and storage devices. For physical media, use shredders or secure disposal services to destroy paper records and old disks. This prevents sensitive information from being recovered after disposal.

B. **Keep a Record of All Media That Is Destroyed:** Maintain a log of all media that has been destroyed, including what was destroyed and when. This record provides a clear audit trail to ensure that sensitive data has been properly disposed of and can be tracked if needed.

C. **Destruction of Old Equipment:** Establish a secure process for disposing of old equipment, such as computers, hard drives, and other digital storage devices. This process should include securely wiping or physically destroying any storage media to prevent data recovery. Proper destruction ensures that sensitive data doesn't fall into the wrong hands.

© 2025 Partner Alliance for Safer Schools

For instance, before decommissioning old laptops, use specialized data-wiping software to ensure that all sensitive information is irretrievable, or physically shred the hard drives to destroy the data.

TIER 2

A. **Enforce Separation of Duties:** By reviewing the people who have multiple roles and access to multiple systems, ensure there is a process to prevent or reduce privilege creep. Critical tasks should be divided among multiple people to reduce the risk of fraud or error. Assign different staff members to different critical tasks so that no single person has full control over a process. For example, one person approves financial transactions, and another executes them, preventing abuse of power or mistakes.

B. **Protect Wireless Access Points With Strong Passwords and Encryption:** Set a complex password for Wi-Fi routers and access points. Ensure passwords contain a mix of letters, numbers, and symbols, and avoid using default or easily guessed passwords like "admin123." Use encryption protocols like WPA3 to protect data transmitted over the network. Implement by configuring all access points to use the most secure encryption methods. Disable outdated Wi-Fi protocols (e.g., WEP) that are vulnerable to attacks. Implement by auditing access points and ensuring only modern, secure protocols are enabled. As information data security is in constant flux, use the latest security controls released by NIST and CISA. For recommendations on specific security products and protection mechanisms, PASS recommends working with a security consultant.

C. **Monitor Privileged Accounts:** PASS recommends, at minimum, a quarterly monitoring of privileged accounts. This includes ensuring that the privilege is being used appropriately. In addition to manual review of all privileged accounts, there are some software-based automated tools for the purpose of monitoring privileged accounts. Use monitoring tools to track privileged accounts' activity, such as logins and changes to systems. Generate regular reports for review by IT staff or administrators to detect unusual behavior.

D. **Limit the Number of Devices That a Person Is Logged Into (User Sessions):** Restrict users to logging into a limited number of devices simultaneously to reduce the risk of account sharing. Roll out by configuring session limits in your system settings. Use network management tools to limit the number of devices a user can log into simultaneously. For example, limit each teacher to one active login session on school systems at a time to reduce security risks.

E. **Data Classification and Tagging:** Categorize and label data based on sensitivity to ensure it is protected according to its risk level. Label the data according to its sensitivity (e.g., confidential, internal, public) and use this classification to guide who has access to it. For example, student records might be labeled "confidential" and only accessible to authorized staff.

F. **Limit the Use of Removable Media:** Restrict the use of external storage devices to prevent unauthorized data transfers. Implement by using system policies to block or control access to removable media. Districts can use software to block unauthorized USB devices from connecting to school computers. This helps prevent malware from being introduced via unknown devices and reduces data loss risks.

G. **Segmentation of VLANS:** Use virtual local area networks (VLANs) to separate different types of network traffic into distinct segments, limiting exposure in case of a breach. For example, keep student traffic, staff traffic, and security system traffic on separate VLANs to limit the spread of attacks across the network.

© 2025 Partner Alliance for Safer Schools

H. **Password Manager With MFA:** Use a password manager that supports MFA to store and protect passwords. Provide staff with access to a password manager that securely stores passwords. Ensure the password manager is protected by MFA, requiring an additional code besides a password to access stored credentials.

TIER 3

A. **Automate the Removal and/or Deactivation of Accounts When Access Is No Longer Required:** Automatically deactivate accounts when no longer needed to reduce human error. Implement by configuring automated workflows tied to HR systems. Use identity management software that automatically deactivated accounts when HR systems mark an employee as terminated or transferred. This automates the process of removing access based on status changes in the system.

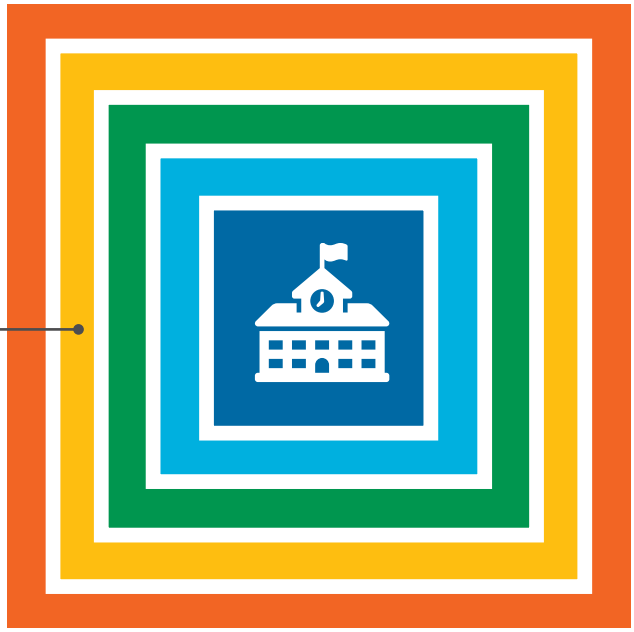
B. **Detect Rogue Hotspots:** Utilize a wireless scanning tool to detect rogue hotspots within the organization.

TIER 4

A. **Record Remote Access Sessions:** Record remote access sessions to detect unauthorized activity. Use remote access tools that allow IT staff to record remote session connections.

© 2025 Partner Alliance for Safer Schools

CAMPUS EXTERIOR PERIMETER LAYER



» QUICKFIND

Campus Exterior Perimeter Layer Checklist 79
Policies And Procedures Component..... 80
Architectural Component 81
Communication Component 83
Video Surveillance Component 85
Detection And Alarms Component 89

© 2025 Partner Alliance for Safer Schools

CAMPUS EXTERIOR PERIMETER LAYER	TIER 1	TIER 2	TIER 3	TIER 4
POLICIES AND PROCEDURES				
» Implement NCS4 Best Practices for Outdoor Activities and Events	✔	✔	✔	✔
» Annual Assessment of Safety of Ground (including Lighting)	✔	✔	✔	✔
» Create Grounds and Facility Use Policies for Outside and Public Groups	✔	✔	✔	✔
» Parking Tags	✔	✔	✔	✔
» Security Patrols		✔	✔	✔
» Assign Staff to Periodically Check Parking Lot		✔	✔	✔
» Persistent Staff Patrol			✔	✔
» RFID Parking Tags			✔	✔
» Annual Assessment for Lighting				✔
» Staff Capability to Initiate Emergency Protocols from Exterior				✔
ARCHITECTURAL				
» Signage Directing Visitors to the Appropriate Areas	✔	✔	✔	✔
» Signage Directing to Emergency Communication Device	✔	✔	✔	✔
» Apply CPTED Principles for Territorial Reinforcement. Access Control and Natural Surveillance	✔	✔	✔	✔
» Trespassing, Video Surveillance and Access Notification Signage	✔	✔	✔	✔
» Properly Positioned Exterior Lights	✔	✔	✔	✔
» Debris Clearance	✔	✔	✔	✔
» Gates at Entrances		✔	✔	✔
» Landscaping to Control Vehicle Access		✔	✔	✔
» Lighting to Enhance Video Surveillance				✔
COMMUNICATION				
» Public Address Systems	✔	✔	✔	✔
» Local Area Two-Way Radio System Between Office and Staff		✔	✔	✔
» Visual Indicators Specific to Hazard			✔	✔
» Digital Low-Band Radio System Connected to District-Wide System			✔	✔
» Two-Way Emergency Phones in Parking Areas			✔	✔
» Install Audio/Video Call Boxes at Key Locations				✔
» Audible and Visual Mass Notification Tied to District-Wide System				✔
VIDEO SURVEILLANCE				
» Fixed Camera, Wide Area Coverage	✔	✔	✔	✔
» Infrared (IR) Cameras or Lighting		✔	✔	✔
» People Identification Field of View at Pickup/Drop-Off Area		✔	✔	✔
» Perimeter Video Analytics		✔	✔	✔
» Wireless Video Data Transmission		✔	✔	✔
» Fixed Camera, Wide Area-Coverage Campus Wide				✔
» PTZ Camera Coverage				✔
DETECTION AND ALARMS				
» Panic Alarm System Within Greenspace Areas		✔	✔	✔

© 2025 Partner Alliance for Safer Schools

POLICIES AND PROCEDURES COMPONENT:

TIER 1

A. **Implement National Center for Spectator Sports Safety and Security (NCS4) Best Practices Guide for Outdoor Activities and Events.** PASS recommends that school districts use the best practices guide[1] developed by the NCS4 when developing policies and procedures for outdoor activities and events.

B. **Annual Assessment of Safety of Ground (Including Lighting)**. An ongoing process should be established for identifying, evaluating and prioritizing vulnerabilities and areas of weakness within the campus perimeter that could have adverse consequences for individual schools and school districts. This can be done by conducting a walk-through of school grounds and facilities and looking at existing crime and school incidence data. The goal should be to design a system of accountability with measurable activities and timelines to address risks that were found. Self-assessments are appropriate and should be done by various district stakeholders that oversee the exterior areas of the facility.

C. **Create Grounds and Facility Use Policies for Outside and Public Groups.** Such policies not only protect schools but also promote the facilities as assets to the community in many ways. While buildings and grounds are maintained primarily for the purpose of educating students, most school boards recognize that district facilities are a valuable community resource and believe they should be made available to the community for beneficial uses that will not interfere with educational activities or disrupt district operations such as renovation, maintenance and/or sanctioned after school activities.

D. **Parking Tags.** Parking decals, stickers or numbered hang tags should be provided to staff members and regular volunteers and prominently displayed on their vehicles; however, these items should not display any information that would identify the employee or their position for their protection. A numbering or lettering system would be the best deployment.

TIER 2

A. **Security Patrols.** School districts can assign security patrols and/or encourage law enforcement to have patrolling officers to discourage trespassing and other unwanted activities.

B. **Assign Staff to Periodically Check Parking Lot.** Staff such as administrators, teachers and custodians assigned to check the parking lot should be equipped with radio communications back to the office. They should also be empowered to initiate an emergency protocol for the school if they detect a threat outside of the building and should be equipped with crisis de-escalation training for dealing with the public.

1 https://ncs4.usm.edu/resources/best-practices/

© 2025 Partner Alliance for Safer Schools

TIER 3

A. **Persistent Staff Patrol.** A trained staff member should be on duty to patrol the exterior of a school, including the parking lot perimeter, at all times during normal operating hours to ensure that safety rules and other practices are being followed and check for unauthorized vehicles in the lot. The greatest benefit to having a person dedicated to this task is that they can focus solely on possible exterior threats of the facility. An assigned staff member should be equipped with radio communications and fully trained as a security officer. They should also be provided with a tablet or other portable device that provides access to data such as parking pass registrations and student information as needed. The device should also provide access to camera feeds and security system information. The assigned staff member can also be provided with a communications device that allows them to initiate a school in lockdown from the outside if a threat is detected approaching the building.

B. **RFID Parking Tags.** Employees use RFID stickers on vehicles for parking lot entry and exit (applicable as part of an access control system).

TIER 4

A. **Annual Assessment for Lighting.** A safety and security assessment of lighting based upon industry and local standards should be performed annually.

B. **Staff Capability to Initiate Emergency Protocols from Exterior.** All employees are provided with the technology and related training to report an emergency and initiate lockdown or other emergency protocols from outside the building through standalone devices, smartphone apps, etc.

ARCHITECTURAL COMPONENT:

TIER 1

A. **Signage (Directing Visitors to the Appropriate Areas).** Basic wayfinding from the perimeter parking lot should be clear from any point within it. Signage is the most direct means of guiding building users and visitors to the appropriate point of entry. Signage is enhanced by indirect cues provided by thoughtfully designed landscape walkways, crosswalks and architectural elements at the desired building entry points. Signage should be placed on every door indicating that all visitors must sign in at the front office and that individuals attempting to enter without authorization are subject to arrest.

B. **Signage Directing to Emergency Communication Device.** Signs should be posted that provide clear direction to an emergency communications device (if property is equipped), designed with an emergency and a user's likely state of heightened stress in mind.

© 2025 Partner Alliance for Safer Schools

C. **Apply CPTED Principles for Territorial Reinforcement, Access Control and Natural Surveillance.** Using CPTED promotes "territorial reinforcement" by clearly designating school property. Fencing, plantings, berms or a blend of all three can be used to discourage trespassers, well-meaning or otherwise. For new construction, landscaping should be planned with clear sight lines in mind. It is also recommended to establish clear sightlines from perimeter windows to the parking lot by removing or trimming vegetation. Exterior lights should be installed at strategic points on the building perimeter, illuminating the area during periods of darkness so that unauthorized and criminal activities are more easily recognized and deterred.

D. **Trespassing, Video Surveillance and Access Notification Signage.** In addition to the physical cues noted above, signage along the boundary of school grounds sends an unambiguous message regarding the hours (if any) when the public is welcome.

   The campus perimeter should be clearly defined with signage stating that entry onto school property is limited to authorized visitors and those on official school business. In cases where school grounds are used by the public after school hours, however, signage at these schools should include hours the grounds are open to public and what activities and items are prohibited, such as drug or alcohol use, unleashed pets, fireworks, dangerous horseplay and weapons. If your district has a security or law enforcement department that monitors and responds to situations on school property, it is recommended the department phone number be posted on the signs. Signage to discourage illegal dumping should be posted on dumpsters and in immediate areas.

E. **Properly Positioned Exterior Lights.** Outdoor lights should be installed at strategic points on the campus perimeter and illuminate the area evenly during periods of darkness so that unauthorized and criminal activities are more easily recognized. Lighting should be directed toward the area rather than outward, with fixtures employing cut-off shrouds which limit "hotspots" for security cameras (either current or future), eliminate glare for residential neighbors and preserve night sky.

F. **Debris Clearance.** The school property should be clear of debris. Trees, shrubs and other growth should be cut back to minimize interference with lines of sight throughout the property. Annual inspection should be scheduled to maintain clear sight lines and limit places where individuals could hide for criminal purposes.

TIER 3

A. **Gates at Entrances.** Gates should be installed at all drive entrances or at other strategic drive "choke points" to allow school officials to effectively lock down the perimeter after regular business hours. This practice discourages the use of school property for unauthorized and/or illegal activities.

B. **Landscaping to Control Vehicle Access.** Materials such as decorative rocks, shrubs and planters can be used to help keep vehicles off unauthorized areas of property.

© 2025 Partner Alliance for Safer Schools

TIER 4

A. **Lighting to Enhance Video Surveillance.** Outdoor lighting should be implemented specifically to enhance video surveillance visualization. Strive for relatively consistent foot candle[2] levels across the area to be monitored, as even lighting allows better imaging than uneven lighting. Minimum foot candle illumination set forth by local planning and zoning authorities generally supports effective lighting levels for surveillance video monitoring.

COMMUNICATION COMPONENT:

TIER 1

A. **Public Address Systems:** Schools should ensure the ability to provide one-way communication to the green space areas of the school property. Green space areas include:
   - Areas between school buildings in which students and staff are present during class changes
   - Playgrounds and athletic fields within the campus perimeter
   - Reunification points within the campus perimeter
   - Temporary/ Mobile Classrooms
   - Parking Lots and Garages

   The minimum standard of providing critical communication outside of the school building is to ensure that students and staff who are not within the building receive a clear, concise and easy-to-understand audible message. This notification can be performed through various low-voltage systems. Mass notification capability within the property layer could be achieved through the addition of a zone on the emergency paging system or fire alarm system that has the voice component. Communication needs within the parking lot (or garage) area is similar to communication needs within the campus perimeter layer. While these areas may be attended for very short periods of time, they still need a communication mechanism to ensure that all persons with this layer are notified of a threat.

TIER 2

A. **Local Area Two-Way Radio System Between Office and Staff.** The property layer of a school encompasses anything from playgrounds to athletic fields. To enhance the ability to communicate a threat to students and staff, a two-way radio system allows the administrative staff to communicate immediately with staff who are responsible for the students who may be outside of the building.

2 A "foot candle" is the most common unit of measure used by lighting professionals to calculate light levels in businesses and outdoor spaces. A foot candle is defined as the illuminance of a single candle within a one-foot radius.

© 2025 Partner Alliance for Safer Schools

TIER 3

A. **Visual Indicators Specific to Hazard.** Providing more than one form of communication (audible) during an emergency event is preferred. The use of visual indicators outside of the building allows for the students and staff to be made aware of a threat through a different sense. According to the NFPA, both audible and visual cues to alert persons are essential to communicating a threat. Enhanced implementations accomplish this through color-coded visual cues that correspond to specific types of threats.

B. **Digital Low-Band Radio System Connected to District-Wide System.** As discussed above, a two-way radio system is the most efficient way to quickly communicate with staff and students outside of the building. A district can implement a two-way radio system that also communicates on a district- and community-wide level. Within the campus perimeter, this allows the staff outside the school to communicate with the district and local emergency responders as needed by simply changing the frequency on the radio.

C. **Two-Way Emergency Phones in Parking Areas.** Depending on the size of the school campus, a parking lot area can encompass a vast amount of space that is difficult to monitor, providing a setting susceptible to threats. It is important to have some sort of two-way communication allowing the persons in the parking lot space to quickly communicate with the security team of the district.

   Two-way emergency phones provide locations from which a person can communicate with the security team of the district. These emergency phones are normally placed strategically and in sufficient numbers so that one is accessible within 200 feet of any location within a parking lot.

   These devices also have the capability to integrate with the video surveillance system to allow for audio and visual communication with security personnel. Use of this technology is particularly important within large campuses that have multiple parking areas.

TIER 4

A. **Install Audio/Video Call Boxes at Key Locations.** Audio and video emergency call boxes have been popular and effective technology deployments for maintaining safe school campuses. While more prevalent on college campuses, many K-12 schools are also realizing the benefits of utilizing video call boxes for emergency situations, and in some cases for access control.

B. **Audible and Visual Mass Notification Tied to District-Wide System.** Many intercom, emergency paging and fire alarm voice communication systems include the capability to be networked into one district-wide system. This technology allows for the use of products from multiple manufacturers integrated together to provide a unified system. Districts should explore using existing technology already installed in schools to economize and maximize the ability to provide a district-wide emergency communication system.

© 2025 Partner Alliance for Safer Schools

VIDEO SURVEILLANCE COMPONENT:

The perimeter of a school includes the area immediately surrounding the facility and school property where students and staff congregate for activities. It may include athletic fields, playgrounds, parking lots and other general use areas. In many cases, school property borders commercial or residential zone areas. It is not uncommon for access to school property to be restricted during school hours but open to the public during off hours and the weekend. The differences in location and multi-use nature of school property means that no two schools are alike. A proper risk assessment will define the risks and mitigation techniques that should be employed.

Video surveillance is one component that can be used to mitigate risks for school perimeters by providing **surveillance, assessment, forensics** and **risk mitigation** as defined in the district-wide layer in the Guidelines.

Today, there are many different capability levels available in video surveillance equipment. Establishing an "operational requirement" for each camera deployed ensures the selection of equipment appropriate to the specific uses for which it is intended. These operational requirements are generally defined as allowing the human operator to do the following visually:

- **Detection**–The ability to determine whether a person or object is in the field of view of the camera
- **Observation**–The ability to differentiate and classify people and objects in the field of view of the camera (e.g., man or woman, child or adult, red or blue jacket, two cars and one truck)
- **Recognition**– The ability to identify an object with a higher degree of certainty, such as recognizing a familiar face or type of specific type of vehicle.
- **Identification**–The ability to identify specific individuals or objects where present in the field of view of the camera (e.g., John Smith, a 2009 Toyota Camry, a license plate number)

Each of these operational requirements is defined by the number of "pixels on target" recorded of the object or person in the field of view. For people, the number of pixels measured across the width of their face determines what operational requirement is achieved. While there are no established standards to define pixels on target to meet specific operational requirements, the following chart outlines generally accepted thresholds in the security industry.

Operational Requirement	Horizontal Pixels/Face	Pixels per Inch
Identification	80	13
Recognition	40	4
Observation	20	2
Detection	4	1

Unless otherwise determined in a risk assessment, **observation** and/or **detection** are the operational requirements for video surveillance of large outdoor areas. See Figures 1 and 2.

© 2025 Partner Alliance for Safer Schools

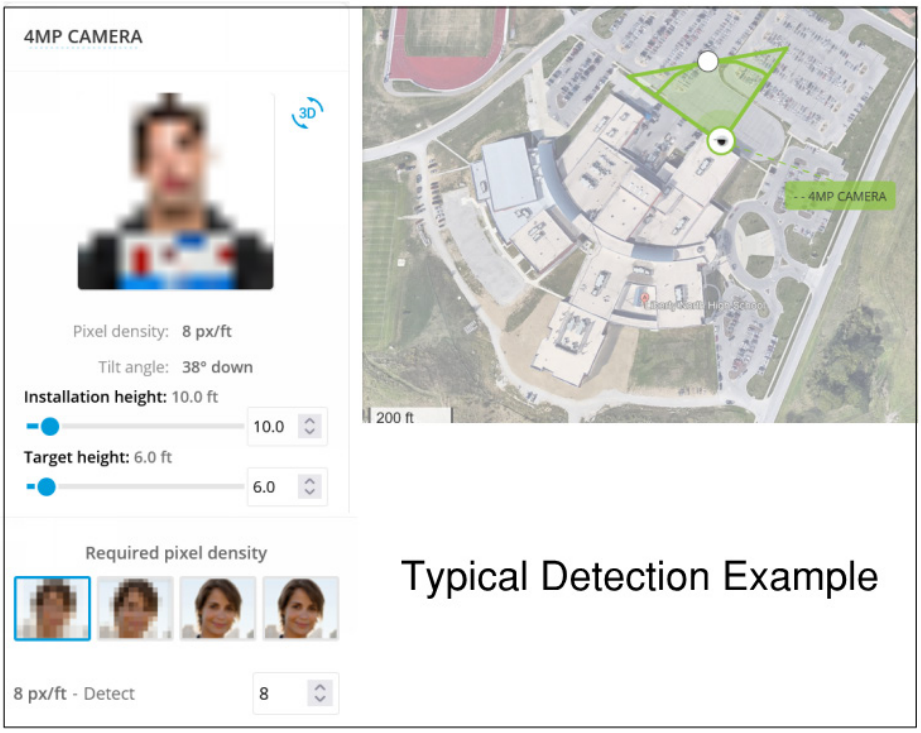


Figure 1. Pixels on Target/Pixel Density Example

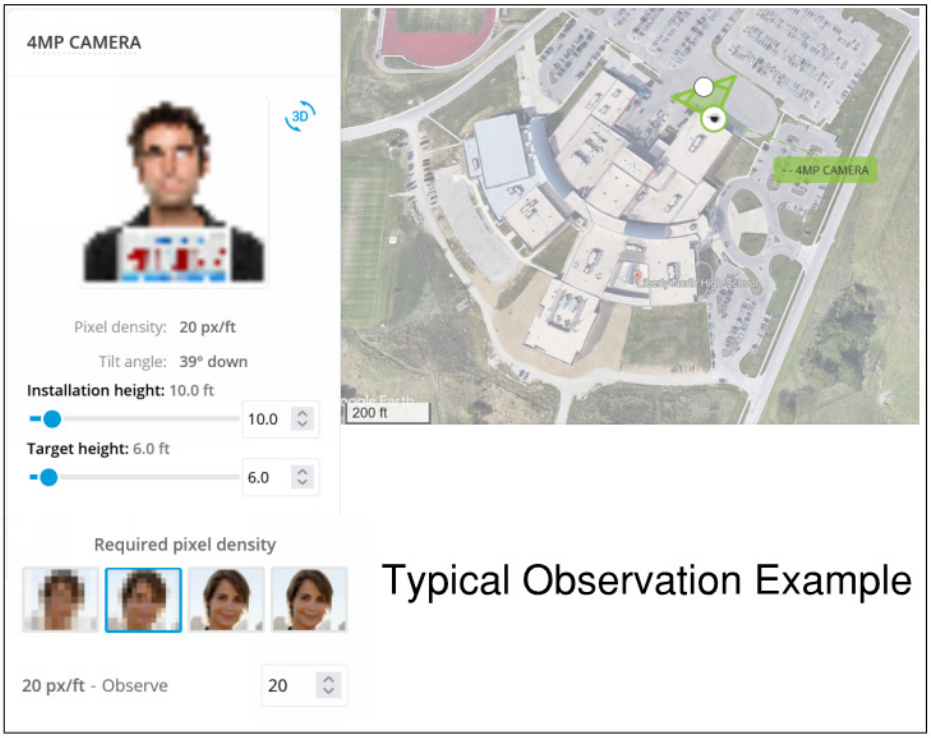


Figure 2. Pixels on Target/Pixel Density Example

© 2025 Partner Alliance for Safer Schools

TIER 1

A. **Fixed Cameras, Wide Area Coverage of Key Campus Areas.** After a local assessment from the school or district's safety team, exterior camera coverage should include identified problem areas such as playgrounds, athletic fields, parking areas, and vehicle entry points with pixels on target based upon operation requirements. Pixel recommendations are outlined in Figures 1 and 2.

   Fixed cameras provide video surveillance of outdoor activities taking place in the cameras field of view. Cameras should be rated for outdoor use to prevent ingress of dust or water and environmentally rated to function in both upper and lower temperature ranges.

TIER 2

A. **Infrared (IR) Cameras or Lighting.** Supplemental lighting, via IR or visible light, refers to adding additional light to a scene to improve video surveillance image quality and usability after hours. Supplemental light can be either IR or visible light. IR lighting is invisible to the human eye but can be captured by a camera providing covert illumination of an area. The main drawback to this approach is that the images recorded and viewed are in black and white only and no colors are represented, which can impair situational awareness for surveillance, assessment and forensic use cases. Visible lighting illuminates an area with white light providing improved situational awareness with color images. There are many types of visible light luminaries, such as LED, halogen and fluorescent, but LED tends to offer long-term cost savings and better color rendition. Adding visible light to an area has the additional benefit of improving "natural surveillance" by human observers, which is a principle of CPTED.

   Image sensor technology has progressed to the point where color imagery is possible in the near absence of visible light. For this reason, some school districts have reduced the use of supplemental lighting to decrease operating costs while still maintaining the operational requirement for the use case defined. This approach decreases natural surveillance, so schools need to evaluate if it is the right approach for them.

B. **People Identification Field of View at Pickup/Drop-Off Area.** Video surveillance covers the specific area where children are released to their parent or guardian, which will ensure that the school has a visual record of to whom a child was released. An ideal situation would be to pair this camera with a fixed camera, wide area coverage field of view to also record details of the vehicle used by the parent or guardian. In some cases, a higher-resolution camera with a wide area lens can provide both. These cameras should be specified to meet the operational requirement of Identification defined above, rated for outdoor use to prevent ingress of dust or water and environmentally rated to function in both upper and lower temperature ranges. They should also include wide dynamic range sensors to ensure image usability.

C. **Perimeter Video Analytics.** This technology uses cameras or sensors to detect a person or object crossing a demarcation point, such as a fence or property line, and proactively alerts school security personnel so that a response can be initiated if required. Implementation of this technology should follow the manufacturer's guidelines for camera selection and placement.

© 2025 Partner Alliance for Safer Schools

D. **Wireless Video Data Transmission.** Wireless data transmission is used when camera placement precludes the use of wired transport due to high costs or distance limitations of the network. There are many wireless technologies available for schools to consider with different network speeds, data transmission rates, and distance or coverage area ranges. A wireless audit of the school and surrounding areas should be conducted to ensure that wireless technology chosen does not interfere with other systems and vice versa. A school should define the video surveillance use case and operational requirement before choosing a wireless technology to deploy. In this manner, a system can be designed around specific video surveillance needs that govern the bandwidth and distance requirements.

TIER 4

A. **Fixed Camera, Wide Area-Coverage Campus Wide:** Fixed camera coverage for the entire campus is most beneficial when districts use a SOC. The field of view should overlap the desired coverage area by at least one meter (when applicable) to ensure that the surveillance, assessment and forensics use cases are met. In some cases, cameras can be mounted directly on the building that houses the system's recording devices; this is the most cost-effective approach but can limit the field of view. Other mounting options include adding cameras to new or existing lighting poles around the campus perimeter or on other buildings on the school property such as athletic or maintenance structures. All these mounting options present the challenge of transmitting the video data back to the facility where video is recorded; this is accomplished through wired or wireless transmission, each with its own cost and technology limitations.

B. **PTZ Camera Coverage.** Pan/Tilt/Zoom Camera coverage should be based on an assessment for what specific needs exist for these types of cameras. PTZ cameras provide a means for proactively assessing a specific area of interest by remotely moving the camera's field of view and focal length; they require personnel manually operating the camera in response to an incident alert. For this reason, PTZ cameras are a great tool for assessment and surveillance use cases. They are of limited use if you do not have an operator but can be set to act as a fixed camera for a specific field of view when not being controlled. In some cases, PTZ cameras are set on a "guard tour" moving from one preset position to the next and providing video coverage of that area for a set amount of time. This way, one camera can cover multiple areas, but there is always the risk of a missed incident if the camera is covering a different area than that of the incident.

   PTZ cameras should be rated for outdoor use to prevent ingress of dust or water and environmentally rated to function in both upper and lower temperature ranges. They should also include wide dynamic range sensors to ensure image usability.

© 2025 Partner Alliance for Safer Schools

DETECTION AND ALARMS COMPONENT:

TIER 3

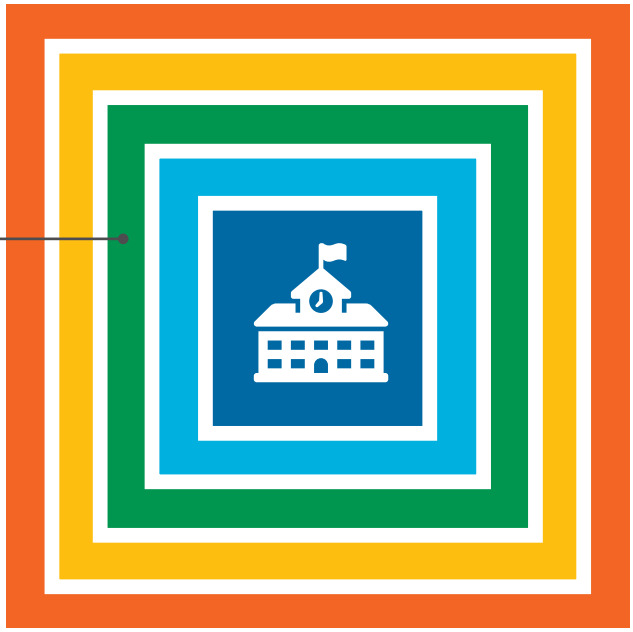
A. **Panic Alarm System Within Greenspace Areas.** All greenspace areas (as defined above) should have panic alarm buttons in easily accessible spaces that are hardwired or wireless physical buttons that are supervised.

   The school or district should consider whether the use of wearable devices for could be effective for personnel in the campus perimeter layer, and if so should ensure the technology selected is capable of being used outdoors and has coverage for all greenspace areas.

   When implementing wireless devices, it is important that the technology has redundancies built-in to ensure that the devices are operating within parameters. Any wireless panic system should be capable of monitoring to verify that each device is communicating with the panic alarm system. In addition, wireless devices should have a redundant way to transmit the signal is important. Finally, the hardware that monitors the wireless devices should have some sort of redundant power source (batteries, UPS, etc.).

© 2025 Partner Alliance for Safer Schools

BUILDING PERIMETER LAYER



» QUICKFIND

Building Perimeter Layer Checklist 91
Policies And Procedures Component 93
People (Roles And Training) Component 94
Architectural Component 94
Communication Component 104
Access Control Component 106
Video Surveillance Component 108
Detection And Alarms Component 111

© 2025 Partner Alliance for Safer Schools

BUILDING PERIMETER LAYER	TIER 1	TIER 2	TIER 3	TIER 4
POLICIES AND PROCEDURES				
» Categorization of ALL Exterior Openings	✔	✔	✔	✔
» Policy Established for Control of Exterior Openings	✔	✔	✔	✔
» Key Control Procedures	✔	✔	✔	✔
» Complete BDA/DAS Site Survey	✔	✔	✔	✔
PEOPLE (ROLES AND TRAINING)				
» Staff Trained on Door Protocols	✔	✔	✔	✔
» Visitor Management Process Training	✔	✔	✔	✔
ARCHITECTURAL				
» Signage Directing Visitors	✔	✔	✔	✔
» Security Key Box for First Responders	✔	✔	✔	✔
» Door Construction (New Construction/Renovation)	✔	✔	✔	✔
» Semi-Secure Visitor Entry Center - Shared Vestibule & Satellite Reception Office	✔	✔	✔	✔
» First Responder Door Numbering System Door #1	✔	✔	✔	✔
» Secured Vestibule	✔	✔	✔	✔
» BDA/DAS System (New Construction/Renovation)	✔	✔	✔	✔
» One-Way Film on Exterior Windows to Prevent Visual Access	✔	✔	✔	✔
» Security Film for Exterior Door Vision Panels and SideLites	✔	✔	✔	✔
» Semi-Secure Visitor Entry Center (Divided) - Divided Shared Vestibule & Satellite Offices		✔	✔	✔
» Security Film for Exterior Door Vision Panels and SideLites		✔	✔	✔
» Force Entry Glass for Exterior Door Vision Panels and SideLites		✔	✔	✔
» Secure Visitor Entry Center - Separate Visitor Entrance & Administration Suite			✔	✔
» Door Construction (New Construction/Renovation)			✔	✔
» Ballistic Security Glass for Exterior Door Vision Panels and SideLites			✔	✔
» Secure Visitor Entry Center with Visitor Area A Separate Enlarged Visitor Entrance and Secure Administration Zone				✔
SECURITY, BALLISTIC AND FORCE PROTECTION GLAZING				
» Primary Entrance Doors and SideLites	✔	✔	✔	✔
» Secondary Entrance Doors and SideLites	✔	✔	✔	✔
» Tertiary Doors	✔	✔	✔	✔
» Egress-Only Doors	✔	✔	✔	✔
» Semi-Secure Visitor Entry Center Glazing	✔	✔	✔	✔
» Exterior Windows (Ground Level)	✔	✔	✔	✔
COMMUNICATION				
» Public Address System	✔	✔	✔	✔
» Main Entry Door Intercom With Two-Way Communications	✔	✔	✔	✔
» Audio-Visual Public Address System (AVPA)		✔	✔	✔
» Unify Communication Systems with Video Surveillance and Access Control		✔	✔	✔
» Audible and Visual Mass Notification Tied to District-Wide System				✔

© 2025 Partner Alliance for Safer Schools

	TIER 1	TIER 2	TIER 3	TIER 4
BUILDING PERIMETER LAYER				
ACCESS CONTROL				
» All Exterior Doors Secured With Lock or Exit Device	✔	✔	✔	✔
» Patented/Restricted Key System	✔	✔	✔	✔
» Key Management System	✔	✔	✔	✔
» Cylinder Dogging with Indicator	✔	✔	✔	✔
» Door Status Monitoring	✔	✔	✔	✔
» All Visitor Entry Exterior, Interior and Office Doors Secured With Remote Release and Audio/Video Door Entry System	✔	✔	✔	✔
» Electronic Access Control of Primary Entrances		✔	✔	✔
» Mobile Credentials for Emergency Responders			✔	✔
» Electronic Access Control of Tertiary Openings				✔
VIDEO SURVEILLANCE				
» Video Intercom at Visitor Entrance Points	✔	✔	✔	✔
» Exterior, Fixed Cameras for All Primary Openings		✔	✔	✔
» Exterior, Fixed Cameras on Secondary, Tertiary & Service Openings		✔	✔	✔
DETECTION AND ALARMS				
» Intrusion Detection on All Exterior Access Points	✔	✔	✔	✔
» Intrusion Detection System Monitored 24/7	✔	✔	✔	✔
» Partitioned Intrusion Detection			✔	✔

© 2025 Partner Alliance for Safer Schools

POLICIES AND PROCEDURES COMPONENT:

TIER 1

A. **Categorization of All Exterior Openings.** Every perimeter door should be classified as either primary, secondary or tertiary openings.

- Primary openings are main entrances, visitor entry center and public entry points (gym, PAC, etc.).
- Secondary openings are primarily for operational entry points such as staff entrances, doors leading to playground, additional buildings, etc., that are typically used on a daily basis for staff access and class change.
- Tertiary openings are emergency egress ONLY exterior doors. These doors include stairwell doors, large assembly areas requiring multiple egress, etc.
- Service openings are doors primarily used for service/utility access. These doors include mechanical, electrical, fire control rooms, etc.

Primary and secondary openings should be assessed for use by the public, staff and students with security enhanced or added as appropriate, such as the use of card readers and/or remote release capability as applicable.

B. **Policy Established for Control of Exterior Openings.** A policy should be set for governing when exterior doors are secured/ unsecured. Per fire and building codes, all perimeter doors allow free exiting of the building in the event of a fire or other emergencies that require evacuation of the building. For entrance into the building, primary and secondary doors should have electronic access control or cylinder (if manual operation). Exit devices should have a visual indicator so that security and building personnel can look at the device and determine if it is in a secure condition. Additionally, these exit devices should allow for dogging (putting into an unlocked state) only by means of a key (policy should minimize the use of this practice, to the extent practicable).

Practical limitations related to existing, especially older, buildings and the flow of students can make it very difficult to secure all perimeter doors. This is especially true at high schools with open campuses. All perimeter doors should be secured when students are in classrooms or when access from the exterior is not required for students to move from building to building. The number of doors unlocked during class changes should be limited. Any exterior doors that are unlocked during class changes should be monitored by a staff member or an SRO.

C. **Key Control Procedures.** Policies and procedures should be established to govern, track and revoke the distribution of keys and other access credentials as necessary. Keys should not be able to be duplicated without following a formal authorization process controlled by the district.

D. **Complete BDA/DAS Site Survey.** Bi-Directional Amplifier (BDA) and Distributed Antenna Systems (DAS) ensure that emergency first responder two-way communications systems will work inside the school, using a repeater or signal booster. Signal boosters may be required to ensure reliable radio communications both for campus staff and local emergency responders in stairwells, hallways, parking lots and other common areas where signals can be interrupted by building materials, dead spots and signal interference. A site survey to determine the need for this equipment can be conducted at no cost by local fire departments or radio manufacturers in many cases.

© 2025 Partner Alliance for Safer Schools

PEOPLE (ROLES AND TRAINING) COMPONENT:

TIER 1

A. **Staff Trained to Lock/Unlock Doors Per Policy.** Teachers, substitutes and other relevant staff should be trained on the proper procedures to lock and unlock primary and secondary doors at necessary times throughout the day. Electronic access measures (at higher TIER levels) can be used to supplement these procedures, facilitating class changes and other access needs.

B. **Visitor Management Process Training.** Admittance of all visitors, including vendors, parents, community members, substitute teachers and others who are not employed by the school, should follow a documented visitor management process led by main office personnel using a single point of entry. All relevant staff, including substitute teachers, should receive full training on the visitor management process.

ARCHITECTURAL COMPONENT:

Secure Visitor Entry Center

The secure visitor entry center allows staff to safely interact with visitors while going through the verification process, rather than allowing them into the office or building prior to vetting them. The multiple physical layers allow for the multiple steps of the verification process to have corresponding levels, with the ultimate goal of only allowing a visitor into the least secure layer of the building they absolutely need access to. The components of the secure visitor entry center consist of the entrance/vestibule space, staff/visitor interaction window, package transfer system, and the relationship to the office/administration area.

When the visitor entry is shared with the main entrance vestibule it creates a semi-secure space due to the fact that a visitor can bypass the intended entry sequence and gain access to the building by piggybacking or tailgating, grabbing a door while someone is leaving, someone inside the building opening the interior door for them, or from door locks/closures not working properly. To create a secure visitor entry center, a separate visitor entrance that only provides access to a secure reception/office area is required.

Regardless of the configuration, the entrance should be locked at all times and be the only means for visitors/vendors to gain entry to the building. An indirect means of communication should be provided through the use of a video doorbell/intercom to allow staff to see and interact with visitors prior to allowing them access to the entry vestibule. Where the space is shared with the main entrance, the interior doors should be locked and monitored at all times, while allowing means for staff to bypass the office area through access-controlled doors. In existing buildings where the office area is remote from the entrance, policies and procedures should be developed for staff to escort visitors from the entrance vestibule to the administrative offices or elsewhere in the building.

A secure interaction window should be provided between the vestibule and reception to allow for direct communication between staff and visitors to continue the verification process and their reason for being at the building. If just dropping

© 2025 Partner Alliance for Safer Schools

off/picking up something this can be completed without any further access to the building by a pass-through tray/drawer and/or package transfer system. If the person does have a valid reason to access the building, they should be processed through the school's visitor management system, prior to being allowed access to the next physical layer. In cases where the visitor does not pass the verification process, they should not be allowed further access into the building. A visitor management system interface should be located in the vestibule that allows visitors to enter their information and scan their ID while being monitored by staff via a computer located in the reception space. Staff should verify all information, and that the ID provided matches the person presenting prior to authorizing the printing of the visitor badge and allowing access to the secure visitor waiting area.

Doors between the secure visitor waiting area and building interior should be provided with access-control measures that allows staff to remotely unlock the doors and the means for credentialed staff access. Additionally, access-controlled doors should be provided between the secure waiting area and reception staff space, along with other administrative areas.

TIER 1

A. **Signage (Directing Visitors to the Appropriate Areas).** Signage should be placed on every door indicating that all visitors must sign in at the front office and that individuals attempting to enter without authorization are subject to arrest.

B. **Security Key Box for First Responders.** A lock/access box, separate from the Fire Department box, should be installed for local law enforcement and first responders for access to credentials and/or keys to the building. The box should be blue in color. Local law enforcement and fire department should be consulted for the location of the lock/access box. There are situations where it is sometimes necessary to install more than one lock/access box. The size of the box should be considered for additional material such as issued keys, throw bag and electronic access keys (see NFPA 3000).

C. **Door Construction (New Construction/Renovation)**. Exterior doors should be a minimum of 1 ¾" thick heavy duty (16 ga.), steel doors or aluminum doors with pry-proof metal frame. Glazing in doors and surrounding frames/windows should be safety laminated.

D. **Semi-Secure Visitor Entry Center - Shared Vestibule & Satellite Reception Office.** When the visitor entrance and vestibule space is shared with the main entrance, it creates a Semi-Secure Visitor Entry Center. (See Figure A) At these shared spaces, additional measures must be taken to offset the lacking physical layers, particularly in the development of policies and procedures, along with the training of staff.

   At minimum, direct access to a Satellite Reception Office should be provided, which allows space for the final steps of the verification process and a secure waiting area for visitors. Where access directly to a conference room and/or office is not available, staff members should escort visitors from the secure visitor waiting area to the office area or elsewhere in the building. Consideration should be given to the layout of this space to allow for future expansion to include access to conference rooms and administrative offices.

© 2025 Partner Alliance for Safer Schools

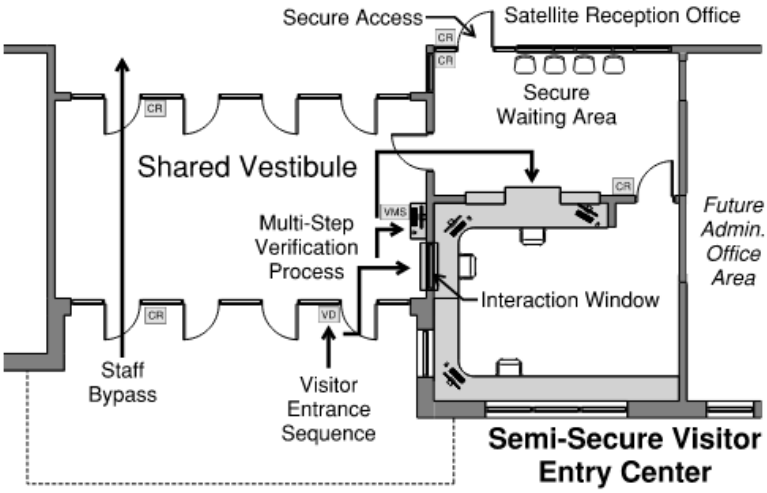


Figure A

A secure interaction window should be provided between the vestibule and reception to allow for direct communication between staff and visitors. Ideally this would also include the means to securely transfer smaller items like papers and small objects from one side to another.

To allow for the safe transfer of larger items, where a package transfer system is not included, a location, like a table, should be provided where these items can be left and later retrieved by when the vestibule is empty.

E. First Responder Door Numbering System Door #1. The Secured Visitor Entry Center, regardless of which Tier level, should be the door labeled #1 per first responder numbering system in the District-Wide Layer. (See District-Wide Layer, Tier 1 – Section B).

F. Secured Vestibule. The main (visitor) entry should be a secured vestibule with a mechanical lock or exit device as required by code and a doorbell. A staff member or authorized volunteer must assess a visitor's request to enter for any overt or suspected threat and then physically open the door or release it electronically if the opening is so equipped. The ability to visually assess the visitor is critical, whether directly or remotely (see intercoms in Communications and Video Surveillance).

G. BDA/DAS System (New Construction/Renovation). Two-way radio signal boosters may be required in new construction/ renovation for compliance with the emergency responder radio coverage. Requirements are determined through a site survey. The evolution of new composite construction materials and wireless networks can interfere with effective radio coverage for first responders. Schools can find more information on these technologies through IFC-510 or NFPA-72, Chapter 24.

H. One-Way Film on Exterior Windows to Prevent Visual Access. One-way window film installed on lower classroom windows prevents visual access from the outside while allowing occupants clear visibility from the inside the classroom.

I. Security Film for Exterior Door Vision Panels and Sidelites. Security window film should be installed on all exterior door vision panels[1] and sidelites (sometimes also referred to as sidelights).[2] Security film serves to deter or delay the

1 Door vision panels are windows incorporated into a door.
2 Sidelites are narrow windows immediately adjacent to a doorway.

© 2025 Partner Alliance for Safer Schools

ability of an attacker to breach a doorway using a firearm or other tool/weapon, in addition to limiting injuries from glass shards resulting from a blast, fire, accident, natural disaster or severe weather event. This type of solution can be retrofitted within most commercial window systems and incorporated into insulating glass units.

TIER 2

A. **Semi-Secure Visitor Entry Center (Divided) - Divided Shared Vestibule & Satellite Offices.** Divided Shared Vestibule & Satellite Offices. This vestibule is similar to the shared vestibule but has a physical barrier that sub-divides the space to allow for a dedicated visitor entrance door and staff-only access, while still allowing for all doors to be used for student drop off or egress. (See Figure B) This space would still only be considered semi-secure, as it is possible to gain access to the building, however it reduces the likelihood of a visitor tailgating a staff member into the building or grabbing a door when someone is leaving.

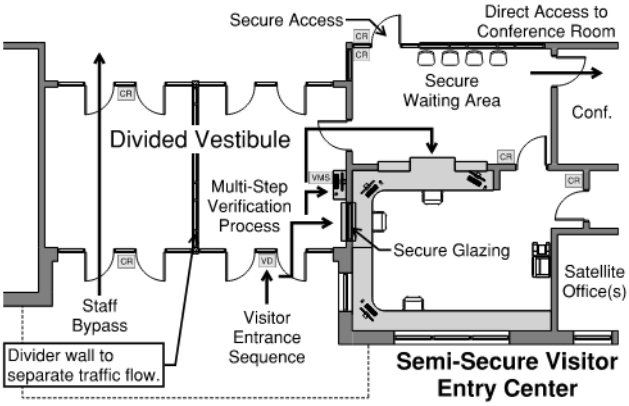


Figure B

Direct access should be provided from the secure waiting area to an adjacent conference room(s) whereas visitors do not need to be escorted through the building for a meeting. Additionally, satellite offices should be provided for administrative staff that require the most interaction with parents and/or visitors. These offices should only be accessible only through doors with access-controlled hardware, ideally located within the receptionist's space and not the visitor waiting area.

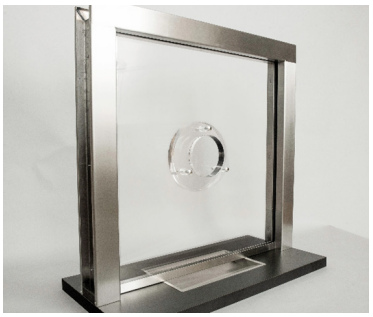






Figure C



Figure D

© 2025 Partner Alliance for Safer Schools

A "teller style" window (See Figure C) should be provided between the vestibule and reception to allow for direct communication and include the means to securely pass small items from one side to another. This window should provide protection against forced entry (See Secure Glazing.) Additionally, a package transfer passthrough drawer or box should be provided to safely pass larger items between visitors and staff. These systems can be incorporated into the interaction window or be a separate device. (See Figure D) Consideration should be given to the size of potential items needing to be transferred on a regular basis when sizing the system. For items that are too large for the package transfer system, policies and procedures should be developed to leave these items in the vestibule and later retrieved by staff.

B. **Security Film for Exterior Door Vision Panels and Sidelites.** Security window film should be installed on all exterior door vision panels and sidelites. Security film serves to deter or delay the ability of an attacker to breach a doorway using a firearm or other tool/weapon, in addition to limiting injuries from glass shards resulting

C. **Force Entry Glass for Exterior Door Vision Panels and Sidelites.** Force entry glass should be considered for the windows, sidelites and door vision panels for the secure visitor entry area. This provides additional protection from staff interacting with visitors.

TIER 3

A. **Secure Visitor Entry Center - Separate Visitor Entrance & Administration Suite.** This separate entrance into a secure space, only allows for access into the Secure Waiting Area and not directly into the rest of the building. (See Figure E) This greatly reduces the ability for a visitor to tailgate staff into the building, as they would have to follow them through multiple doors, or be let into the building, as they have no reason to be in the entrance vestibule.

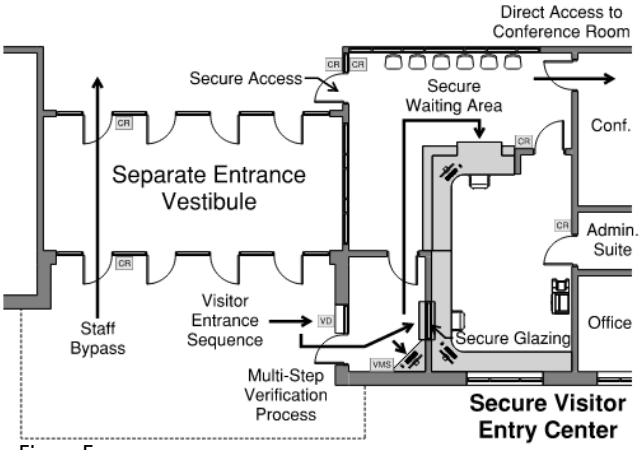


Figure E

Direct access to conference room(s) and/or meeting spaces should be provided and sized according to the school's needs. Consideration should be given to providing access directly from the Secure Visitor Waiting Area to amenities, like restrooms, without having to allow visitors access to the interior of the building or administrative areas. A complete Administrative Suite should be provided and include all administrative functions and required support spaces. Secure

© 2025 Partner Alliance for Safer Schools

access to the Administrative Suite should be provided through doors with access-controlled hardware. Access from the secure waiting area to the office area should only be provided within the reception area, thus providing an additional layer between these two spaces.

The secure interaction window and package transfer system should provide protection against forced entry and ballistics. (See Secure Glazing)

B. **Door Construction (New Construction/Renovation).** Doors should be constructed with a minimum of 1-¾" thick maximum duty steel installed in a steel frame.

C. **Ballistic Security Glass for Exterior Door Vision Panels and Sidelites.** Several forms of security glass are available, incorporating acrylic, polycarbonate and other materials. Each has specific characteristics, weight and thickness depending on the intended use and level of ballistic resistance required. Security glass should be installed in all exterior door vision panels and sidelites and should meet or exceed the UL Level 3 standard for ballistic protection.

TIER 4

A. **Secure Visitor Entry Center With Visitor Area A Separate Enlarged Visitor Entrance and Secure Administration Zone.** This space is similar to the secure visitor entry center but provides additional space for visitor waiting to check in, and direct access to functions like restrooms. This allows more people to be in the secure vestibule while checking in without allowing them into the secure visitor waiting area. Additionally, administrative areas are completely separate from the public areas of the school. With secure secondary access into the administration area and direct egress to the exterior. This creates a secure administrative zone which provides a secure area for administrative functions with secured access to the rest of the school. See Figure F.

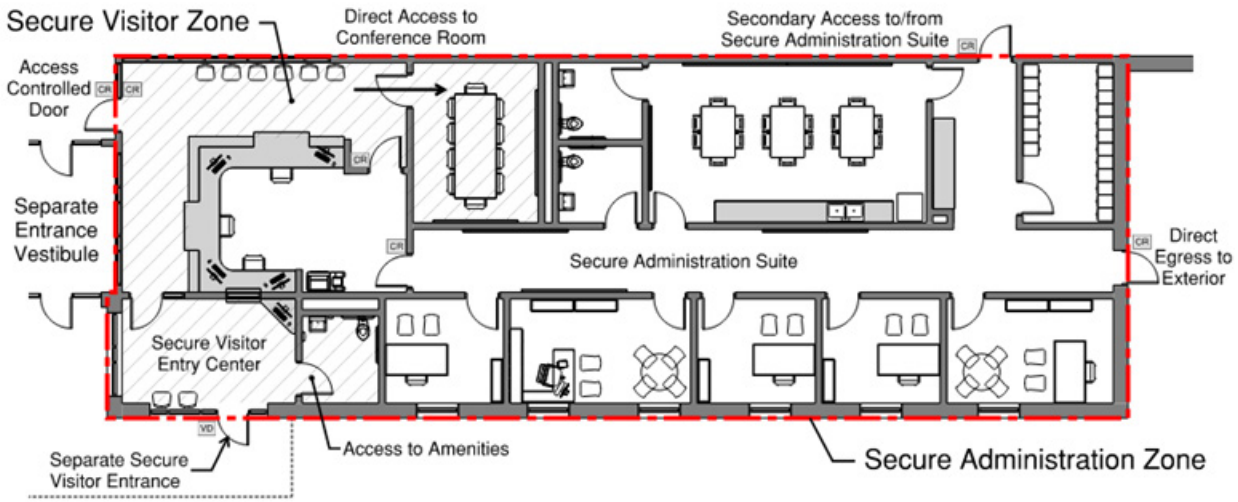


Figure F

© 2025 Partner Alliance for Safer Schools

- The Administrative Suite should not only provide controlled access from the reception space but also have a secondary secure entry point from the building interior. This allows staff to access the Administrative Suite without having to go through the visitor waiting area, which reduces traffic and interior doors being opened, as well as reducing the potential conflicts between parents/visitors and administrative staff. Additionally, direct egress to the exterior should be provided, allowing staff a way to safely exit the building in the event of an emergency, without having to go through the waiting area and/or building where an incident could be occurring.
- The interaction window and package transfer system should provide protection against force entry and ballistics. (See Security Glazing.)

SECURITY GLAZING

The term "security glazing" can encompass a large number of products and systems that provide increased levels of security, but it is important to understand that the glazing is only a portion of the system. Consideration must also be given to the door, door frame, hardware, lock, and surrounding wall to fully account for the security level. It is important to point out that no solution will 100% prevent a determined assailant from gaining access to the building. However, it does allow for the security principles of deter, detect, delay and defend, to be implemented. The intent of utilization of security glazing is to delay an active threat, essentially buying time for resources to be deployed to defend against the threat. Each additional layer of security increases this amount of time while also creating multiple points to detect the intrusion. The overall goal is to deter an active threat from even considering an attempt at gaining access to the building by force.

Security glazing is most commonly categorized into two types: ballistic and force protection. These terms are applied through rigid testing procedures and understanding how and why these procedures were developed will assist in understanding which type should be utilized.

BALLISTIC GLAZING:

Testing procedures for ballistic glazing require the system to stop a certain number of projectiles of a prescribed weight and velocity to achieve the specific rating. There is no requirement for the glazing to stay in the frame after the testing is completed, and additional projectiles are permitted to pass through the glazing after completion of the testing. Currently the two most commonly used testing standards are the "Underwriters Laboratory (UL) 752 Standard for Ballistic Resistance" and the "National Institute of Justice (NIJ) Standard 0108.01 Ballistic Resistant Protective Materials."

FORCE PROTECTION GLAZING:

The notable difference with force protection glazing is that projectiles may penetrate the glass, it is required to stay in the frame even when force is applied after the fact. At this time the only testing procedure that addresses force protection from an active assailant perspective, is the ASTM-F3561 "Standard Test Method for Forced-Entry-Resistance of Fenestration Systems After Simulated Active Shooter Attack." The testing procedure consists of compromising the glazing with ballistic penetration, then a battering ram is used to applying a prescribed amount of forces until the glass assembly fails. While

© 2025 Partner Alliance for Safer Schools

the ASTM-F5361 is to be applied to complete assembles, the appendix does prescribe how testing can be applied to the components of the system, including glazing and film products. ASTM is currently working on creating a separate standard for these criteria with the intent of having equivalent levels to the ASTM-F5361.

TIER 1

A. **Primary Entrance Doors and Sidelites:** Primary entrance doors and sitelites should be ASTM-F5361 Level 1 (or equivalent).

B. **Secondary Entrance Doors and Sidelites:** Doors and sidelites that have direct public access should be rated to ASTM-F5361 Level 1 (or equivalent), other locations should be safety laminated.

C. **Tertiary Doors:** These doors should not have any windows or openings. Where vents are required, consideration should be given to their size. If the spaces beyond these doors have access to the building interior, additional considerations should be considered.

D. **Egress-Only Doors:** These doors should not have any glazing, if glazing is required it should be a narrow lite to limit any potential access. Glazing should be Laminated.

E. **Semi-Secure Visitor Entry Center Glazing.** Exterior Doors & Sidelites should, at minimum, be laminated, and priority given to interior windows as an assailant could gain access to the vestibule area before their intentions are known. Ideally, exterior glazing should be rated the same as that of the interior.

   Suggested Glazing Levels for Doors, Sidelites and Windows:

   - Interior Vestibule Doors, Sidelites and/or Windows – ASTM-F5361 Level 1 (or equivalent).
   - Staff/Visitor Interaction Window – ASTM-F5361 Level 3 (or equivalent).
   - Interior Doors & Windows between Secure Visitor Waiting Area and Building Interior – Safety Laminated
   - Exterior Windows at Reception and Offices – Safety Laminated

F. **Exterior Windows (Ground Level)** – Locations at mass congregant areas should be rated to ASTM-F5361 Level 1 (or equivalent), all other locations should be safety laminated.

TIER 2

A. **Primary Entrance Doors and Sidelites:** Primary entrance doors and sitelites should be ASTM-F5361 Level 3 (or equivalent).

B. **Secondary Entrance Doors and Sidelites:** Doors and sidelites that have direct public access should be rated to ASTM-F5361 Level 3 (or equivalent), other locations should be rated to ASTM-F3561 Level 1 (or equivalent).

C. **Tertiary Doors:** These doors should not have windows or vents, where vents are required tamper resistant vents should be provided.

© 2025 Partner Alliance for Safer Schools

D. **Egress-Only Doors:** These doors should not have any glazing, if glazing is required it should be a narrow lite to limit any potential access. Glazing should be rated to ASTM-F5361 Level 1.

E. **Semi-Secure Visitor Entry Center Glazing:**
Suggested Glazing Levels for Doors, Sidelites and Windows:

- Exterior Doors & Sidelites - ASTM-F5361 Level 1 (or equivalent).
- Interior Vestibule Doors, Sidelites and/or Windows - ASTM-F5361 Level 3 (or equivalent).
- Staff/Visitor Interaction Window - ASTM-F5361 Level 5 (or equivalent).
- Interior Doors & Windows between Secure Visitor Waiting Area and Building Interior - ASTM-F5361 Level 1 (or equivalent).
- Exterior Windows at Reception and Offices - Locations that have direct public access should be rated to ASTM-F5361 Level 1 (or equivalent), other locations should be safety laminated.

F. **Exterior Windows (Ground Level)** - Consideration should be given for windows in locations that have direct public access to be rated to ASTM-F5361 Level 1 (or equivalent).

TIER 3

A. **Primary Entrance Doors and Sidelites:** Primary entrance doors and sitelites should be ASTM-F5361 Level 5 (or equivalent).

B. **Secondary Entrance Doors and Sidelites:** Doors and sidelites that have direct public access should be rated to ASTM-F5361 Level 5 (or equivalent), other locations should be rated to ASTM-F3561 Level 3e (or equivalent).

C. **Tertiary Doors:** These doors should not have windows or vents, where vents are required tamper resistant vents should be provided.

D. **Egress Only Doors:** These doors should not have any glazing, if glazing is required it should be a narrow lite to limit any potential access. Glazing should be rated to ASTM-F5361 Level 3.

E. **Secure Visitor Entry Center Glazing:**
Suggested Glazing Levels for Doors, Sidelites and Windows:

- Exterior Doors & Sidelites - ASTM-F5361 Level 3 (or equivalent).
- Interior Vestibule Doors, Sidelites and/or Windows - ASTM-F5361 Level 5 (or equivalent).
- Staff/Visitor Interaction Window - UL572 Level 3 (or equivalent) AND ASTM-F5361 Level 5 (or equivalent).
- Interior Doors & Windows between Secure Visitor Waiting Area and Building Interior - ASTM-F5361 Level 3 (or equivalent).
- Exterior Windows at Reception and Offices - Locations that have direct public access should be rated to ASTM-F5361 Level 3 (or equivalent), other locations should be rated to ASTM-F5361 Level 1 (or equivalent).

© 2025 Partner Alliance for Safer Schools

F. **Exterior Windows (Ground Level):** At locations that have direct public access should be rated to ASTM-F5361 Level 1 (or equivalent).

TIER 4

A. **Primary Entrance Doors and Sidelites:** Primary entrance doors and sitelites should be rated both to UL572 Level 3 (or equivalent) and ASTM-F5361 Level 5 (or equivalent).

B. **Secondary Entrance Doors and Sidelites:** Doors and sidelites that have direct public access should be rated to both UL572 Level 3 (or equivalent) and ASTM-F5361 Level 5 (or equivalent), other locations should be rated to ASTM-F3561 Level 5 (or equivalent).

C. **Tertiary Doors:** These doors should not have windows or vents, where vents are required tamper resistant vents should be provided.

D. **Egress-Only Doors:** These doors should not have any glazing, if glazing is required it should be a narrow lite to limit any potential access. Glazing should be rated to ASTM-F5361 Level 3.

E. **Secure Visitor Entry Center Glazing:**

Suggested Glazing Levels for Doors, Sidelites and Windows:

- Exterior Doors & Sidelites – ASTM-F5361 Level 5 (or equivalent).
- Interior Vestibule Doors, Sidelites and/or Windows – UL572 Level 3 (or equivalent) AND ASTM-F5361 Level 5 (or equivalent).
- Staff/Visitor Interaction Window – UL572 Level 7 (or equivalent) AND ASTM-F5361 Level 5 (or equivalent).
- Interior Doors & Windows between Secure Visitor Waiting Area and Building Interior – UL572 Level 3 (or equivalent) AND ASTM-F5361 Level 5 (or equivalent).
- Exterior Windows at Reception and Offices – Locations that have direct public access should be rated to ASTM-F5361 Level 3 (or equivalent), other locations should be rated to ASTM-F5361 Level 1 (or equivalent).

F. **Exterior Windows (Ground Level):** At locations that have direct public access should be rated to ASTM-F5361 Level 3 (or equivalent).

© 2025 Partner Alliance for Safer Schools

COMMUNICATION COMPONENT:

TIER 1

A. **Public Address System.** As within the campus perimeter layer, a school should have a one-way communication system reaching the areas immediately outside the building. In some cases, this will cover parking lots and playgrounds, but the priority for communication is for the areas in which students and staff would be outside near the building. These areas can include:
    - Drop-off/pickup areas
    - Sidewalks
    - Bus loading and unloading areas
    - Stand-alone mobile classrooms
    - Parking lots and garages

B. **Main Entry Door Intercom With Two-Way Communications**. This is an example of an area where access control, video surveillance and communication can be unified into a comprehensive system (see Video Intercoms below). As discussed in the architectural component, the main entrance should be secured with a means to remotely unlock the door. The entry process consists of audible communication followed by use of access control and video surveillance systems, which provide staff with the ability to remotely assess a visitor's request to enter and grant or deny access as dictated by policy or procedure.

TIER 2

A. **Audio-Visual Public Address System (AVPA):** Audio-visual public address systems include both intelligible audio and a visual component. NFPA defines AVPA as emergency communication systems (ECS). AVPA provide means of dual notification for those who might be sight or hearing impaired. The visual aspect of the system should have the capability of multiple colors to define specific threats. For example, red is for fire, blue for emergencies, etc.

    Some of the key elements for a NFPA 72, Chapter 24-compliant AVPA/ECS system include:
    - Intelligible audible communication in all areas in which staff and students occupy a space. "Intelligible" is defined as a clear, concise verbal signal that is easily understood. For practical purposes this means having public address speakers[3] in all classrooms, in addition to key shelter in place areas:
        - » All Instructional Areas (Classrooms)
        - » Hallways
        - » Administration Areas
        - » Staff Areas such as break rooms and work rooms

3 Relevant standards include UL 2017, Standard for General-Purpose Signaling Devices and Systems.

© 2025 Partner Alliance for Safer Schools

  - » Restrooms
  - » Public Areas including but not limited to:
    - Common areas
    - Collaborative areas
    - Library/media center
    - Auditorium/performing arts area
    - Gymnasium/weight-training rooms
    - Cafeteria including kitchen
- There must be two locations from which a message can be communicated throughout a school building using the system–generally the main/front office and a secondary secure location.
- The communication system should have an alternate power source, whether this is battery backup, an uninterruptible power supply or a backup generator, in case of main power failure.

Schools/districts need to be aware of the Americans with Disabilities Act (ADA) requirements for visual notification. There are specific types of strobes and strobes synchronize in order to prevent inducing physical harm to students and staff. In addition, ADA has some requirements on where visual notification should be installed.

Schools/districts should investigate possible interfaces to audio-visual resources that are already in use for education. For example, many televisions and messaging boards have the ability to be used for emergency messages.

Schools/districts should also be aware of the changes to International Building Code regarding elevator emergency communication. As of 2024, all elevators are to have an audio and video communication system in the elevator that is monitored 24/7.

B. **Unify Communication Systems with Video Surveillance and Access Control.** Communication systems should be integrated with access control and video surveillance to provide a unified security platform. The ability for school or district personnel to see what is happening around the building perimeter allows them to assess emergency situations and provide critical information to the students and staff through communication systems. Additionally, unification with the access control system allows for doors to be locked and unlocked remotely.

TIER 4

A. **Audible and Visual Mass Notification Tied to District-Wide System.** The public address system that provides notification around the building perimeter should be a "zone" of the district-wide communication system to provide a way to deliver emergency communication from a district-wide perspective.

© 2025 Partner Alliance for Safer Schools

ACCESS CONTROL COMPONENT:

Each school should invest in a plan to secure its building perimeter with an access control system that uses a combination of electronic and mechanical locks. Mechanical locks form the base for any access control system; however, electronic systems allow for historical and/or real-time tracking of ingress through secured doors, mitigates the expense of replacement of lost keys, allows for immediate deletion of access credentials when necessary and provides a means for the immediate lockdown of doors in the system.

Exterior doors should comply with appropriate locally enforced building codes for new educational occupancies, existing educational occupancies, new day care occupancies, existing day care occupancies, new business occupancies, existing business occupancies and ADA requirements.

TIER 1

A. **All Exterior Doors Secured with Lock or Exit Device.** Every exterior door not routinely used for class changes (secondary/ tertiary) should be secured with a working mechanical (or electronic) lock or exit device compliant with appropriate locally enforced building codes as well as the ADA. Tertiary openings should be exit only with no outside trim and should not have dogging mechanisms.

B. **Patented/Restricted Key System.** A patented or restricted key system offers protection against unauthorized key duplication by ensuring only authorized individuals can order key blanks and cut keys and cylinders for a key system. These common systems allow districts to control who has access to keys and can order them, which is a basic security function.

C. **Key Management System.** Requests for keys should be handled by a process in which each key distributed is logged and documented. Various types of systems and technologies are available to secure keys and track access and distribution.

D. **Cylinder Dogging with Indicator.** Where exit devices are provided with dogging feature (the ability to hold the exit device in an unlocked condition), the dogging mechanism should be the cylinder type with a visual indicator easily showing security staff whether the device is locked or unlocked.

E. **Door Status Monitoring.** All exterior doors should be electronically monitored to indicate whether the door is open or closed. This is typically done with a door position switch, which is either wired or wireless, and monitored centrally and remotely through a facility's access control system. Additionally, the "latchbolt" of the door can be monitored to see if the door is locked, in addition to being closed. Latchbolt monitoring, along with monitoring the door status (open/ closed), provides the most effective way to ensure exteriors door are both closed and secure from the outside.

© 2025 Partner Alliance for Safer Schools

F. **All Visitor Entry Exterior, Interior and Office Doors Secured With Remote Release and Audio/Video Door Entry System.** Secure visitor entrance(s) should have an audible and visual means to communicate and identify the visitor requesting access to the building. This could be as simple as a doorbell and staff being able to visually see the visitor outside the door. However, it is better to use of an audio/visual door entry system that provides both audio and video to a remote location. Most of these systems also allow for the remote release of the door.

G. **Electronic Access Control of Primary Entrances.** Exterior doors that are considered primary entrances should have electronic access control, both to limit the distribution of keys and to enhance the school's ability to control who can gain access to a specific building and when they can gain access. This access control also provides the ability for a school to audit who accessed a given opening and when. Required remote door release mechanisms should be by means of electric latch retraction for exit devices or electric locks.

TIER 2

A. **Electronic Access Control of Secondary Entrances.** Exterior doors that are considered secondary entrances should also have electronic access control, both to limit the distribution of keys and to enhance the school's ability to control who can gain access to a specific building and when they can gain access. This access control also provides the ability for a school to audit who accessed a given opening and when. Required remote door release mechanisms should be by means of electric latch retraction for exit devices or electric locks.

TIER 3

A. **Mobile Credentials for Emergency Responders.** When used with the door numbering system, mobile credentials can allow emergency responders instant access to the facility, and any openings equipped with access control provide the ability for responders to enter the building closest to the emergency event. In addition, mobile credentials provide for certain access rights for certain times and/or events as well as control when emergency responders are allowed into the building.

TIER 4

A. **Electronic Access Control of Tertiary Openings.** Exterior doors that are considered tertiary openings should be equipped with electronic access control so that these doors can be remotely unlocked and/or be locked/unlocked via the electronic access control.

© 2025 Partner Alliance for Safer Schools

VIDEO SURVEILLANCE COMPONENT:

Video surveillance is one component that can be used to mitigate risks at the building perimeter by providing surveillance, assessment, forensics and risk mitigation as defined in the district layer video surveillance portion of the PASS guidelines. Having a visual record of people entering and leaving, and the activities they engage in at entrances, will provide another layer of deterrence for unwanted activities; it may also provide valuable situational awareness during emergencies.

There are many different capability levels available in video surveillance equipment. Establishing an "operational requirement" for each camera deployed ensures the selection of equipment appropriate to the specific uses for which it is intended. These operational requirements are defined as allowing the human operator to do the following visually:

- **Detection** – The ability to determine whether a person or object is in the field of view of the camera
- **Observation** – The ability to differentiate and classify people and objects in the field of view of the camera (e.g., man or woman, child or adult, red or blue jacket, two cars and one truck)
- **Recognition** – The ability to identify an object with a higher degree of certainty, such as recognizing a familiar face or type of specific type of vehicle.
- **Identification** – The ability to identify specific individuals or objects where present in the field of view of the camera (e.g., John Smith, a 2009 Toyota Camry, a license plate number)

Each of these operational requirements are defined by the number of "pixels on target" recorded of the object or person in the field of view. For people, the number of pixels measured across the width of their face determines what operational requirement is achieved. While there are no established standards to define pixels on target to meet specific operational requirements, the following chart outlines generally accepted thresholds in the security industry.

Operational Requirement	Horizontal Pixels/Face	Pixels per Inch
Identification	80	13
Recognition	40	4
Observation	20	2
Detection	4	1

Unless otherwise stated or defined in a risk assessment, recognition and/or identification is the operational requirement for video surveillance of entrances at the building perimeter. See Figures 1 and 2.

© 2025 Partner Alliance for Safer Schools

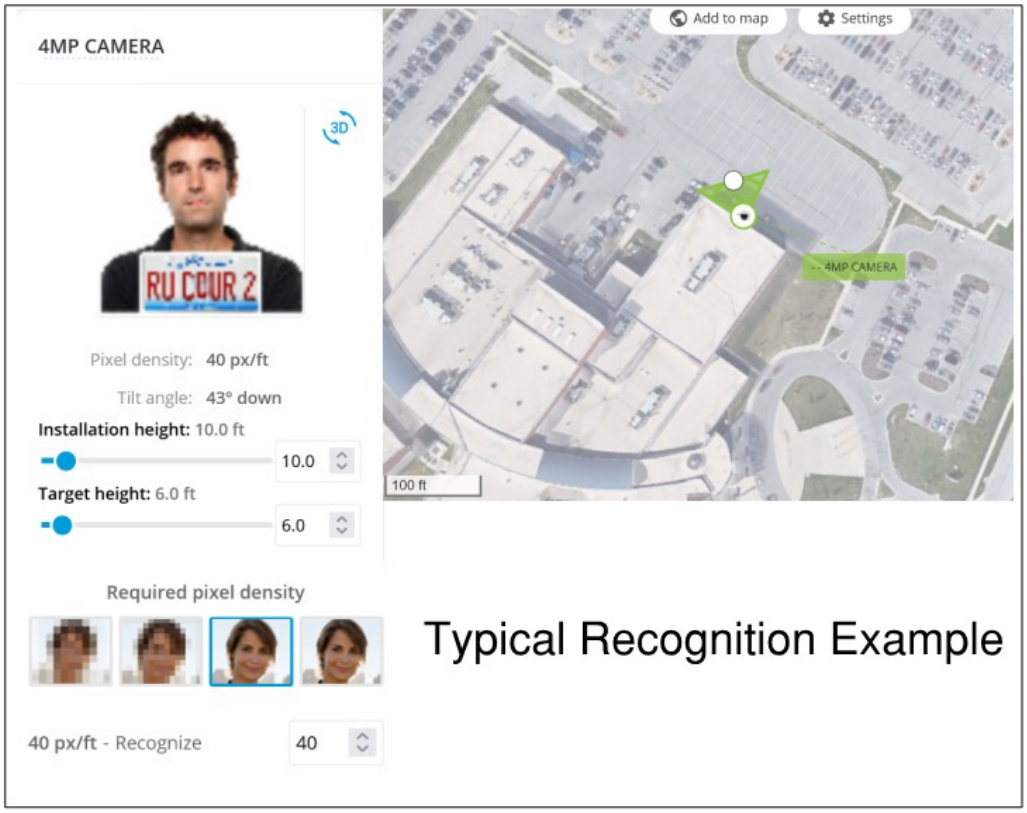


Figure 1.

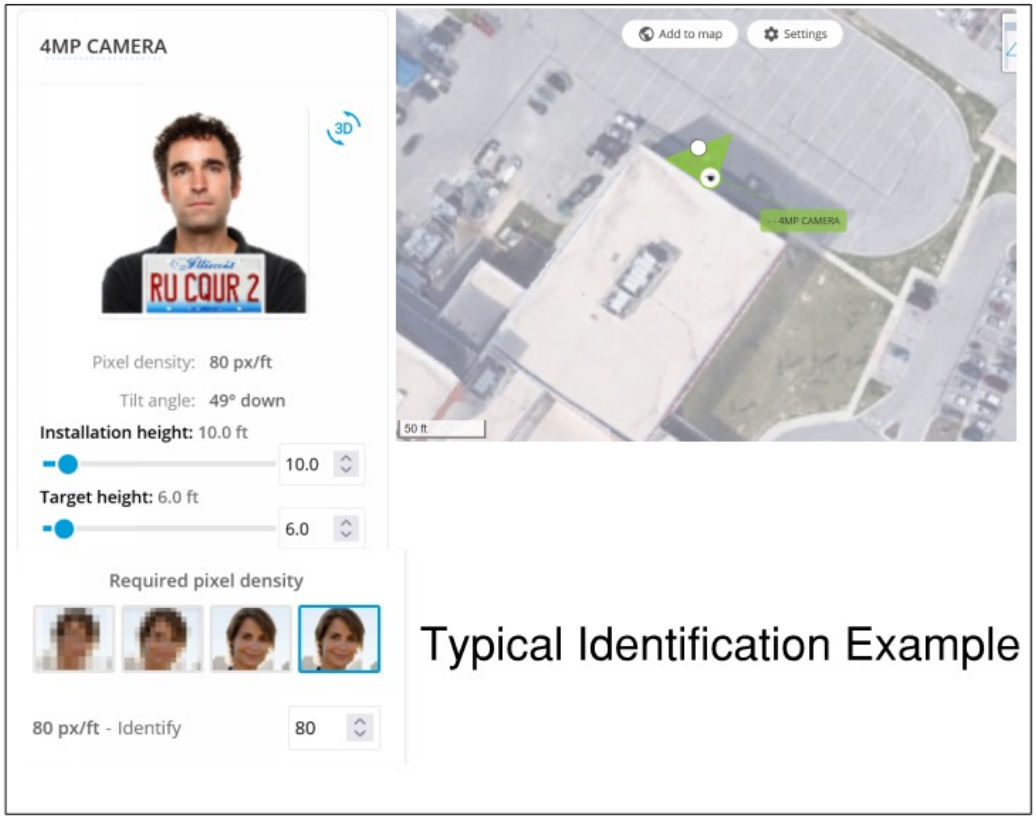


Figure 2.

© 2025 Partner Alliance for Safer Schools

TIER 1

A. **Video Intercom at Visitor Entrance Points.** A video intercom should always be used when there is no direct line of sight to the person that is screening incoming visitors. These devices enable schools to speak with and observe visitors at the main entrance and any other areas, such as loading docks, where people other than students, faculty and staff need to enter the building. The use of networked video intercoms is recommended, enabling screening from multiple devices such as a monitor in the front office or on mobile devices if needed. Networked video intercoms can also be recorded on the video management system, providing a visual record of activities at entrance points. The intercom should be integrated with an electronic access control system to enable screeners to unlock the door remotely, regardless of the monitoring device they are using. Some districts require visitors to display a valid photo ID before the door is remotely unlocked, providing visual audit logs of people entering buildings, which can be compared with data in visitor management systems.

B. **Exterior, Fixed Camera Coverage for All Primary Openings.** All video surveillance systems should provide a visual record of people entering the facility. Every exterior door should be included, even if it is always locked, since students or staff can easily open or prop doors from the inside to let someone enter the building, bypassing the requirement for screening at the main entrance.

   There are generally two methods for configuring the field of view from these cameras:

   1. Mount facing the door, thereby recording people entering the building
   2. Mount facing the hallway, thereby recording people leaving the building and recording who they are taking with, if applicable

It is preferable to mount cameras facing the door to record people entering the building to ensure schools have a visual record of someone entering (at a quality level allowing for identification), as the other cameras inside the building and outside the entrance, in many cases, can be used to determine if they were accompanied by someone else when leaving.

TIER 2

A. **Exterior, Fixed Camera Coverage at All Secondary, Tertiary and Service Openings.** Cameras should be mounted on the exterior wall of the school pointed towards all entry/exit points in a manner that provides the widest possible field of view of the area. In many cases, this will result in a profile view of the people existing in the building. Where possible, due to the layout of the exterior walls, the cameras may have a direct forward-facing field of view which would be the preferred placement. This field of view provides a visual record of people loitering at exits and provides recordings of people entering the facility through entry points other than the main entrance. In most cases, this also provides a broad overview of school property just outside of the school perimeter, supporting additional uses. Exterior cameras should be rated for outdoor use to prevent ingress of dust or water and environmentally rated to function in both upper and lower temperature ranges. Outdoor cameras should also include wide dynamic range sensors to ensure image usability.

© 2025 Partner Alliance for Safer Schools

DETECTION AND ALARMS COMPONENT:

TIER 1

A. **Intrusion Detection System on All Exterior Access Points.** If a school is not equipped with an access control system that can monitor whether each exterior door is open or closed, an intrusion detection system should be implemented that uses door position switches to monitor the status of doors.

B. **Intrusion Detection System Monitored 24/7.** As discussed in the district layer, every school building should have the intrusion system report to a central monitoring station; this allows for first responders to be made aware of a possible intrusion into the school building. The monitoring of the system should be via a hardwired telephone line, IP connection or cellular type dialer.

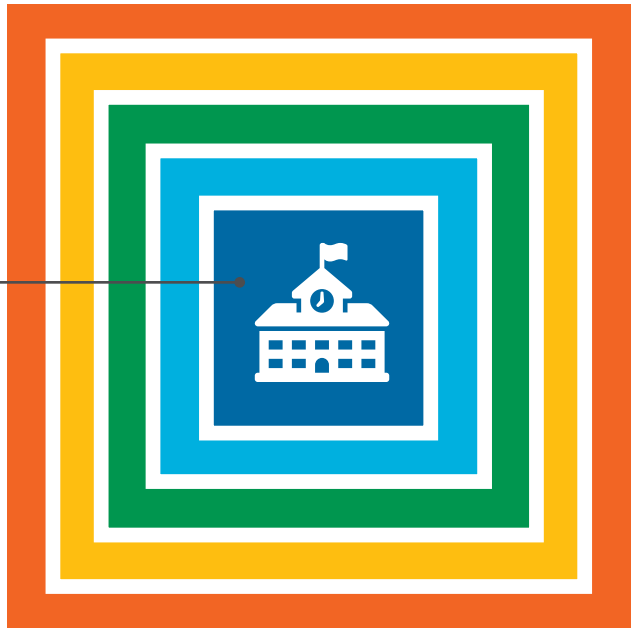
TIER 3

A. **Partitioned Intrusion Detection.** Intrusion systems also allow for the ability to secure interior portions of the building while some portions of the building are being used for other activities; this is called having "partitions" in the intrusion system. Through programming and design, the intrusion system can be set to have certain partitions armed while others are not.

   For example, a school is holding a basketball game in the gymnasium. While the gymnasium is being used by the public, the rest of the school should not be accessed. Intrusion system partitioning allows for the gymnasium to be used while sensors in other portions of the building will alarm to detect anyone who may enter unauthorized areas. This is an important aspect to intrusion for not just unauthorized entry, but also for other unique risks that schools face. Some examples are gang activity, bullying and illicit drug use. A properly installed intrusion system can help manage and deter threats to unoccupied buildings as well as when the building is occupied.

© 2025 Partner Alliance for Safer Schools

CLASSROOM/INTERIOR LAYER



» QUICKFIND

Classroom Interior Layer Checklist.....113
Policies And Procedures Component 115
People (Roles And Training) Component.....116
Architectural Component.....116
Communication Component 120
Access Control Component.....123
Video Surveillance Component.....127
Detection And Alarms Component 131

© 2025 Partner Alliance for Safer Schools

CLASSROOM INTERIOR LAYER	TIER 1	TIER 2	TIER 3	TIER 4
POLICIES AND PROCEDURES				
» Classroom Doors Closed and Locked When Occupied	✔	✔	✔	✔
» Designate Shelter Areas Outside Corridor Line of Sight	✔	✔	✔	✔
PEOPLE (ROLES AND TRAINING)				
» Teachers, Staff & Substitutes Trained on Emergency Protocols	✔	✔	✔	✔
ARCHITECTURAL				
» Door Construction (New Construction/Renovation)	✔	✔	✔	✔
» Security Film on Door Vision Panels and SideLites	✔	✔	✔	✔
» Narrow-Lite Style Doors With Blinds	✔	✔	✔	✔
» Compartmentalized Building (Cross-Corridor Doors)	✔	✔	✔	✔
» Safety/Security Optimization of Classroom Door Installation (New Construction)	✔	✔	✔	✔
» Door Construction (New Construction/Renovation)		✔	✔	✔
» Reinforced Walls at Shelter Areas		✔	✔	✔
» Reduced Concentration of People in Cafeterias and Open Environment Collaboration Spaces				✔
» Reinforced Classroom/Corridor Walls (New Construction)				✔
SECURITY GLAZING				
» Interior Building Separation Doors/Windows	✔	✔	✔	✔
» Interior Doors/Windows at Mass Congregate Areas	✔	✔	✔	✔
» Classrooms Doors and SideLites	✔	✔	✔	✔
» Administrative Office Doors and SideLites	✔	✔	✔	✔
COMMUNICATION				
» Public Address System With 2-Way Intercom	✔	✔	✔	✔
» E-911 Added to Phone System (No Codes)	✔	✔	✔	✔
» Local Area Two-Way Radio System for Local Staff		✔	✔	✔
» E-911 Provides Specific Phone Location		✔	✔	✔
» Audio-Visual Public Address System		✔	✔	✔
» Communication of Emergency Announcements		✔	✔	✔
» Local Area Two-Way radio System for All Staff, Including Teachers		✔	✔	✔
» BDA/DAS System			✔	✔
» Mass Notification Tied to District-Wide System			✔	✔
» AVPA Communication via Outside Calls (With Record Call Options)				✔
» Use of Mobile Applications and Social Media				✔
ACCESS CONTROL				
» Classroom and Shelter-in-Place Doors Lockable From Inside	✔	✔	✔	✔
» Classroom Doors Closed and Locked When Occupied	✔	✔	✔	✔
» Locks with Visual Indicator		✔	✔	✔
» Stand-Alone Electronic Locks with Fob			✔	✔
» Networked Electronic Locks				✔

© 2025 Partner Alliance for Safer Schools

	TIER 1	TIER 2	TIER 3	TIER 4
CLASSROOM INTERIOR LAYER				
VIDEO SURVEILLANCE				
» Fixed Camera Coverage of Primary Openings	✔	✔	✔	✔
» Fixed Camera Coverage of All Common and Known Problem Areas	✔	✔	✔	✔
» Fixed Camera Coverage of Stairwells, Hallways and Restroom Entrances		✔	✔	✔
» Fixed Camera Coverage of Restricted Areas		✔	✔	✔
» Fixed Camera Coverage of Classrooms			✔	✔
» Classroom Cameras with Audio Recording				✔
DETECTION AND ALARMS				
» Panic Alarm System in Each Building	✔	✔	✔	✔
» Panic Alarm System in Each Classroom	✔	✔	✔	✔
» Panic Alarm System With Wearable Device		✔	✔	✔
» Intrusion Detection System Covering All Hallways and Public Areas		✔	✔	✔
» Unification of Fire Alarm and Panic Alarm Systems		✔	✔	✔
» Unification of Panic Alarm Systems And Access Control System		✔	✔	✔
» Unification of Panic Alarm Systems with Video Surveillance System		✔	✔	✔
» Unification of Panic Alarm Systems and Communication Systems		✔	✔	✔
» Unified Communication and Detection System Monitored 24/7		✔	✔	✔
» Unified Communication and Detection System Monitored by District-Wide SOC		✔	✔	✔
» Unification of Alarms, Communications, Video Surveillance and Access Control Systems		✔	✔	✔
» Panic Alarm System with Wearable Devices to All Staff			✔	✔
» Intrusion Detection System Covering All Classrooms			✔	✔

© 2025 Partner Alliance for Safer Schools

The most important assets to protect in a classroom (and on school grounds, for that matter) are students, staff, faculty and visitors. The security components within outer layers detailed in this guide also serve to protect classrooms and other interior areas of a school facility. These best practices relate to securing the classroom and shelter doors against active threats, unauthorized visitors and criminals. Shelter doors include areas of the building other than classrooms where building occupants could "shelter in place" during an emergency. These openings include gymnasiums, cafeterias, libraries, media centers, offices, teacher's lounges and auditoriums.

POLICIES AND PROCEDURES COMPONENT:

TIER 1

A. **Classroom Doors Closed and Locked When Occupied.** Classroom doors should be closed and locked when classes are in session or the rooms are otherwise occupied. Schools should work with first responders, local law enforcement and EMS to coordinate how access is gained to classrooms under the various TIER levels listed below.

B. **Designate Shelter Areas Outside Corridor Line of Sight.** Each classroom should have a pre-identified area in which the occupants could shelter out of the line of sight from the entry door during an emergency (Figures A and B). This could be a nook in the room layout or simply a "hard corner." This location in each classroom should be clearly identified to both staff and students using the classroom.

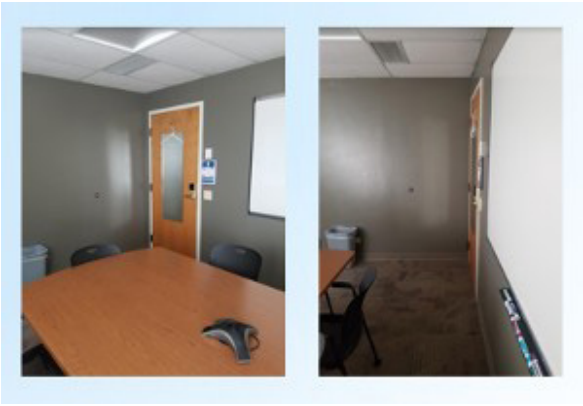


Figure A. View from Room Center View from "Hard Corner"

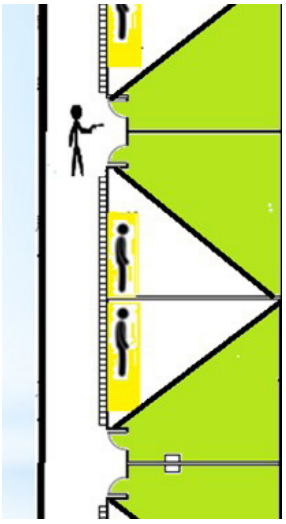


Figure B. Green Areas Viewable Through Door Vision Panel

© 2025 Partner Alliance for Safer Schools

PEOPLE (ROLES AND TRAINING) COMPONENT:

TIER 1

A. **Teachers, Staff and Substitutes Trained on Emergency Protocols.** Teachers and supervising staff have several important responsibilities before and during an emergency. Students will count on teachers and supervising staff to provide direction. The actions of teachers and supervising staff are integral to successful response in an emergency. Teachers must follow the directives of the site administrator/principal or their designee but also be able to act on their own in an emergency when direction is not available (see Policies and Procedures in the District-Wide Layer).

ARCHITECTURAL COMPONENT:

Architectural planning and design are key components in the security and safety of building occupants. Functional spaces, their shelter in place locations, and egress paths can enhance safety through effectively deterring and delaying adversarial behaviors.

Planning decisions made by a project team during the conceptual phase – where general building organization, circulation paths, compartmentalization options, and building egress locations are determined – influence the effectiveness of both life-safety and construction cost. During this phase of work, it is advantageous to assess all conceptual plan options from this perspective. This is also the best time to have the school dstrict's security team review planning options and life-safety strategies. Areas of focus may include the following:

- **Compartmentalization**: Reduce an intruder's access to a limited area of the school by means of strategically placed doorways in corridors (Figure C). In those locations, doors are held open via electromagnetic devices in normal conditions, which can then be released to automatically close and lock when a lock-down alarm is activated.

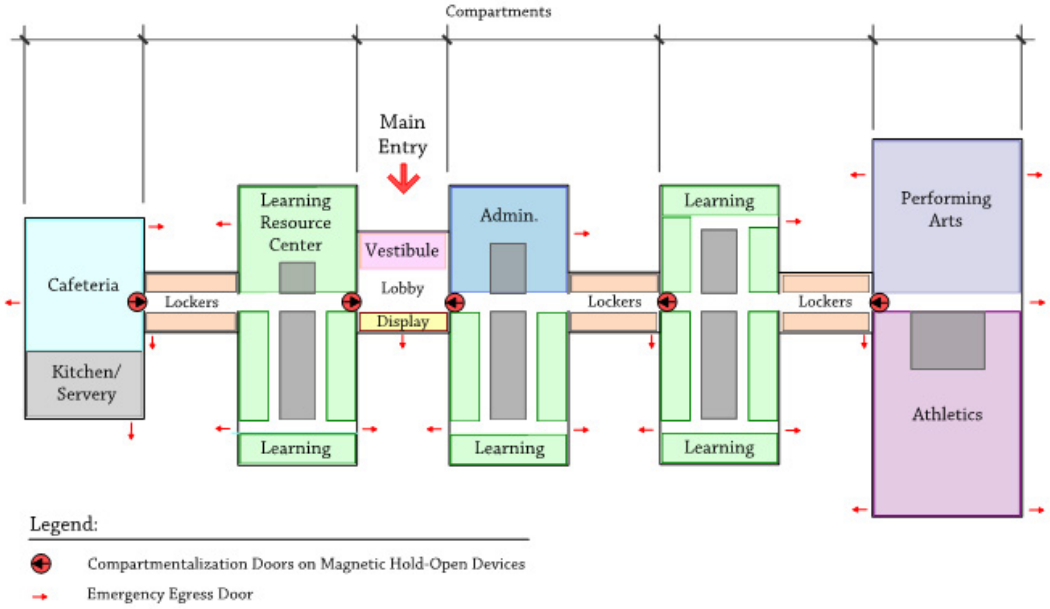


Figure C. Compartmentalization Diagram

© 2025 Partner Alliance for Safer Schools

Doors are then only accessible from the push side and locked on the pull side. In a compartmentalized approach, each compartment will require its own separate means of egress.

- **Efficiency of Egress from Areas of Assembly:** Egress efficiency from places where people gather – gymnasiums, cafeterias, libraries, and auditoriums – benefits from direct access to the outdoors from multiple locations within the space. Isolating these functions to a degree will result in greater perimeter wall exposure, i.e., a perimeter wall on three sides of an assembly function in lieu of one will allow for more exterior egress door locations, hence a potential for more rapid and efficient evacuation during a threatening event.
- **Corridor Geometry** – Straight vs. Curved, (or segmented): While straight corridors provide clear lines of sight for surveillance, faster evacuation, and easier security response they increase vulnerability due to a clear line of sight for a greater distance, and often lack natural barriers leaving fewer places for people to shield themselves from a threat. Curved, (or segmented) corridors reduce the line of sight for assailants and provide inherent natural cover; however, they pose obstructed views for security and may slow the process of evacuation in emergency conditions. These tradeoffs need to be considered in selection.

TIER 1

A. **Door Construction (New Construction/Renovation).** Classroom/Corridor doors should be a minimum of 1 ¾" thick heavy duty (16 ga.), steel or solid core wood doors installed in steel frame.

B. **Security Film on Door Vision Panels and Sidelites.** Security window film should be installed on all classroom and shelter in place/lockdown room door vision panels[1] and sidelites.[2] Security film serves to deter or delay the ability of an attacker to breach a doorway using a firearm or other tool/weapon, in addition to limiting injuries from glass shards resulting from a blast. This type of solution can be retrofitted within most commercial window systems and incorporated into insulating glass units. Installation is typically performed by an authorized installer, and they must follow the manufacturer's recommended procedures in order for these products to be effective.

C. **"Narrow-Lite" Style Classroom Doors with Blinds.** Classroom doors should include windows (narrow-lite style) for visual access both inside and outside the classroom (See Figure D below). Blinds should be integrated into the design to cover these windows during a lockdown.

D. **Compartmentalize Building with Cross-Corridor Doors.** Interior cross-corridor doors should be used to confine an emergency event to a limited area of the building. These doors should normally be held open with electromagnetic devices that resist tampering and release upon activation of the lockdown process. Cross-corridor doors should be

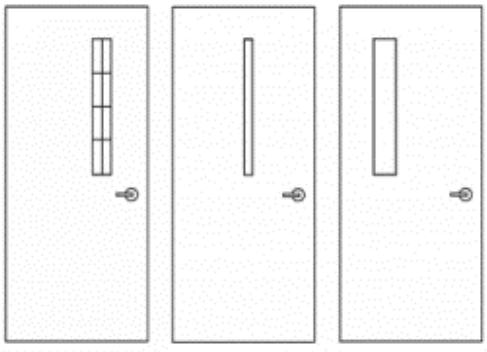


Figure D: Common narrow-lite style classroom doors

1 Door vision panels are windows incorporated into a door.
2 Sidelites are narrow windows immediately adjacent to a doorway.

© 2025 Partner Alliance for Safer Schools

equipped with exit-only panic hardware and either a cylinder to manually gain access with a key or integration with an electronic access control system to electronically gain access.

E. **Safety/Security Optimization of Classroom Door Installation (New Construction).** Where budgets prohibit the width of corridors of a dimension allowing the minimum width of egress required by code without encroachment by outswing doors, an alcove will need to be provided. In most instances the walls adjacent to classroom doors should be angled or beveled, (as opposed to 90-degree corners) to form an alcove of a depth not greater than that required to maintain minimum clear width; this permits better sight and surveillance by public safety personnel. This will both 1) provide visual access that minimizes hiding nooks and 2) allow classroom doors to swing open toward the corridor for easy exit without diminishing the required egress width in the corridor.

TIER 2

A. **Door Construction (New Construction/Renovation).** Classroom doors should be a minimum of 1 ¾" thick heavy-duty steel or attack resistant wood doors installed in steel frame.

B. **Reinforced Walls at Shelter in Place Areas (New Construction):** Corridor/Classroom walls should be of masonry construction extending from floor to underside of structure or roof deck. Use 6-inch nominal concrete masonry units (CMU) minimum in non-load-bearing conditions, or as dictated by height of wall and/or structural engineer's recommendations.

TIER 4

A. **Reduced Concentration of People in Cafeterias and Open Environment Collaboration Spaces:** Plan these functions in ways that distribute the occupants in a set of smaller zones as opposed to one large common area. In a cafeteria, this can be accomplished with a quasi 'food court' approach with de-centralized seating.

B. **Reinforced Classroom/Corridor Walls - (New Construction):** Classroom/corridor walls should be of masonry construction extending from floor to underside of structure or roof deck. Use 8-inch nominal concrete masonry units (CMU) fully grouted, 6" poured concrete or ballistic rated fiber panels.

SECURITY GLAZING:

TIER 1

A. **Interior Building Separation Doors/Windows:** Doors and or windows that separate the interior of the building areas should be rated to ASTM-F3561 Level 1 (or equivalent).

B. **Interior Doors/Windows at Mass Congregate Areas:** Doors and windows at mass congregation areas should be Safety Laminated, with a primary focus on getting staff and students safely out of these spaces.

© 2025 Partner Alliance for Safer Schools

C. **Classrooms Doors and Sidelites:** Classroom doors and sidelites should be rated to ASTM-F3561 Level 1 (or equivalent).

D. **Administrative Office Doors and Sidelites:** Doors and sidelites for administrative office areas should be Safety Laminated, unless accessible directly from a corridor, then they should be rated to ASTM-F3561 Level 1 (or equivalent).

TIER 2

A. **Interior Building Separation Doors/Windows:** Doors and or windows that separate the interior of the building areas should be rated to ASTM-F3561 Level 3 (or equivalent).

B. **Interior Doors/Windows at Mass Congregate Areas:** Doors and windows at mass congregation areas should be rated to ASTM-F3561 Level 1 (or equivalent).
Safety Laminated, with a primary focus on getting staff and students safely out of these spaces.

C. **Classrooms Doors and Sidelites:** Classroom doors and sidelites should be rated to ASTM-F3561 Level 3 (or equivalent).

D. **Administrative Office Doors and Sidelites:** Doors and sidelites for administrative office areas should be rated to ASTM-F3561 Level 1 (or equivalent).

TIER 3

A. **Interior Building Separation Doors/Windows:** Doors and or windows that separate the interior of the building areas should be rated to ASTM-F3561 Level 5 (or equivalent).

B. **Interior Doors/Windows at Mass Congregate Areas:** Doors and windows at mass congregation areas should be rated to ASTM-F3561 Level 3 (or equivalent).

C. **Classrooms Doors and Sidelites**: Classroom doors and sidelites should be rated to ASTM-F3561 Level 5 (or equivalent). Consideration should be given to ballistic ratings in high-risk areas.

D. **Administrative Office Doors and Sidelites:** Doors and sidelites for administrative office areas should be rated to ASTM-F3561 Level 3 (or equivalent).

TIER 4

A. **Interior Building Separation Doors/Windows:** Doors and or windows that separate the interior of the building areas should be rated to both UL572 Level 7 (or equivalent) and ASTM-F3561 Level 5 (or equivalent).

B. **Interior Doors/Windows at Mass Congregate Areas:** Doors and windows at mass congregation areas should be rated to ASTM-F3561 Level 3 (or equivalent).

C. **Classrooms Doors and Sidelites:** Classroom doors and sidelites should be rated to both UL572 Level 3 (or equivalent) and ASTM-F3561 Level 5 (or equivalent).

© 2025 Partner Alliance for Safer Schools

D. **Administrative Office Doors and Sidelites:** Doors and sidelites for administrative office areas should be rated to ASTM-F3561 Level 5 (or equivalent). Consideration should be given to ballistic ratings in high-risk areas.

COMMUNICATION COMPONENT:

TIER 1

A. **Public Address with Two-Way Intercom System.** At minimum, the building should have a public address system that can deliver emergency communications audibly and intelligibly to all areas of the building. All areas include but not limited to the following:

- All instructional areas (classrooms)
- Hallways
- Administration areas
- Staff areas such as break rooms and workrooms
- Restrooms
- Public areas including but not limited to:
  - » Common areas
  - » Collaborative areas
  - » Library/media center
  - » Auditorium/performing arts area
  - » Gymnasium/weight-training rooms
  - » Cafeteria including kitchen

If a school has an older fire system that only has horns and not a voice-capable system, the horns can be used to create a different tone cadence to notify for a weather or active safety threat in a very similar manner as a fire alarm. It is recommended that public address systems be implemented in compliance with NFPA 72 Chapter 24 (see In-Building Emergency Communications System).

The two-way intercom system shall provide two-way communication between all learning spaces and work areas to central locations. The call-in button should have a normal (day-to-day communication) and an emergency call indication. It is extremely important that the that individuals within the learning spaces and work areas can easily identify whether the call is an emergency or not.

B. **E-911 Added to Phone System (No Codes).** Many enterprise phone systems require a code or number to be dialed before receiving a phone line to dial outside the facility. All phone systems should be set up so that no code or additional prefix number needs to be dialed for a 911 call.[3] This "E-911" feature ensures that anyone from any phone can dial 911 without any other actions.

C. **Local Area Two-Way Radio System for Select Staff.** A local area network radio system allows reliable voice communications between select staff on campus during an emergency in addition to day-to-day local school communications. At minimum, radios should be provided to key administrative staff, the front office and staff supervising

3 Relevant standards include National Electrical Manufacturers Association SB-40, Communications Systems for Life Safety in Schools.

© 2025 Partner Alliance for Safer Schools

the playground or other outdoor activities.4 Commercial radio systems should be used rather than off-the-shelf consumer products or radios designed for recreational use. As noted in the district-wide layer, public schools as government entities must use radio systems licensed under the FCC Universal Licensing System.[5]

TIER 2

A. **E-911 Provides Specific Phone Location.** The phone system should have the ability to provide the location of the device that calls 911 to the 911 call center.

B. **Audio-Visual Public Address System (AVPA):** Audio-visual public-address systems include both intelligible audio and a visual component. NFPA defines AVPA as emergency communication systems (ECS). AVPA provide means of dual notification for those who might be sight or hearing impaired. The visual aspect of the system should have the capability of multiple colors to define specific threats. For example, red is for fire, blue for emergencies, etc.

   Schools/districts need to be aware of the ADA requirements for visual notification. There are specific types of strobes and strobes synchronize in order to prevent inducing physical harm to students and staff. In addition, ADA has some requirements on where visual notification should be installed.

   Schools/districts should investigate possible interfaces to audio-visual resources that are already in use for education. For example, many televisions and messaging boards have the ability to be used for emergency messages.

C. **Communication of Emergency Announcements:** The emergency communication system (whether through the public address system, mass notification system (fire alarm); must provide an override of any audible announcements for emergency announcements. In addition, the emergency message should have a distinct tone. It is recommended to use the process of creating emergency priorities to override and send emergency messages in accordance with NFPA 1660.

D. **Local Area Two-Way Radio System for All Staff, Including Teachers.** A local area network radio system allows reliable voice communications between all staff on campus during an emergency in addition to day-to-day local school communications. As noted, commercial radio systems should be used rather than off-the-shelf consumer products or radios designed for recreational use.

TIER 3

A. **BDA/DAS System.** Signal boosters may be required to ensure reliable campus two-way radio communications and first responder radio coverage in stairwells, hallways and other common areas where signals can be interrupted by building materials, dead spots and signal interference (see BDA/DAS explanation in the District-Wide Layer). These technologies can incorporate boosters for two-way radios and cellular and are typically custom designed for each unique environment.

4 "The principal, vice principal, front office staff, playground supervisors, bus drivers, lunch duty staff, crossing guards and SROs should have these devices," DHS Primer to Design Safe School Projects, https://www.dhs.gov/xlibrary/assets/st/bips07_428_schools.pdf

5 For license example, see http://wireless2.fcc.gov/UlsApp/ApplicationSearch/applMain.jsp?applID=9075468.

© 2025 Partner Alliance for Safer Schools

B. **Mass Notification Tied to District-Wide System.** As described within other layers, the AVPA communication system should be integrated with the district-wide mass notification system. Within this integration, the school can receive instant alerts for weather and other emergencies that can affect the school.

There are a variety of technologies to interface the in-building communication systems to wide-area systems. Some of the ways to unify the systems are as follows:

- Hardwired Audio Connections: This is a physical connection between the wide area notification system to the in-building communication system, like a hardwired microphone that is connected to the in-building system.
- Voice over IP (VoIP) Connection: A VoIP connection allows audio transmission across a district's IT network. This connection can be made through a variety of technologies that include:
  - » A VoIP phone system
  - » Handheld radio to IP systems
  - » Radio frequency to analog conversion systems

Since wide area communications systems are intended to share emergency communications across a large area such as a municipality, county or state, some states have adopted specific technologies or platforms to be used for such communications. For this reason, schools should work with local and state law enforcement to see what standards are in place before unifying communications technologies.

TIER 4

A. **AVPA Communication via Outside Calls (With Record Call Option).** During an emergency, it may become necessary for a first responder outside of the school to provide critical information to the staff and students inside the school. Two-way intercom systems can be configured to allow an outside call to trigger a mechanism to communicate a building-wide emergency message, allowing first responders to communicate to persons inside the building when they are incapable of reaching the main office or other area inside the school from which building-wide messages could otherwise be transmitted.

It is critically important for a system to record and log messages that are being announced during the emergency for review after the emergency event has ended. Every emergency event is an opportunity to learn how to better strengthen processes, procedures and technology to mitigate danger.

B. **Use of Mobile Applications and Social Media.** Emergency communications are most effective when they can be transmitted across multiple channels; however, it's important to ensure the most effective mechanisms receive the highest implementation priority.

One well-known study[6] found that people best responded to communication in the following order:

- Phone call from a known person
- Live voice communication through a public address system

6 "Organizational Communication in Emergencies: Using Multiple Channels and Sources to Combat Noise and Capture Attention," Stephens, Keri K. April 2013, eric.ed.gov/?id=EJ1004715

© 2025 Partner Alliance for Safer Schools

- Social media notification
- Text message notification

This data supports the conclusion of many life safety experts that the most efficient way to provide information in an emergency is through one-way live voice (and visual) communication systems; however, there are other communications mechanisms that can be very effective and offer certain advantages depending on the type of threat. Using multiple emergency communications methods supports an all-hazards approach to safety and security.

Mobile Applications: There are many applications that can be installed on mobile devices for staff and students to both alert the school or district to an emergency and receive emergency communications. Some applications can send video recordings and/or streaming in real time, while others can provide an alert that instantly notifies key personnel that a threat is in process. Some can even provide the location of the device via GPS. Administrators should ensure mobile applications are used in a strategic manner that conforms to the policies and procedures the school and/or district have in place.

Some considerations for evaluating mobile applications include:

- Does the application support emergency communication for all building occupants?
- What is the policy for mobile device use in the school? Mobile applications may be unable to provide timely to staff and students if mobile devices are not allowed to be used during class time.
- Is the cellular and/or wireless network capable of sending emergency notifications to hundreds or thousands of devices at one time?

Social Media: Nearly all schools and districts already have X (formerly Twitter) and/or Facebook accounts for the district, schools and school activities; however, each school should also have a social media account that is specific to emergency situations. This feed will allow the school and/or district to send information out to not only the students and staff, but also to parents and the surrounding community. A separate account for emergencies can assist in differentiating normal day-to-day postings from urgent information about emergency events.

ACCESS CONTROL COMPONENT:

Whether mechanical or electronic locks are installed at classroom, shelter-in-place and other interior openings, interior doors should comply with appropriate locally enforced building codes for new educational occupancies, existing educational occupancies, new day care occupancies, existing day care occupancies, new business occupancies, existing business occupancies and the ADA. School administrators should work with local life safety experts to determine code compliance related to securing classroom/interior doors.

While many types of mechanical and electronic locks are available, certain functionality is essential for classroom doors (and other shelter-in-place doors) from a safety and security standpoint.

© 2025 Partner Alliance for Safer Schools

A. Classroom locks should be specifically designed for classroom doors and lockable from the inside of the room.[7]

B. Any lock must allow keyed or electronic access from the corridor side for access by authorized personnel without a special tool or knowledge.[8]

C. Any lock shall always allow free egress from the inside of the room.[9]

D. Locks should ideally have a visual indicator so that the condition of the lock (locked or unlocked) is visible to room occupants.

Some manufacturers offer code-compliant conversion or retrofit kits which are capable of converting existing locks to comply with the above criteria.

TIER 1

A. Classroom and Shelter-in-Place Doors Lockable From the Inside: Classroom and shelter-in-place doors must have the ability to be locked from the inside by all occupants and should be keyed or otherwise accessible on the corridor side for quick access by authorized personnel. Classroom doors must have one single motion to open the door for egress. This is critical as many classroom doors in use today do not meet these criteria. As schools modernize their facilities, they should also place emphasis on clarifying human roles and communicating processes to staff that are essential to effective use of the hardware that is chosen.

PASS recommends that such doors be capable of being locked from the inside by all occupants without use of an additional device such as a key. Under extreme stress, duress or high anxiety , people tend to lose fine motor skills and dexterity needed to use them effectively.[10]

Additional devices affixed or temporarily affixed to the door, such as "barricade" or "secondary locking" devices, offer NO advantage over an existing code-compliant lock. These devices can increase liability and risk and most violate fire and life safety codes as well as the federal law – ADA. For further information see 5 Reasons Schools Should Avoid Classroom Barricade Devices[11] and the PASS Whitepaper on Classroom Barricade Devices.[12]

B. Classroom Doors Closed and Locked When Occupied. Classroom doors should be closed and locked when classes are in session or the rooms are otherwise occupied. Schools should ensure first responders, local law enforcement and EMS can access locked classrooms.

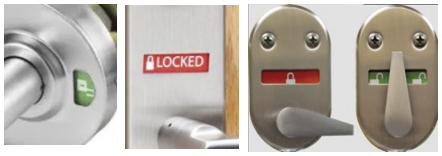
7 See IBC 2021 Edition, Section 1010.2.8 & NFPA 101, 2022 Edition, Section 15.2.2.2.4.
8 See IBC 2021 Edition, Section 1010.2.8 & NFPA 101, 2022 Edition, Section 15.2.2.2.4.
9 Free egress generally means the door can be opened from the inside with a single motion and without the use of a key, special knowledge or effort. See IBC 2021, Edition, Section 1010.2.8 & NFPA 101 2022 Edition, Section 15.2.2.2.4.
10 https://icisf.org/impact-of-the-tach-psych-effect-while-under-stress-duress-or-heightened-anxiety/
11 https://passk12.org/wp-content/uploads/2019/09/5-Reasons-Schools-Should-Avoid-Classroom-Barricade-Devices-PASSK12.pdf
12 https://passk12.org/wp-content/uploads/2019/04/PASS-WHITEPAPER-Classroom-Barricades-2019-04-10.pdf

© 2025 Partner Alliance for Safer Schools

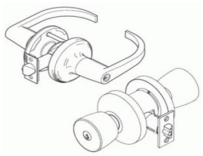
K-12 Interior Door Lock Types And Functions

1. **All code compliant models feature single motion exiting from interior at all times, regardless of locking status of exterior.**
2. All mechanical locks feature an exterior keyed cylinder for entry
3. Most electronic locks include a mechanical key override
4. **Category 2-5 locks should include a door visual indicator on the inside**

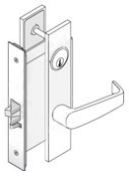
Examples of Indicators

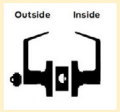
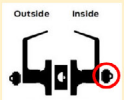
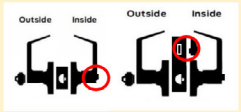


Bored Locks (Lever & Knob)

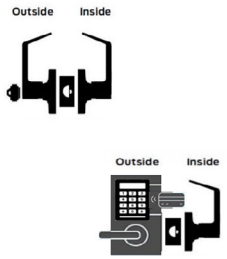


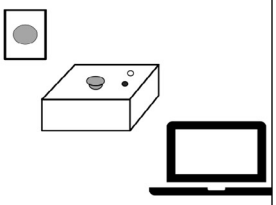
Mortise Locks



Groups	Description	Category 1	Category 2	Category 3	Category 4	Category 5
A	**Traditional Classroom Locksets (Unlocked in the morning, Locked At End Of Day)**	**Blank Inside** 	**Inside Cylinder** 	**Inside Activator** 	**Electronic Hybrid 1** 	**Electronic Hybrid 2** 
	Lock/Unlock Method	**Key**	**Key**	**Key**	**Key, Card or Keypad**	**Key, Card or Keypad**
	Lock Initiation	No interior capability Locks exterior lever	Key on inside Locks exterior lever	Inside turnpiece or button Locks exterior lever, deadbolt projected on some models	Remote - No other inside method Locks exterior lever	Remote or Interior lock control Locks exterior lever, deadbolt projected on some models
	Forced Entry Protection	Latch	Latch	Generally a latch, some models with a deadbolt	Latch	Generally a latch, some models with a deadbolt
	Major Benefit		Teacher can lock the door without entering hallway	Anyone in room can lock the door quickly	Remote lock/unlock of door is possible	Remote lock/unlock of door possible and anyone in the room can quickly lock the door
	Lock Initiation Discussion Points	1. Only person with key can lock the door 2. Key holder must enter hallway to lock door	1. Only person with key can lock door from inside or outside	1. Anyone in room can lock door from the inside	If teacher (or protocol) is to keep door unlocked during the day, door can be locked remotely (see concerns below)	Same as Type 4, but with inside activation button
	Areas of concern & discussion	1. Exposure to harm when entering hallway 2. Length of time to initiate lockdown procedures 3. Possibility that key may not be accessible 4. Room cannot be locked down if teacher is not in the room 5. Effect of stress on fine motor skills 6. No locking bolt	1. Length of time to initiate lockdown procedures 2. Possibility that key may not be accessible 3. Effect of stress on fine motor skills 4. Room cannot be locked down if teacher is not in the room 5. Confusion regarding which way to turn the key on locks without indicators 6. No locking bolt on most models 7. Cylindrical locks never have a locking bolt	1. Kids or an assailant may lock the door, restricting entry to anyone with a key 2. No locking bolt on most models 3. Cylindrical locks require an additional integrated auxiliary lock to have a locking bolt	1. Complexity of operation 2. Offers a variety of credential lockout options 3. Same Concerns 2-6 of Catagory 1	Same Concerns as Catagory 3 & 4

© 2025 Partner Alliance for Safer Schools

B	Always Locked on Hall Side (No Free Entry)	Mechanical	Card Access	Keypad	
	Entry Method Options	Key	Key or Card	Key or code	
	Lock Initiation	Not required, exterior lever always locked	Not required, exterior lever always locked	Not required, exterior lever always locked	
	Forced Entry Protection	Latch	Latch	Latch	
	Major Benefit	Door is always locked	Door is always locked	Door is always locked	
	Areas of concern & discussion	1. Teacher needs to respond and go to door to allow entry 2. Teachers will prop door open to avoid having to continuously GC respond to entry requests 3. Classroom exiting restricted by teachers to minimize having to open the door 4. No locking bolt	1. Teacher needs to respond and go to door to allow entry 2. Teachers will prop door open to avoid having to continuously respond to entry requests 3. Classroom exiting restricted by teachers to minimize having to open the door 4. Software, programming to maintain system 5. No locking bolt on most models	1. Teacher needs to respond and go to door to allow entry 2. Teachers will prop door open to avoid having to continuously respond to entry requests 3. Classroom exiting restricted by teachers to minimize having to open the door 4. Software, programming to maintain system 5. Code can be observed by students and used for entry 6. No locking bolt on most models	

C	Electric Locking of Type A (Traditional Classroom)	Emergency locking station in room	Remote locking from central location (office)	External locking from (Central station, Police, etc.)	
	Entry Method Options	1. Pendant transmitter 2. Wall-mounted activation	1. Wired or wireless signal and control	1. Different systems	
	Major Benefit	Can Lock door and/or initiate a lockdown without approaching the door	Can Lock door and/or initiate a lockdown from a remote location	Can Lock door and/or initiate a lockdown from a remote location	
	Areas of concern & discussion	1. Transmitter: Same as key- only one person can initiate 2. Wall station: Same as inside turnpiece 3. No locking bolt	1. Notification required to initiate 2. Same issues as key - no way to initiate from within room 3. Potential to lock assailant in room 4. Requires communication to be effective 5. No locking bolt on most models	1. Same as central location 2. Requires infrastructure 3. No locking bolt on most models	

TIER 2

A. **Locks With Visual Indicator**. Classroom locks that provide a visual indicator allow the condition of the lock (locked or unlocked) to be visible to staff and room occupants, without them having to exit the room to check.

TIER 3

A. **Stand-Alone Electronic Locks With Fob.** In electronic systems, doors should be equipped with a stand-alone electronic door lock that can be locked wirelessly from a fob or other device from anywhere in the classroom. Electronic stand-alone locks can be locked remotely with a fob or other electronic actuator, generally from up to 75 feet away. This should include a visual indicator and provide keyed or credential access on the corridor side for quick access by authorized personnel.

TIER 4

A. **Networked Electronic Locks**. In networked systems, doors are equipped with electronic locking systems that can be initiated both remotely from a central location or by a teacher in the classroom and tied into the school security system. Networked locks should also include a visual indicator. Some locks have the ability to be programmed to send a signal to a command center and/or lock down a pre-programmed section of the building if actuated locally.

© 2025 Partner Alliance for Safer Schools

VIDEO SURVEILLANCE COMPONENT:

Video surveillance can be used to mitigate risks for the classroom and interior perimeter by providing surveillance, assessment, forensics and risk mitigation as defined in the district-wide layer in the guidelines. Having a visual record of student, staff, faculty and visitor activity throughout the day provides another layer of deterrence for unwanted activities; it may also provide valuable situational awareness during emergencies.

There are many different capability levels available in video surveillance equipment. Establishing an "operational requirement" for each camera deployed ensures the selection of equipment appropriate to the specific uses for which it is intended. These operational requirements are defined as allowing the human operator to do the following visually:

- **Detection** – The ability to determine whether a person or object is in the field of view of the camera
- **Observation** – The ability to differentiate and classify people and objects in the field of view of the camera (e.g., man or woman, child or adult, red or blue jacket, two cars and one truck)
- **Recognition** – The ability to identify an object with a higher degree of certainty, such as recognizing a familiar face or type of specific type of vehicle.
- **Identification** – The ability to identify specific individuals or objects where present in the field of view of the camera (e.g., John Smith, a 2009 Toyota Camry, a license plate number)

Each of these operational requirements is defined by the number of "pixels on target" recorded of the object or person in the field of view. For people, the number of pixels measured across the width of their face determines what operational requirement is achieved. While there are no established standards to define pixels on target to meet specific operational requirements, this chart outlines generally accepted thresholds in the security industry.

Operational Requirement	Horizontal Pixels/Face	Pixels per Inch
Identification	80	13
Recognition	40	4
Observation	20	2
Detection	4	1

Unless otherwise stated or defined in a risk assessment, recognition or identification includes the operational requirements for video surveillance within the classroom and interior perimeter, depending on specific use. Since these are indoor applications, at some distances identification can be achieved, but at longer distances, only detection will be possible.

Fixed cameras inside of the building do have some challenges to consider. When determining the location of a camera, the school/district should consider the following:

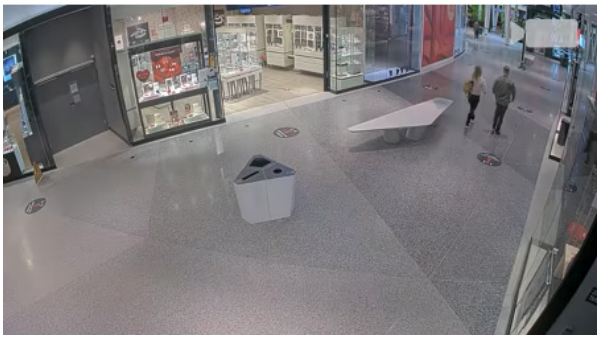
- **Environment:** Sunlight and lighting are important factors to consider. The camera should be placed in a manner that sunlight will not "wash-out" the image. In addition, adequate lighting should be in place for any time that the building is

© 2025 Partner Alliance for Safer Schools

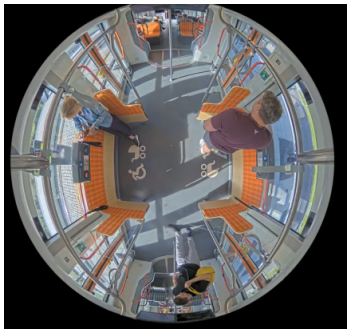
in use. After hours lighting should be considered for certain areas, such as primary openings, to ensure that a quality image is recorded.

- **Recent IP cameras** generally have wide dynamic range (WDR) and infrared (IR) built into the camera. WDR is the technology process to ensure a crisp and quality image as the lighting of the area in view changes. IR is the use of infrared light to provide "light" in a darkened space. Understand that the use of IR will cause the camera to switch to a black and white view in order to provide the best image possible. All new cameras should have WDR and IR.
- **Megapixel sizes:** IP cameras today come in a variety of sizes, commonly measured in megapixels (MP). When selecting a location for a camera, it is important to consider what type of camera will best fit the application. Currently the most common camera size ranges are 720P (2MP), 1080P (4MP or HD) and 4K (8MP) cameras. There are cameras that will have sizes above 8MP, but typically cameras in this size range are appropriate for the building interior.
- **Single and Multiple Imager Cameras:** IP cameras have a different quantity of imagers (lenses on the camera). The typical variety is single imager (1 lens), dual imager (2 lenses) and quad imager (4 lenses). Single imager cameras are typically used for a fixed location in which recognition is needed (e.g., doorway, visitor area). Dual imager cameras, referred to as 180-degree cameras, have two lenses that generally allow a full 180-degree view from the camera location. Quad imager cameras, also referred to as 360-degree cameras, have four lenses that can be moved to provide anywhere from a 180- to 360-degree view of any area. Also used in security are "fisheye" cameras which are a single imager camera that is focused through a lens that provides a 360-degree view of an area. The type of camera is important when evaluating the what the school/district wants to be able to "see" in the field of view of the camera.

Typical Camera Imager Views



Fixed Camera – Single Imager View



Fisheye Camera View



Two Imager 180-Degree View



4 Imager 360-Degree View

© 2025 Partner Alliance for Safer Schools

TIER 1

A. **Fixed Camera Coverage of Primary Openings.** Fixed camera coverage for the primary opening area should be implemented to provide a visual record of people entering the facility. The field of view should provide for identification. The video intercom provides camera coverage of people approaching the entrance, while cameras mounted in the vestibule and lobby area record movement and activities as people enter the facility.

   Schools/districts should place importance on video surveillance in areas for visitors and students entering and leaving the building. In addition to entrances, cameras should be installed in areas where students and visitors sign in and sign out of the facility, so that the field of view includes persons entering, exiting and signing in/out, to provide for identification. Ideally, this includes a camera facing the entrance door to provide an image of a person entering and a camera facing out from the door so that a person can be identified when exiting, and cameras placed for the sign in/out area(s).

B. **Fixed Camera Coverage of All Common and Known Problem Areas**. Video surveillance should cover all areas where students interact daily. These areas include cafeterias, libraries, gymnasiums, media, theaters and other common areas. Additional places to consider include areas where students and/or parents interact with staff, such as the main office or rooms that are used for parent-teacher conferences. Fixed domes are also preferable to traditional box format cameras, as the latter can be manually moved to point in a different direction than intended.

TIER 2

A. **Fixed Camera Coverage of Stairwells, Hallways and Restroom Entrances.** These areas are often identified in risk assessments as areas of concern, particularly in middle schools and high schools. Often, students loiter in stairwells between classes, making these areas important to cover. Incidents between students can occur in restrooms which, due to privacy considerations, cannot be covered by video surveillance, but it is appropriate and necessary to have a visual record of people entering and leaving these areas. Coverage of hallways is critical from a security and incident response perspective. Recognition is the operational requirement for video surveillance in these areas.

B. **Fixed Camera Coverage of Restricted Areas.** Access to certain areas within a school is restricted to authorized staff members, and the areas are usually secured behind a locked door. Video surveillance of these areas will provide a visual record of people entering and the activities taking place within them. Such areas can include server rooms, IT closets, maintenance closets and lab areas where chemicals are stored, for example. Identification and recognition are the operational requirements for video surveillance in these areas.

© 2025 Partner Alliance for Safer Schools

TIER 3

A. **Fixed Camera Coverage of Classrooms.** Classrooms should have video surveillance to assist in the overall safety and security of students and staff. Classroom cameras can be installed and recorded for e-learning and forensic purposes. Live view of cameras should be discouraged. Schools/districts should investigate their state and local laws on video surveillance cameras, and data retention, before installing cameras in the classrooms. In some localities this is restricted while others require cameras in certain types of classrooms.

   While teachers and students may have concerns with cameras in the classrooms, classrooms are public spaces with no expectation of privacy. According to Statista.com, 85% of school classrooms have digital learning tools such as Zoom or Teams. These tools were vital to the teachers and students during the pandemic for educational purposes and video surveillance cameras can now play a role in the safety and security of students and staff. Districts should consider providing information to students and staff as to how surveillance can create a safe and secure atmosphere.[13]

TIER 4

A. **Classroom Cameras with Audio Recording.** Classroom cameras should record audio when an active threat occurs. Many systems allow for an input (panic button or keyword) to initiate an alert on the video management system that can trigger the recording of audio. Polices and procedures should limit use of audio functions to specific safety and security scenarios only.. Schools/districts should investigate the state and local laws on video surveillance audio recording, and data retention, before recording audio in the classrooms.

   Audio analytics are security technologies that use software to analyze sounds and identify patterns or unexpected sounds. It can help security teams respond to threats more quickly and accurately by:

   - **Detecting threats** – Audio analytics can identify sounds like glass breaking, gunshots, or verbal aggression.
   - **Estimating direction** – Some audio analytics can determine where a sound is coming from.
   - **Triggering responses** – Audio analytics can trigger actions like recording video, playing an audio message, or alerting security staff.
   - **Protecting privacy** – Some audio analytics can capture and detect sounds without saving the original audio stream.

   The use of audio analytics can greatly assist in providing alerts for areas in which cameras are not allowed such as locker rooms, restrooms, etc.

13 https://www.statista.com/statistics/1076708/uses-digital-learning-tools-us-k-12-teachers/)

© 2025 Partner Alliance for Safer Schools

DETECTION AND ALARMS COMPONENT :

TIER 1

A. **Panic Alarm System in Each Building.** Each building must have a panic alarm system that sends automatic signal to local law enforcement for immediate response. Activation must automatically notify law enforcement through a 24/7 monitoring station and/or 911 call center, in accordance with state and local law. Additionally, physical panic buttons should be located in the common areas of each building. At minimum the primary areas for panic buttons include but are not limited to:

- Front/main office
- Counseling office
- Cafeteria
- Library
- One per hallway

B. **Panic Alarm System in Each Classroom.** Each classroom should have a panic alarm button. The panic button may be wired or wireless.

Schools should consult local law enforcement, security professionals and district's safety and security team to determine whether the primary areas are enough or additional locations are needed. In addition to the primary locations, secondary locations for panic buttons should also be installed. Secondary locations could include other areas based on our risk assessment and recommendations of the district's safety and security team, local law enforcement and emergency first responders.

An advantage of intrusion detection technology is the ability to add devices to the system in a cost-effective manner. One use of the intrusion system is to allow for panic buttons to be installed that can assist in implementing procedures for a variety of life safety threats. It is important that the school/district consider how existing intrusion, networks and other technologies could provide panic alarm systems. Intrusion systems also have wireless capabilities allowing teachers to carry devices on their persons that can alert administration, district and possibly first responders that emergency events are taking place. Coordination with law enforcement and other first responders is recommended if the decision is made to implement such a system.

TIER 2

A. **Panic Alarm System With Wearable Devices.** Wearable devices are wireless devices that allow for a panic alarm to be initiated. Wearables devices should be provided to all staff that supervise children, security personnel, health and counseling staff.

When implementing wireless devices, it is important that the technology has redundancies built-in to ensure that the devices are working properly and operating within parameters. Wireless panic systems should have some sort of supervision that shows that the devices are communicating with the panic alarm system. In addition, the ability for the wireless devices to have a redundant way to transmit the signal is important. Finally, the hardware that monitors the wireless devices should have some sort of redundant power source (batteries, UPS, etc.).

© 2025 Partner Alliance for Safer Schools

B. Intrusion Detection System Covering All Hallways and Public Areas. While intrusion detection can be limited to the breach of the building from the outside, the addition of motion sensors inside the building assists as a second level of detection in case an entry occurs that does not involve a door or window being breached. By covering hallways and public areas, the intrusion system can deter events such as theft and internal vandalism by persons who may "hide out" in the school building after the building closes.

The ability to monitor hallways and public areas also supports an all-hazard approach to safety in the event of an emergency. Responding to a weather threat, an intrusion system can be activated to alert administration to any movement in the areas where staff and students should not be during the weather emergency. The system also assists in active threat drills to see how quickly hallways and public areas are evacuated and in tracking a potential perpetrator while under an active threat scenario.

C. Unification of Fire Alarm and Panic Alarm Systems: The school should investigate the ability to interface the fire alarm and panic alarm systems to prevent conflicting alarms. For example, the fire alarm systems have the ability to "delay" notification of a fire alarm until authorized personnel can investigate as to whether the alarm is real or false.

NFPA allows for notification of a fire alarm to be delayed until an authorized person can investigate as to whether the alarm is false. This "private mode" of notification is available on most fire alarm systems. Schools/districts must work with the local AHJ when determining whether the fire alarm notification can be delayed during a panic alarm event.

D. Unification of Panic Systems And Access Control System: The panic alarm system should be unified with the access control system to allow for the response process to be automated. Most access control systems are capable of receiving information from the panic system via relays or software interface.

Unification of the access control system with the panic alarm systems allows for automation of such processes including:

- Locking appropriate doors inside and outside of the building.
- Closing doors in hallways to further partition the building, restricting access to unwanted individuals.
- Restricting access control via credentials to prevent opening doors that should be locked during the event.
- Allowing credentials for first responders and law enforcement to gain access to all areas of the building to efficiently respond to the event. See Access Control Component in the Building Property Layer for more information.

E. Unification of Panic Alarm Systems With Video Surveillance System: The panic alarm system should provide an automated "alert" to the video surveillance system that will activate functions of the video surveillance system that are critical to live event information. Video surveillance systems have the ability to take information from the panic alarm system so that video from appropriate cameras is automatically provided to the SOC, and to persons monitoring the video surveillance system as well as providing real time information to first responders. See Communication Component for Audio integration with video surveillance systems.

Further, with the use of video analytics and AI, video surveillance systems can provide real time detection of specific anomalies in actions or movements inside and outside the building , providing the basis for, or in response to an alert.

© 2025 Partner Alliance for Safer Schools

F. **Unification of Panic Alarm Systems and Communication Systems:** The unification of the detection and alarm systems with the communication system allows for automation of emergency procedures as well. For example, the activation of a panic alarm can automate the simultaneous transmission of emergency messages.

G. **Unified Communication and Detection System Monitored 24/7.** For districts that do not have an SOC: At the building level, administrators should investigate how other life safety and detection systems can be unified to provide an efficient way to activate emergency procedures and notify students, staff and visitors that a threat is imminent. The systems should be monitored by either a central monitoring service or 911 center. For example, the intercom, fire alarm and paging systems can all be integrated with the intrusion system to provide instant alert of a threat. This unification allows monitoring by a central monitoring system. As with a fire alarm, a process should be in place to drill and train for the event protocol of monitoring the system 24/7.

H. **Unified Communication and Detection System Monitored by District-Wide SOC.** For districts that do have a SOC, it is important that the intrusion system is monitored by the SOC during regular school hours as well as after hour and weekend events, allowing the district to provide alerts and notifications district-wide or to individual schools. This allows the intrusion system to not just be used to provide information at the facility that has the event but also allows for processes to be implemented at other facilities, based on the threat detected.

I. **Unification of Alarms, Communications, Video Surveillance and Access Control Systems.** As districts implement intrusion detection technology, the goal should always be greater unification with other systems to provide the best protection for staff and students. For example, devices such as door position switches on the intrusion system can also be used with the access control system, as well as provide an input to the video surveillance system to tag activity at a door.

TIER 3

A. **Panic Alarm System With Wearable Devices to All Staff.** Wearable panic devices should be provided to all school staff members including providing devices to substitute teachers and personnel that are regularly in the building.

B. **Intrusion Detection System Covering All Classrooms.** The benefits of using detection systems within a classroom are two-fold. Detection inside the classroom allows for an alert to be sent to administration when persons are inside classrooms during hours in which they should not be admitted. Intrusion, when covering all classrooms and hallways, can also assist in knowing when the building is evacuated after an emergency event as well assist in clearing a building and re-unification efforts.

© 2025 Partner Alliance for Safer Schools

ADDITIONAL RESOURCES

© 2025 Partner Alliance for Safer Schools

Enhanced Technologies

Schools may want to consider certain enhancements or special features of safety and security components described in the Tier Continuum. Below are just a few of these technologies and security system features that have received significant recent interest, as well as their potential benefits.

The Pilot Program

First, a pilot project is a good way for districts to evaluate new security products, particularly enhanced technologies, prior to full-scale implementation. This allows the collection of data on its performance, refinement of processes and even finding additional beneficial uses. Many manufacturers and integrators will provide products and services that can be tested by end users in a small, controlled location before they are deployed on a larger scale. PASS encourages end users "to try before you buy" when it comes to enhanced technologies to ensure that the technology or service will work with your district security posture and systems.

The Goal: Unified Security and Life Safety Systems

Any enhanced technology implementation should further the unification of security and safety components and related systems by school districts. Unified systems address the difficulties of integrating technologies across different platforms and within the connected environment in which they reside. Properly implemented, a unified system eases integration of new components and allows a district to continue to evolve and expand. It is important for a school district to work with their integrator to ensure facility infrastructure can support any new technology as part of a unified system.

Weapons and Prohibited Items Detection

The need for weapons and prohibited items detection systems will vary across schools and districts based on physical layout and risk profile. While such technologies alone cannot prevent all weapons from entering schools, they can provide an additional and critical layer of safety and security for students, staff and visitors, when procured and utilized as designed (see also Brandished Weapons Analytics discussed in the District-Wide Layer). Modern detection technologies could play a key role in averting or mitigating attacks. According to a 2021 U.S. Secret Service analysis of plots against schools from 2006-2018, over half the plotters in 67 averted attacks (n=37, 55%) chose to use at least two or three types of weapons, and in nearly all of the cases (n=64, 96%) the weapon(s) of choice were firearms, versus incendiary devices or knives (which are more difficult to detect). The "human factor" is critical. Implementation should support clearly communicated district- wide policies on what is permitted on campus and should be accompanied by clear procedures and staff training regarding the response when a prohibited item or threat is detected.

Metal Detectors

Traditionally, detection has been carried out through use of walk-through metal detectors (WTMDs) or hand-held metal detectors (HHMD), often with the latter as secondary screening. This will be most effective when the number of entry points to a building or sporting fields for events, etc. are limited to one or as few as possible. If a person transiting the WTMD triggers an alarm, they are quickly moved aside where security uses a HHMD to pinpoint the object in question without having to physically touch them. WTMDs

© 2025 Partner Alliance for Safer Schools

combined with HHMDs provide a faster, more accurate and less intrusive than hand-held screening alone resulting in an overall better experience for students and staff. With HHMD alone, screening consistency and accuracy can vary among individual screeners. Passive detection. Several technologies are becoming available that allow contraband and weapons detection without intrusive or labor- intensive screening–with the potential for tremendous positive impact on school safety. For example, terahertz and millimeter wave technology can detect a wide range of both metal and nonmetal items through a variety of materials and from a distance. Additionally, advanced image analysis in conjunction with video surveillance systems has been increasingly leveraged for weapons detection.

Vape Detectors

Vape detection was discussed as a feature of several safety and security components within the Tier Continuum. Vaping is not only a significant health risk to children, but it has also become an enormous behavioral issue within many schools as it is very difficult to detect. Vape detection technology is now available that utilizes multifunction sensors resembling smoke or carbon monoxide detectors. These devices can detect vaping in places such as bathrooms or confined areas. Currently most of the providers offer a service that will send a text notification to designated staff when there is a detection of vaping in the vicinity of one of the sensors. An effective best practice in conjunction with vape detectors is to ensure that there is camera coverage of the hallways outside of restrooms or entrances where this activity commonly occurs. When a detection is made, the time of the vape detection and images of entry and exit into the space can be compared. Sensors should be hardened against vandalism and deployment should be accompanied by other procedures to counter efforts to defeat or disable them, such as sealing or alarming any restroom windows.

Electronic Hall Passes

The use of electronic hall pass systems in concert with detection technologies is an approach that can help further reduce student vaping, in addition to many other benefits. These systems typically allow students to use electronic devices to submit requests for hall passes more freely and conveniently. When a request is submitted electronically, the teacher can quickly approve or deny the request with less classroom disruption and more time on tasks. Other authorized staff can see that the pass has been issued on their devices, which makes it easier for them to tell if a student they encounter during instructional periods has a valid hall pass and is in a location consistent with the pass.

These systems can help prevent vandalism, truancy, sexual misconduct, fights and other problem behaviors, by displaying and controlling which students have passes at specific times. One example is being able to enforce "no contact" orders related to harassment or stalking. Administrators can enter the names of students who are not supposed to have contact with each other, so the system will not approve requests from either student if the other student is out of class with a pass.

Enhanced Data Analytics for Threat Detection

More video and audio analytics capabilities are being included or available with modern security systems. Audio analytics involves the use of sensors and software that can detect and identify specific acoustic signatures of threat indicators, such as glass breaking, gunshots, aggression or panic in people's voices and audible alarms (see discussion of audio analytics within the Video Surveillance Component throughout the Guidelines). This technology can be loaded directly on cameras (as most network cameras

© 2025 Partner Alliance for Safer Schools

already include a microphone), providing a dual-sensor technology capability within the same coverage area, or by using stand-alone devices. When triggered, an alert can be sent to designated safety and security staff to review the video and determine if a response is required. If incorporated on a camera, audio analytics are not limited by its field of view, so in some cases a trigger may require other means to verify a threat. There are additional types of sensors as well for gunshot detection that would provide similar alerts, including those based on technology to detect specific shockwave, infrared or smoke signatures from firearms discharge.

In more frequent events, speeding is a major factor in a large proportion of crashes, injuries and fatalities on school grounds. Some video management systems have speeding vehicle analytics. The systems can be helpful in detecting dangerous driving behaviors of students, especially in high school parking lots. Additionally, license plate reader (LPR) and data solutions can provide the ability to enter license plate information for vehicles where notification to safety and security staff is needed upon entry, such as for vehicles belonging to individuals involved in custody issues for example. License plate data can also be processed through criminal and sexual offender databases provide early warning to security and safety personnel if a related vehicle enters the property. Implementation of any of these technologies should follow manufacturer guidelines for sensor selection and placement.

Biometrics

Biometrics are the measurement and matching of physical characteristics unique to an individual, which provides an accurate way to authenticate identity that is often more efficient and secure than other methods. Use of biometric technologies in K-12 schools is becoming more prevalent as they become widely deployed in the private sector to improve business practices and secure financial transactions. While the primary rationale for use of biometrics by a school or district is to streamline administrative functions requiring identity verification and enhance data security (such as account access), there are physical security applications as well.

Finger scanning technology offers a good example of how biometric authentication technology can enhance operations without compromising privacy. During electronic enrollment of the biometric, a staff member or student's fingerprint is translated to a numerical format based on features of the finger lines, creating a unique code that is then associated with the person's identity in a school database. The fingerprint itself is not recorded–only the unique code issued by the specific software used is retained. From a technological standpoint, the process cannot be reversed to create a fingerprint based on the unique code. Additionally, all biometrics providers use proprietary algorithms to create and compare the codes, making it nearly impossible for data to be used outside the system and beyond the purpose for which it was created. Use of biometrics should be governed by a use policy set at the district level, include requirements such as providing a parental opt-out procedure to ensure any student participation in account access or verification applications is voluntary, and ensuring the destruction of all biometric-related information associated with a student or employee when they end their association with a school.

Biometric readers can reduce or eliminate the need for (and expense of) using cards and keys or remembering PINs and account numbers. Biometrics-based check-in for transportation pick up/drop off for example, works the same as card-based check-in but may offer a more reliable process without the need for the student to remember and carry an ID card. Keys and cards do not identify the person holding them and thus are more vulnerable to use by unauthorized persons.

© 2025 Partner Alliance for Safer Schools

Facial Recognition

While biometric technologies like finger scanning have been used for many years in K-12, the emergence of facial recognition offers some advantages by allowing a touchless interface and requiring less complex technology, using digital images for account enrollment and verification. It also offers other promising benefits for enhancing security systems and procedures.

Now commonly available as a video analytic feature within video surveillance systems used in K-12, facial recogntion is being utilized for both forensic and preventative purposes (see discussion on video analytics within the District-Wide Layer). Most commonly these purposes include alerting staff to the presence of individuals who have made threats of violence against a school; helping to immediately locate missing children on school grounds or determine their whereabouts; and providing alerts to staff in common situations where specific individuals are prohibited from entering school grounds under a court order or district determination.

Additionally, there is growing utilization in K-12 and higher education environments in access control systems as a voluntary identification credential for student and staff access to athletic facilities and other areas.

It is critical that any implementation of biometric technologies for such purposes closely adhere to any applicable laws that restrict use of such technologies in schools. Additionally, the security planning team should keep community stakeholders informed, providing clear information about the purpose and parameters for using the technology, where it unifies with other security components, and a thorough use policy. Such transparency can help address any misperceptions about the security of information collected or potential for misuse.

© 2025 Partner Alliance for Safer Schools

Key Resources

Partner Alliance for Safer Schools (PASS)
passk12.org

Americans with Disabilities Act, 1991
ada.gov

Door Security and Safety Foundation
lockdontblock.org

Final Report of the Federal Commission on School Safety
www2.ed.gov/documents/school-safety/school-safety-report.pdf

National Association of School Resource Officers–Best Practices for School Resource Officer Programs
nasro.org/clientuploads/NASRO_BestPractices21.pdf

National Association of State Fire Marshals–Classroom Door Security and Locking Hardware
firemarshals.org/NASFM-Documents

National Center for Spectator Sports Safety and Security
ncs4.com

National Council on School Facilities
facilitiescouncil.org/ncsf-home

National Fire Protection Association (NFPA)
nfpa.org/Codes-and-Standards/All-Codes-and-Standards/List-of-Codes-and-Standards

- NFPA 72–National Fire Alarm and Signaling Code NFPA 730–Guide for Premises Security
- NFPA 731–Standard for the Installation of Electronic Premises Security Systems
- NFPA 3000–Standard for an Active Shooter/Hostile Event Response (ASHER) Program

National School Boards Association Center for Safe Schools
nsba4safeschools.org

National Systems Contractors Association
nsca.org

© 2025 Partner Alliance for Safer Schools

Readiness and Emergency Management for Schools Technical Assistance Center
rems.ed.gov

- Guide for Developing High-Quality School Emergency Operations Plans
  rems.ed.gov/docs/REMS_K-12_Guide_508.pdf
- EOP Interactive Tools
  rems.ed.gov/EOPinteractivetools.aspx?AspxAutoDetectCookieSupport=1
- Cybersecurity Considerations for K-12 Schools and School Districts
  rems.ed.gov/trainings/CourseCybersecurity.aspx
- Assessing Your School Site
  rems.ed.gov/trainings/CourseSiteAssessment.aspx
- Planning to Recover from Emergencies at Districts and Schools
  rems.ed.gov/webinarDetail?id=17
- K-12 School Planning and Response Teams: Developing and Enhancing the School Emergency Operations Plan (Checklist)
  rems.ed.gov/docs/SchoolEOPChecklist_508C.pdf
- State Emergency Management Resources
  rems.ed.gov/StateResources.aspx
- Emergency Management Virtual Toolkit
  rems.ed.gov/EMVirtualToolkitRegistration.aspx

Safe and Sound Schools: a Sandy Hook Initiative–Straight A Safety Improvement Toolkits
safeandsoundschools.org/programs-2/toolkits

Security Industry Association
securityindustry.org

SIA Guide to School Security Funding
securityindustry.org/report/sia-guide-to-school-security-funding

The Police Foundation–Averted School Violence Database
asvnearmiss.org

© 2025 Partner Alliance for Safer Schools

Federal School Safety Clearinghouse
schoolsafety.gov

- Threat Assessment and Reporting
  schoolsafety.gov/threat-assessment-and-reporting
- Targeted Violence
  schoolsafety.gov/targeted-violence

U.S. Department of Homeland Security–Building and Infrastructure Protection Series: Primer to Design Safe School Projects in Case of Terrorist Attacks and School Shootings (FEMA-428/BIPS-07)
dhs.gov/xlibrary/assets/st/bips07_428_schools.pdf

FEMA Training–Preparing for Emergencies: What School Staff Need to Know
firstrespondertraining.gov/frts/npccatalog?id=3208

FEMA Sample School Emergency Operations Plan (for Training Purposes)
training.fema.gov/programs/emischool/el361toolkit/assets/sampleplan.pdftraining.fema.gov/programs/emischool/el361toolkit/assets/sampleplan.pdf

FEMA Training–School Incident Command Systems
training.fema.gov/is/courseoverview.aspx?code=IS-100.c&lang=en

FEMA Homeland Security Exercise and Evaluation Program (HSEEP) Guidelines
fema.gov/emergency-managers/national-preparedness/exercises/hseep

Family Educational Rights and Privacy Act: A Guide for Emergency Managers and Law Enforcement
fbi.gov/file-repository/ferpa-guide.pdf/view

FAQs on Photos and Videos under FERPA
studentprivacy.ed.gov/faq/faqs-photos-and-videos-under-ferpa

U.S. Department of Health and Human Services–Resources After a School Tragedy
mhttcnetwork.org/centers/mhttc-network-coordinating-office/product/after-school-tragedyreadiness-response-recovery

Developing a Memorandum of Understanding (MOU) for School-Justice Partnerships: Technical Assistance Tools
ncjfcj.org/publications/developing-a-memorandum-of-understanding-mou-for-school-justice-partnerships-technical-assistance-tools/

© 2025 Partner Alliance for Safer Schools

Memorandum of Understanding (MOU): School Resource Officer Program & Other Law Enforcement Responses to School-Based Incidents (Example)
montgomeryschoolsmd.org/uploadedFiles/departments/security-new/Executed%20SRO%20MOU.PDF

Trauma Sensitive School Training Package: Building Trauma-Sensitive Schools
safesupportivelearning.ed.gov/building-trauma-sensitive-schools

© 2025 Partner Alliance for Safer Schools

PASS
Partner Alliance
for Safer Schools

passk12.org

© 2025 Partner Alliance for Safer Schools