



PASS

Partner Alliance
for Safer Schools

SCHOOL SAFETY AND SECURITY CHECKLIST

TIER 1	TIER 2	TIER 3	TIER 4
-----------	-----------	-----------	-----------



DISTRICT-WIDE LAYER

STATUS

YEAR

NOTES

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		✓	✓	✓

TIER 1	TIER 2	TIER 3	TIER 4
-----------	-----------	-----------	-----------



DISTRICT-WIDE LAYER (cont.)

STATUS

YEAR

NOTES

WEATHER MONITORING

» Monitor NOAA Local Weather Information	✓	✓	✓	✓
» Weather Monitoring Service		✓	✓	✓
» Weather Monitoring Station at Central School Facility			✓	✓

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			✓	✓
» 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 w/ Access Control, Video Surveillance and Comm. Systems				
» Two Way Emergency Phones				
» Graphical User Interface for Operators				
» Intrusion and Duress Alarms Monitored by a District-Wide SOC				



DIGITAL INFRASTRUCTURE LAYER

TIER 1	TIER 2	TIER 3	TIER 4
-----------	-----------	-----------	-----------

STATUS

YEAR

NOTES

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			✓	✓



DIGITAL INFRASTRUCTURE LAYER (cont.)

STATUS

YEAR

NOTES

POLICIES AND PROCEDURES

» 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	✓	✓	✓	✓



DIGITAL INFRASTRUCTURE LAYER (cont.)

TIER 1	TIER 2	TIER 3	TIER 4
-----------	-----------	-----------	-----------

STATUS

YEAR

NOTES

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				✓

**DIGITAL INFRASTRUCTURE LAYER** (cont.)

TIER 1	TIER 2	TIER 3	TIER 4
-----------	-----------	-----------	-----------

STATUS**YEAR****NOTES****COMMUNICATION**

» Communication Plan (Email, Phone, Contacts, etc.)	✓	✓	✓	✓			
» Communicate With Key Stakeholders When Performing Maintenance on Network Systems	✓	✓	✓	✓			
» Vulnerability Reporting Program			✓	✓			

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	✓	✓	✓	✓			

COMMUNICATION

» 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 PROCESSING AND TRANSPARENCY

» Fixed Camera, Wide Area Coverage	✓	✓	✓	✓			
» Infrared (IR) Cameras or Lighting		✓	✓	✓			
» Wireless Video Data Transmission		✓	✓	✓			



DIGITAL INFRASTRUCTURE LAYER (cont.)

	TIER 1	TIER 2	TIER 3	TIER 4	STATUS	YEAR	NOTES
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				✓			

TIER 1	TIER 2	TIER 3	TIER 4
-----------	-----------	-----------	-----------



CAMPUS EXTERIOR PERIMETER LAYER

STATUS

YEAR

NOTES

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				✓			

DETECTIONS AND ALARMS

» Panic Alarm System Within Greenspace Areas		✓	✓	✓			
--	--	---	---	---	--	--	--



BUILDING PERIMETER LAYER

	TIER 1	TIER 2	TIER 3	TIER 4	STATUS	YEAR	NOTES
POLICIES AND PROCEDURES							
» Categorization of ALL Exterior Openings	✓	✓	✓	✓			
» Policy Established for Control of Exterior Openings	✓	✓	✓	✓			
» Key Control Procedures	✓	✓	✓	✓			
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				✓			



BUILDING PERIMETER LAYER

ACCESS CONTROL

	TIER 1	TIER 2	TIER 3	TIER 4	STATUS	YEAR	NOTES
» 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			✓	✓			



CLASSROOM INTERIOR LAYER

	TIER 1	TIER 2	TIER 3	TIER 4	STATUS	YEAR	NOTES
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				✓			



CLASSROOM INTERIOR LAYER

	TIER 1	TIER 2	TIER 3	TIER 4	STATUS	YEAR	NOTES
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			✓	✓			



PASS
Partner Alliance
for Safer Schools

passk12.org