

Electronic Security Guidelines for Schools



Introduction



Who: I am a security consultant with Homeland Safety Systems Inc.

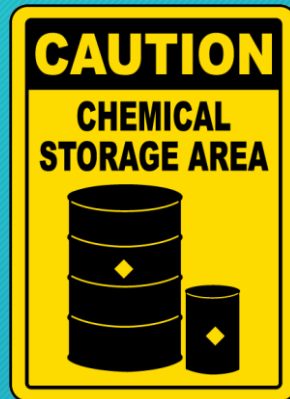


What: We are a system design and manufacturing company that specializes in access control, digital surveillance, intrusion alarms, metal detectors, and system integration.



Why: Our goal is to help schools maintain a safe setting for both students and staff. We will provide an overview of school security, the steps needed to develop and implement a security plan, and how it can enhance student achievement

Types of Internal Threats



- Behavior of students
- Active threats – Ex. active shooter
- Passive threats – Ex. network attack
- After-school activities – Ex. visitors may be present with minimal security
- Utility failures and accidents
- Chemical storage and disposal
- Fire

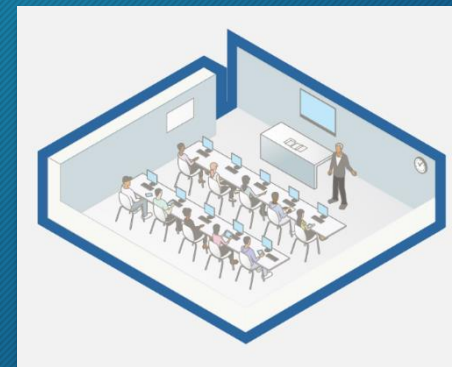
Types of External Threats

- Natural disasters
- Nearby Industries
- Local criminal activity
- Nearby prisons
- Major highways and roadways
- Railroads
- Availability of emergency responders



Layers of Protection

- Outer Perimeter – Ex. Parking lot, adjacent athletic field, outlying buildings. This can be multi-layered.
- Building Perimeter – With primary and secondary entry points
- Interior Spaces – Ex. classrooms, staff offices, hallways and stairwells, cafeteria, gymnasium, auditorium



Security Solutions

Special technologies and system uses apply to each area on campus:

Perimeter – Basic Intrusion Detection System and surveillance

Building – Access Control and surveillance

Interior Spaces – Surveillance



System Equipment Options

Access Control

An **Access Control System** is made up of doors, frames, hinges, door closers, gates, locks, keys, card readers, card and tokens, biometric readers, and software

Entry/exit points:

- Primary (main entrance)
- Secondary (exterior doors)
- Other (Interior openings, grouped into partitions of the building)

Building occupants should be given specific access rights to certain areas of the school.



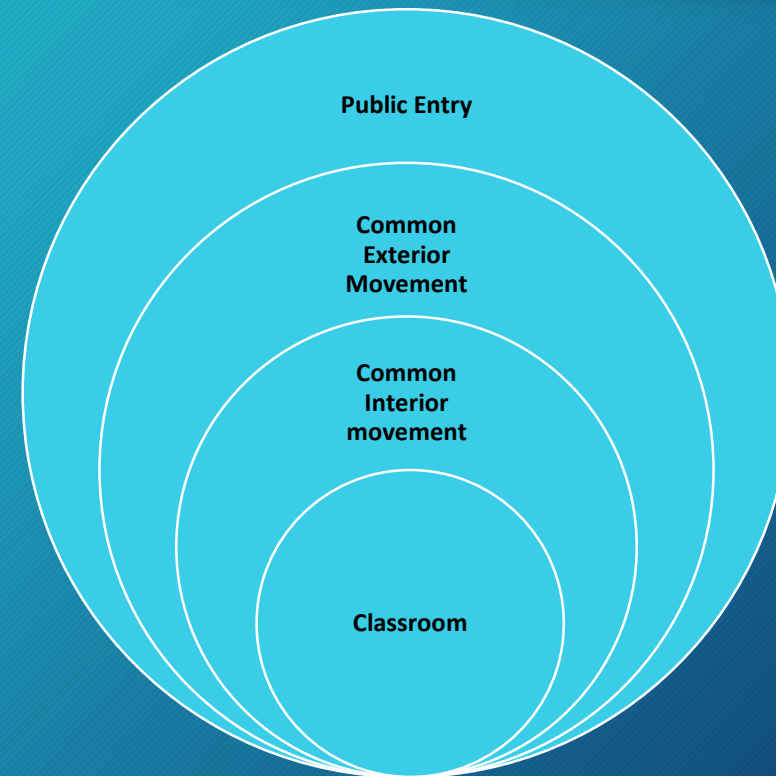
Layers of Access Control Security

Controlled access through a primary entrance:

- Commonly used to provide a secure area
- The outer door is typically locked during normal school hours
- The interior set of doors are locked during school hours but allow free egress.
- Interior doors are controlled by a card reader (for faculty and staff) and can be controlled from the main office (for visitors).

Temporary badging:

- Offers added control for visitors, as well as temporary staff (substitute teachers or temporary custodians) and contractors.
- Provides availability for layered security options



Surveillance

A **Surveillance System** is made up of cameras, special cabling, and a monitoring system.



- Cameras are often placed at exterior doors to verify alarms or screen visitors, and to monitor who is coming and going in the building.
- Used for large areas (interior and exterior) to monitor certain activities that provide safe passage along certain routes of transit for students and staff.
- Should support IP-video transmission and be selected based on the manufacturer's specifications for their intended use.

Monitoring and Supervision

A **Monitoring System** is made up of display screens, video and data, and video recording devices.

- Performed by personnel watching live feeds on a display screen, usually with the intent of providing immediate response to an event.
- Passive Monitoring is recorded and viewed or analyzed later, usually as part of an event investigation.
- Can be done on-site or remotely by professional monitoring service providers as a full-time or part-time supplemental service.



Panic Buttons

Panic Buttons are usually part of a more general intrusion system.

- Can be placed in fixed locations for key staff, such as the main office or portable devices
- Can be used by certain school staff who work late hours or with high-risk students.
- Alarm signals sent by these devices may go to a monitoring center (internal or external) to verify the alarm, not direct dial to first responders.



Intrusion Detection Systems

Intrusion Detection Systems (burglar alarms) are used for perimeter control, for either an outer perimeter or the building perimeter.



- Sensor driven and activate alarm warnings when a violation of the perimeter is detected, such as open door, motion detected, broken glass, etc.
- Alarm activates the **Communication System** calling a monitoring station for verification, possibly by on-site guards or captured video.
- Can automatically activate video recording.

Communication System

The **Communication System** includes parts of several other systems, wired and wireless, such as:

Intercom Systems

- Video and voice
- Used for entry verification or for general school communications

Local Alarm Annunciators

- For fire, intrusion, and other emergencies

Internal Notifications

- Sent to classrooms through smart boards or staff cell phones

External Calls to 911

- Police, private responders, or fire

Two-Way Radios

- Used by staff or guards to compliment security system that is in place during emergencies



Emergency Preparedness

- In recent years, the percentage of public schools reporting the use of security cameras increased from **19 to 75 percent**.
- The increase in school shootings and school related crimes has put a strain on the learning environment.
- **Motion Detection Cameras** provide an alert of unauthorized access to the facility to help with emergency preparedness.



Mechanical Devices and Materials

Locks and keys:

- Includes both electronic locks controlled by an access control software system and mechanical locks
- Key tracking software can be used to create a database of who has been issued which keys.
- The Security Manager should do periodic system reviews that include locks and physical barrier to entry, at least quarterly.



Metal Detectors

- The ability to detect weapons from people entering the building
- Certain districts may benefit from weapon detection more than others
- Are meant to complement a wider security strategy
- Ensures a safe environment so teachers and students can focus on learning



Signage

- Direct visitors toward desired main entry point
- Deter undesired activities, such as “no trespassing,” “drug-free zone,” “this area monitored by cameras,” etc.
- Inform visitors of surveillance, especially video and audio recording (Disclosure might be required by local laws.)
- Signage should be clearly visible and readable
- Direct occupants in emergencies toward designated safe areas or evacuation routes



Scale and Funding Considerations

Decision Maker Approvals

The school should hold community consultations early, giving all affected parties an opportunity to provide input and to prepare for coming potential changes.

These parties include:

- School Board
- Parents
- Faculty/Staff
- Students
- Custodians



Compatibility with Existing Equipment

Non-proprietary Equipment

- More cost effective in the long-run
- More likely to ensure compatibility with other equipment (existing and future)
- Allows more flexibility

Proprietary Equipment

Needed to extend an existing proprietary system instead of replacing it, or for special advanced applications

Future Planning

Scaling – Systems can be implemented with phased-in additions for multi-year budgeting.

Infrastructure – It is usually more cost-effective to include the security system infrastructure in planned construction.

Recurring costs - Should consider costs for licensing and permits, lost and new cards or tokens, ongoing maintenance, remote monitoring systems, signage, data backups, and video storage.

Funding Sources

User Fees

- Cost offsets
- One-time initial fees
- Recovery of reoccurring costs (such as for lost access cards)

Sponsors

- Private donors
- Alumni associations

Public-Private Partnerships

- Agencies that work with private industry in community safety programs

Bond Elections

- Local government funding, voted on by the local community

Government Grants - Federal funds for emergency preparedness, direct or matched to local government funding (ex. COPS Grant)



Cultural Considerations

Geographical Location and Community Values



Many local factors affect the school's choice in system operation and performance.

Local law enforcement can provide:

- Useful crime data
- Historical analysis
- Types of crime and frequency

This information should be discussed with security professionals during their security surveys.

Local Laws and Codes

Schools should consult their local police department and fire marshal for advice on laws regarding:

- The rights of the public to school access
- Prohibited items
- Requirements for construction methods
- Required inspections



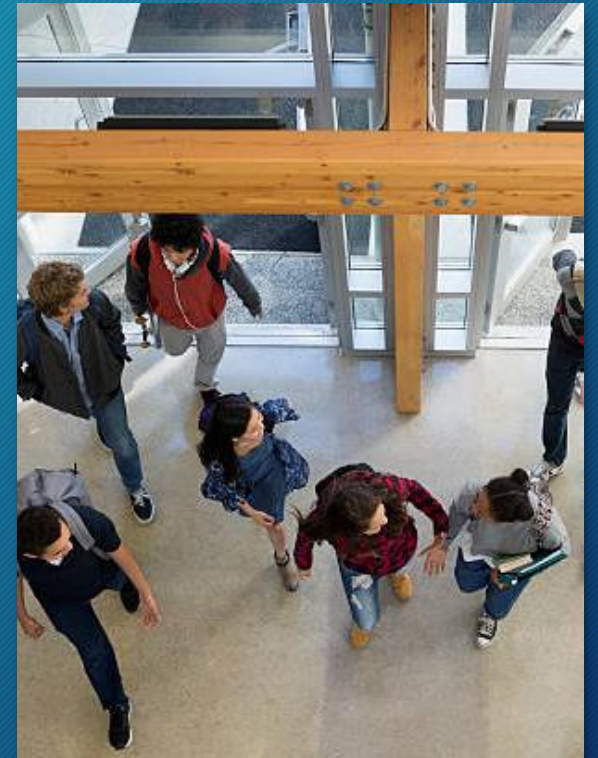
Safety vs. Convenience

School administrators should:

- Help all school personnel understand how they will use the system and what to expect.
- **Communicate effectively** throughout the planning stages to manage expectations.

The security system may:

- Change traffic patterns
- Interfere with freedom of movement for students, staff, and visitors
- Limit ease of access through secondary points



Activities and Visitors

School administrators should:

- Review typical activities and routines, both during school hours and after-hours, as well as typical types of visitors they expect.
- Review desired alternate uses for the school, special events, and multi-purpose areas.
- Discuss flexibility of reconfiguring the system with potential security contractors.



Non-Compliant Access Control Products

- “The Sleeve” is a device that slips over the closer-arm of a door to prevent the door from being opened from the outside.
- Prevents individuals from entering or exiting a classroom in the event of an emergency
- ADA restricts the height of an operable part of most locks and latches on doors to a range of 34 to 48 inches to prevent the unintentional trapping of someone with a physical handicap.



Selection of Contractors

Types of Procurement

GSA Schedule Contract

- Simplified procurement process
- Compliant with all laws and regulations
- Prices are already deemed fair and reasonable
- Access to emerging technologies and innovative solutions

Registered Vendor with State of Arkansas

- Competitive pricing
- Meets standards of quality
- Reduced risk by going with a trusted vendor



Types of Procurement Cont.

TIPS/TAPS (Interlocal Purchasing System)

- Full line of contract solutions
- Competitive bidding process on behalf of its member's needs
- Saves time and money
- Quality pricing
- Ability to select vendor and representative you want



Methods of Solicitation

Sole source (No-bid contract) – There is only one person or company that can meet the projects needs. Any attempt to obtain bids would result in only one person or company being available to meet the need.

Request for Information (RFI) – to determine who is interested and their capabilities

Request for Quote (RFQ) – to obtain a simple price quote, usually for early or general budgetary planning

Request for Proposal (RFP) – to obtain a proposal with a system design, price quote, and terms of fulfillment

Indefinite Delivery Indefinite Quantity (IDIQ) – provide a method of order from existing indefinite-delivery contracts awarded by another agency.

Sources Sought/RFI – used by government agencies to solicit interest in a project under consideration by that agency. It is not an actual bid or proposal solicitation.

Team Member Roles and Key Stakeholders

Involve Key Stakeholders

- School administrators should review the threat assessment and cultural considerations and adjust the design if necessary.
- All stakeholders should be kept informed of the decisions and tradeoffs being made during this process.
- All affected parties should be notified of the work being done, including the community, faculty, students, parents, and other frequent visitors.



A Security Team

A school administrator should designate individuals to key functional roles on the **internal** and **external** security team.

Internal Roles	External Roles
Safety Manager	School Board Liaison
Security Manager	Life Safety Liaison
Facilities Manager	Law Enforcement Liaison
IT Manager	

The school administrator should also seek advice from qualified security professionals early in the planning process. Security consultants can help coordinate among team members and outside agencies.

Team Member Roles

Consultant (provider role)

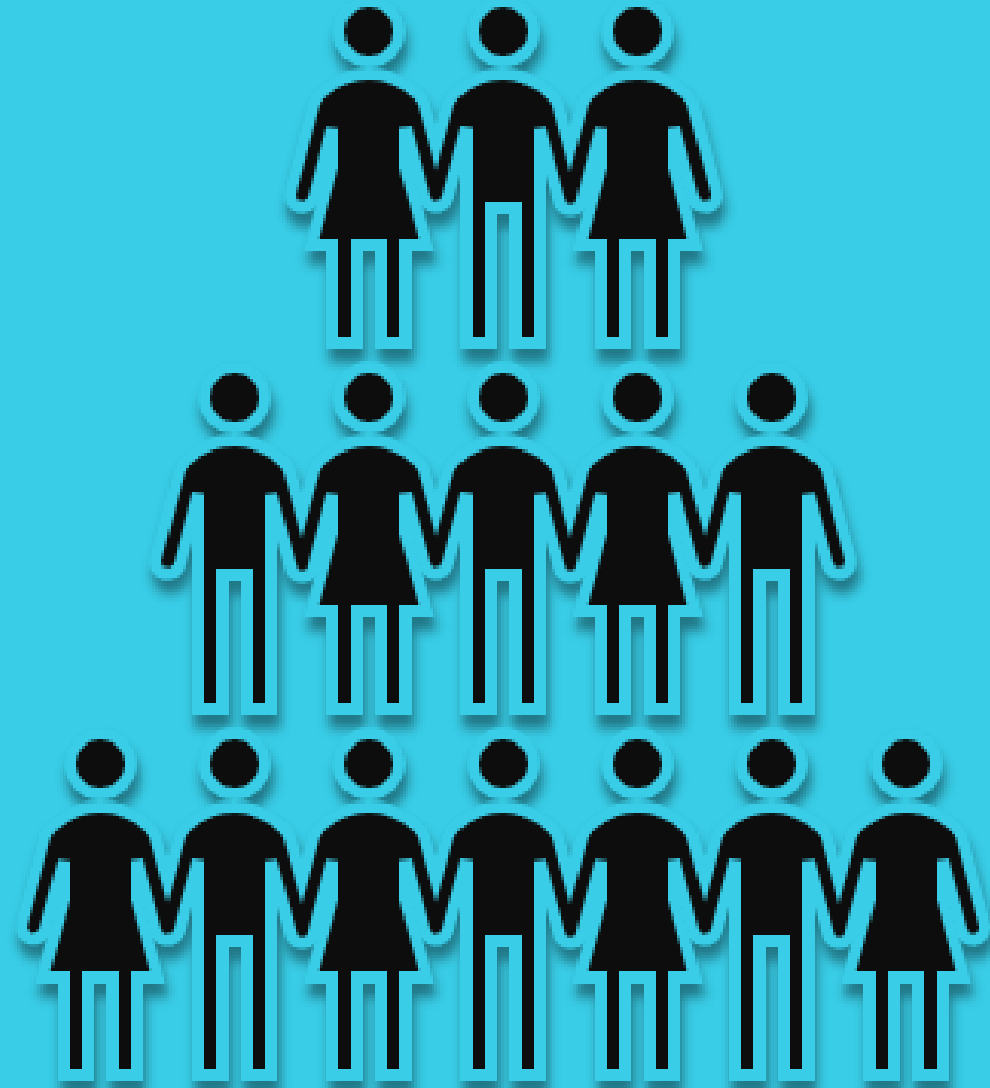
Integrator (provider role)

Safety Manager (customer role)

Security Manager (customer role)

Facilities Manager (customer role)

IT Manager (customer role)



Modes of Operation

Modes of Operation

Normal

- Accommodates routine traffic patterns during normal school hours
- Primary focus should be on controlling access to interior and exterior openings, monitoring activities, and communicating with occupants

Special

- After-hours activities, special events, or special visitors
- Surveillance and monitoring will change

Emergency

- When there is an active threat
- System can direct students to shelter, evacuate, etc.



Lockdown and Egress

- Lockdown can be controlled locally (each door individually) or from a central control, locking all internal doors and external entry points simultaneously.
- First responder access can be provided with special access cards, given to select first responders in advance of an incident, which will allow them to enter a building in lockdown through the access control system.
- Locking systems should be configured to always allow egress. Codes for fire and life safety require it.
- Security professionals should be well versed in building codes and prevailing laws. They can coordinate with the necessary parties and advise the school administrator of requirements and options for modes of system operation.

System Integration Installation

Planning

Planning is the first step needed for installation. A documentation package should be put together that includes:

Site plans	Sketches of any planned construction
Floor plans	Emergency processes and procedures
Fire escape plans	A record of who has authorized access to the interior and exterior areas of the school
Layout drawings for existing electronic systems (noting the brands of those systems)	List of key holders
Emergency call list (for fire and security responders)	List of access control holders

Stages of Installation

Rough in – This stage is when the infrastructure is installed, including conduit and cabling

Finish – This stage involves mounting components, such as cameras and card readers, connecting them to the infrastructure wiring, and then programming the system software

Commissioning – The final stage of deployment is the system test and customer acceptance

Review - During system test, the security team should conduct a full analysis of all system functions in normal and emergency states.

Security Preparation and Awareness



Once installation is complete, the integrator should provide:

- “As built” drawings showing device locations, interconnectivity, and wiring.
- The operation and maintenance manuals for each piece of equipment installed

The school should:

- Review and revise all standing security plans (emergency drills, list of key/access card holders)
- Develop a **Security Awareness Program**

System Use and Maintenance

The school should:

- Designate clearly identified roles for Access Control, Monitoring Systems, and Surveillance

The Security Manager should:

- Conduct periodic visual inspections of both the electronic and mechanical components quarterly
- Provide routine preventative maintenance for environmental degradation.



Training

- Operators who are charged with controlling the system or monitoring its status should be provided with system training by the Integrator.
- All system users, including staff and students, **should be trained on how to use the new security system**, including routine operation and what to expect in an emergency.



Student Outcomes

Classroom Enhancement Solutions



- **Classroom enhancement solutions** is a comprehensive technology deployment designed to maintain a safe and efficient atmosphere in the classroom.
- This involves audio and video recordings that allow for prompt evaluation for student and teacher in every classroom.
- Audio and video can be viewed live and recorded to be viewed later. Past recordings can be saved for documentation in the event of an incident in the classroom.

Helps you to be Proactive

When it comes to education, being **proactive** is far more beneficial than being reactive to safety situations.

Audio and video coverage in the classroom can:

- Improve student achievement and overall academic performance
- Enhance communication between student, teacher, parent, and administrator.
- Improve accountability in the classroom, as well as records the overall efficiency of each educator



Bullying Prevention



Studies show that **21 percent** of students ages 12-18 report being bullied at school.

Audio and video recordings in the classroom can:

- Provide undeniable evidence for administration to **take-action against bullying**
- Eliminate student-teacher conflict in the classroom
- Encourage both student and teacher to remain accountable for their actions.

Can Help Minimize Drug Activity

Video surveillance cameras can help:

- Alert staff to signs of potential drug usage in which students are exhibiting strange behaviors
- Capture student interactions to identify high-risk students
- **Monitor, identify, and mitigate high-risk areas** where drug activity is common.



Jeopardy!

Equipment

Student Outcomes

General Security

Threats

Other



100

100

100

100

100

200

200

200

200

200

300

300

300

300

300

400

400

400

400

400

Any Questions???

Presented by



(888) 909-2261

Equipment - 100

Question:

_____ is made up of doors, frames, hinges, door closers, gates, locks, keys, card readers, card and token, and biometric reads software

Answer:

Access Control

Equipment - 200

Question:

A _____ is made up of display screens, video and data, and video recording devices.

Answer:

Monitoring System

Equipment - 300

Question:

A _____ is made up of cameras, special cabling, and a monitoring system

Answer:

Surveillance System

Equipment - 400

Question:

_____ can detect weapons that are brought into a building.

Answer:

Metal Detectors

Student Outcomes - 100

Question:

Audio and video recording helps schools to be _____ vs. reactive

Answer:

Proactive

Student Outcomes - 200

Question:

Audio and video recording can provide undeniable evidence for administration to take action against _____

Answer:

Bullying

Student Outcomes - 300

Question:

Video surveillance can help monitor, identify, and mitigate high risk areas where _____ is common.

Answer:

Crime, drug activity, bullying, etc.

Student Outcomes - 400

Question:

Once installation is complete, the school should develop a _____ to ensure that students and staff know security procedures and expectations.

Answer:

Security Awareness Program

Threats - 100

Question:

A student's behavior can be considered what kind of threat?

Answer:

Internal Threat

Threats - 200

Question:

Nearby prisons and local criminal activity are considered what kind of threats?

Answer:

External threats

Threats - 300

Question:

What are the 3 layers of security protection?

Answer:

Outer perimeter, building perimeter, and interior spaces

Threats - 400

Question:

_____ deters undesired activities such as “no trespassing,” “drug free zone,” or “this area is monitored by cameras.”

Answer:

Signage

General Security - 100

Question:

_____ can provide administrators with useful crime data, historical analysis, and types of crime and the frequency of crime to help them choose the right security system for their school.

Answer:

Local law enforcement

General Security - 200

Question:

The school administrator should _____ effectively throughout the planning stages of the security process to manage expectations.

Answer:

Communicate

General Security - 300

Question:

School administrators should _____ all students and staff members on how to properly use security equipment

Answer:

Train

General Security - 400

Question:

The Security Manager is a/an _____ role of the security team.

Answer:

Internal

Other - 100

Question:

A “ _____ ” is against fire code, and is a device that slips over the closer-arm of a door to prevent the door from being opened from the outside

Answer:

“Sleeve”

Other - 300

Question:

_____, also known as burglar alarms, are used for perimeter control and activate alarm warnings when a violation of the perimeter is detected

Answer:

Intrusion Detection Systems

Other - 200

Question:

_____ will provide an alert of unauthorized access to the facility.

Answer:

Motion Detection Cameras

Other - 400

Question:

What type of procurement process provides a simplified process, is compliant with all laws and regulations, offers reasonable prices, and allows access to emerging technologies?

Answer:

GSA Schedule Contract