

K-12 School Security Checklist April 2013



Appendix 1

This baseline security practices checklist is intended only as a guide; it is not a requirement under any regulation or legislation. *Please note: the below checklists may or may not directly correspond to sections specifically discussed in the "K-12 Schools Security Practices Guide;" those items without specific reference to the document do not have a corresponding section number listed in the left-most column.*

ACCESS	CONTROL		
2.2.1	The facility perimeter and areas within the facility that	YES	NO
2.2.1	require access control are well defined.		
2.2.1	The facility limits building access points.	YES	NO
2.2.1	Designated access points are monitored to control facility	YES	NO
2.2.1	access.		
2.2.1	Positive entry control systems are established (e.g.,	YES	NO
2.2.1	telephone entry control, biometric access control).		
2.2.1	Signs direct visitors to designated building entrances and	YES	NO
2.2.1	exits.		
2.2.1	Exterior doors to gyms, maintenance areas, kitchen, and	YES	NO
2.2.1	delivery areas are secured when not in use.		
2.2.1	Visitors are required to check in with the front office	YES	NO
2.2.1	upon arrival and departure.		
2.2.1	Visitors are provided with school issued identification	YES	NO
2.2.1	badges when on school grounds.		
2.2.1	Policies are in place for those with and without	YES	NO
2.2.1	appointments or official school business.		
2.2.1	Vendors and contractor personnel are escorted	YES	NO
2.2.1	throughout the facility.		
2.2.1	Background checks are conducted on all school	YES	NO
2.2.1	employees, vendors, and contractors.		
2.2.3	A key control program is established that monitors keys,	YES	NO
2.2.3	entry cards, and duplicates.		
2.2.3	Key control program is audited annually.	YES	NO
2.2.3			
BUILDIN	G EXTERIOR		
2.2.1	Policies are in place that restrict access to bus-loading	YES	NO
2.2.1	zones.		
2.2.1	Bus-loading, unloading, drop off zones and fire zones are	YES	NO
2.2.1	clearly marked.		
2.2.1	School designates areas for use of parking lots (e.g., staff	YES	NO
2.2.1	lot, student lot, visitor spaces).		
2.2.1	Parking system incorporates an identification system	YES	NO
2.2.1	(e.g., placards in windshields).		
2.2.1	Appropriate perimeter barriers or gates are installed and	YES	NO
2.2.1	secured when not in use		

	Perimeter barriers are clear to enable continuous	YES	NO
2.2.1	monitoring and to inhibit concealment of people or		
	packages.		
	Windows are locked securely.	YES	NO
	, ,, ,, ,, ,	П	П
	Window hardware and frames are regularly inspected for	YES	NO
	security weaknesses.		
	Facility has visual surveillance capability (e.g.,	YES	NO
	designated surveillance points, cleared lines of sight).	TABE C	NO
	Clear zones adjacent to buildings are free of vegetation	YES	NO
	and other obstructions.		
	Barriers are installed to protect doors and windows from	YES	NO
	small arms fire and explosive blast effects.		
	School grounds are adequately lit.	YES	NO
	Vandalism and graffiti is documented and removed.	YES	NO
	č		
	Mechanical, electrical, and other equipment are	YES	NO
2.2.1	surrounded by protective enclosures to prevent		П
2.2.1	unauthorized access.		
	Access to the roof is restricted.	YES	NO
	Access to the foot is restricted.		NO
	Constitution and the	VEC	NO
	Speed limits are posted.	YES	NO
	Covered walkways are adequately lit to ensure visual	YES	NO
	surveillance.		
	Fire hydrants are clearly visible.	YES	NO
RIII DIN	IG INTERIOR		
DCIEDI	School front office is clearly marked.	YES	NO
	School front office is cicarry marked.		
	First aid/school names office location is alcomby montred	VEC	NO
	First aid/school nurse office location is clearly marked.	YES	NO
			NO
2.2.1	Critical utility systems and equipment are secured and	YES	NO
	locked.		
	Employees are familiar and trained with how to shut off	YES	NO
	utility services.		
	A positive inventory is kept on chemicals in use or used	YES	NO
	in science classes or laboratory areas.		
	Roof access doors are secured and locked	YES	NO
	Custodial and storage closets are secured and locked.	YES	NO
		П	
	The number of containers and trashcans in hallways,	YES	NO
	atriums, and lobby areas are minimized.		
	·	YES	NO
	Unassigned lockers are secured.	1 E3	NO

	Stairwells, hallways, and restrooms are adequately lit.	YES	NO
	Enclosed stairwells are monitored, either electronically or by security personnel,	YES	NO
	Smoke detectors have vandal-resistant features (e.g., tamper alarms or protective cages).	YES	NO
	Doors and locks are in good condition.	YES	NO
	Easy access to fire extinguishers.	YES	NO
	Adequate access to first aid supplies (e.g., automated external defibrillators (AEDs)).	YES	NO
	Class III type fire doors with crash bar capabilities and automatic activation are installed.	YES	NO
	Blast fragment retention film is on windows.	YES	NO
CLASSRC	OOM SECURITY		
4.2.3	Classroom safe zones or protection areas are established.	YES	NO
4.2.2	Classroom has access to two-way communication system.	YES	NO
	All areas of the classroom are visible from the classroom door.	YES	NO
	Classroom doors can be locked from the inside.	YES	NO
4.2.3	Classroom doors with windows can be covered.	YES	NO
	Classrooms have adequate aisle space for quick exits.	YES	NO
4.2.7	Class rosters are reviewed and updated on a regular basis.	YES	NO
	Faculty and staff are assigned to check that all classrooms and bathrooms are locked after the school day.	YES	NO
	Valuable items are secured (e.g., instruments, computers, video equipment).	YES	NO
	Chemicals, poisons, and flammable materials are properly secured and stored.	YES	NO
	Fire extinguishers are inspected on an annual basis.	YES	NO
	Personnel working with hazardous materials have received appropriate training.	YES	NO
SCHOOL	CULTURE		
3	Faculty, students, and staff are all provided with security information and training.	YES	NO

	Security information and training includes information	YES	NO
	on how first responders operate to avoid hindering		
	operations.		
3	Security information and training includes training on	YES	NO
3	how to identify suspicious packages.		
	Faculty and staff have been trained to appropriately	YES	NO
	respond to and report threatening/suspicious phone calls.		
3	Faculty and staff monitor hallways, stairwells, and	YES	NO
	restrooms during school hours.		
	Students do not have access to the school without direct	YES	NO
	staff supervision.	TATE C	
	Curricula and programs aimed at preventing harmful	YES	NO
3.5	behaviors are implemented (e.g., social problem-solving,		
	life skills, anti-bullying, mentoring programs, character		
	education).	VEC	NO
	School maintains, reviews, and updates a code of	YES	NO
	conduct/school handbook. Code of conduct/school handbook contains standard	YES	NO
	definitions and procedures that identify school crime.		NO
	School has a well-developed network of service	YES	NO
3.5	providers that students can be referred to (e.g., mental		
3.3	health services)		
	Photo identification badges are issued to all faculty,	YES	NO
	students, and staff.		
	students, and start.		
COMMI	INICATION CYCTEM		
COMMU	NICATION SYSTEM Systems are installed that mayide two years	YES	NO
4.2.2	Systems are installed that provide two- way communication between faculty, staff, administrators,		
4.2.2	and security personnel.		
	Communication system is installed that provides	YES	NO
	communication system is instance that provides communication with all people at the school, including		
4.2.2	faculty, students, staff, emergency response teams, and		
	visitors.		
	Regular communication with local law enforcement and	YES	NO
4	emergency responders is established.		
4	Procedures are developed for communicating with public	YES	NO
4	and the media regarding security issues.		
4	A notification protocol is developed that outlines who	YES	NO
4	should be contacted in emergencies and how.		
	· · · · · · · · · · · · · · · · · · ·		•
REPORT	TING PROCEDURES		
	School has a single point of contact for reporting threats,	YES	NO
3.4	threatening behavior, or concerning behavior.		
2.4	The identified point of contact for reporting potential	YES	NO
3.4	threats is available 24/7.		
	There are multiple ways someone can reach the point of	YES	NO
3.4		_	
	contact for reporting potential threats (e.g., email,		
	telephone, online, in-person).	Ш	

3.4	Reporting can be anonymous.	YES	NO
	There are clear policies in place for collecting and acting	YES	NO
3.4	on information about a threatening or potentially	П	П
	threatening situation.	_	
	Policies explain how information will be handled	YES	NO
3.4	confidentially and appropriately.		
	tomiconium uno appropriatory.		<u> </u>
CECLIDI			
SECURI.	TY EQUIPMENT	VEC	NO
	Facility has security system installed (e.g., CCTV, IP	YES	NO
	cameras, digital camera integration and intrusion		
	detection and alarm system).	* TEG	MO
	Video security systems are connected to the building's	YES	NO
	emergency power supply.		
	Alarm system is connected to local law enforcement.	YES	NO
	Security camera tapes or recordings are retained for an	YES	NO
	allotted time period.		
	All emergency response equipment and supplies are	YES	NO
	checked on a regular basis.		
	School has adequate utility service capability to meet	YES	NO
	normal and emergency needs.		
	Magnetometers (metal detectors) and x-ray equipment	YES	NO
	are installed.		
SECURIT	TY PERSONNEL		T
	A school security director is designated to develop,	YES	NO
	implement, and coordinate all security-related activities.		
	School security personnel include an armed trained	YES	NO
	police officer or school resource officer.		
	School security personnel are stationed at a single	YES	NO
	school.		
	School security personnel are a visible and regular	YES	NO
	presence during school hours of operation.		
	School security personnel are deployed during normal	YES	NO
	school hours of operation and special events.		
2.2.1	Security personnel check for unauthorized vehicles in	YES	NO
2.2.1	parking lots or on school grounds.		
	Halls, common areas, and gyms are monitored for	YES	NO
	suspicious items (e.g., backpacks, briefcases, boxes).		
	Security personnel are deployed to assigned areas to	YES	NO
	regularly inspect sensitive or critical areas (e.g.,		
	auditoriums or under stages where items such as		
	weapons or explosive materials can be hidden).		
	Faculty and staff monitor hallways, stairwells, and	YES	NO
	restrooms during school hours.		
	Security personnel regularly inspect and secure doors.	YES	NO
			_

	If the building is used after school hours, security		NO
	personnel are present.		
	School safety audits are conducted on a regular or	YES	NO
	continuing basis.		
			1
CVDEDCI	ECURITY		
CIDERSI		VEC	NO
	School maintains a well-trained computer security staff.	YES	NO
	C-1 - 1 C - 1 - 1 - 1 - 1 - 1 - 1 - 1 -	VEC	
	School faculty and staff are required to use passwords	YES	NO
	and unique login information to access electronic files.	VEC	NO
	Students are required to use passwords and unique login	YES	NO
	information to access electronic files.	TATE C	NO
	Security plans for computer and information systems are	YES	NO
	established.		
	These computer and information system security systems	YES	NO
	include both hardware and software.		
	Faculty and staff are trained in safe and secure computer	YES	NO
	use.		
	Students are trained in safe and secure computer use.	YES	NO
	Cybersafety and cyberbullying programs are provided	YES	NO
	for students.		
	Computers include filters to monitor internet activity on	YES	NO
	school computers.		
	Video security system is adequately protected against	YES	NO
	hackers.		
EMERGE	ENCY OPERATIONS PLAN		
	A comprehensive school emergency operations plan has	YES	NO
4.2	been developed.		
	Plan has been developed in coordination with community	YES	NO
4	partners (e.g., local law enforcement, emergency medical		
_	personnel, and fire department personnel)		
	Plan takes into consideration numerous circumstances	YES	NO
4.2.3	and criteria for response (e.g., lockdown, evacuation,		
7.2.3	shelter-in-place).		
	Plan contains an updated map of the school's floor plan	YES	NO
4.2	that includes room numbers, evacuation routes, and		
4.2	utility shut offs.		
	Plan defines roles and responsibilities—that is, creates an	YES	NO
	organizational system (e.g., school security commander,		
4.2.1	public information officer, etc.)		
4.2.1	*Consider following Incident Command System (ICS)		
	structure ¹		
	Plan contains a method for reporting incidents internally	VEC	NO
422	1 0	YES	_
4.2.2	to faculty, students, and staff (e.g., mass notification		
	system).		

 $^{^{1}\} http://www.fema.gov/incident-command-system$

120	Plan contains a method for reporting incidents externally	YES	NO
4.2.8	to media, families, neighbors, and the community.		
	Plan contains directions that provide for the needs of	YES	NO
4.2.4	students, staff, and visitors with disabilities and other		
	functional and access needs.		
4.2.5	Plan considers necessary equipment and supplies to	YES	NO
4.2.3	respond to a crisis.		
4.2.6	Plan contains common vocabulary.	YES	NO
4.2.0			
4.2.7	Plan includes an accountability system that accounts for	YES	NO
4.2.7	all faculty, students, staff, and visitors.		
	Plan contains a parent reunification system that ensures	YES	NO
4.2.7	students are only released to authorized individuals after		
	an incident.		
	Plain contains action checklists for teachers,	YES	NO
5	administrative staff, and other staff located throughout		
	the school to follow during incident response.		
	Plan includes components for post-incident	YES	NO
6	response/recovery (e.g., stress management, mental		
0	health services, infrastructure restoration, post-incident		
	evaluation, business continuity plans etc.)		
4.2	Plan is reviewed and updated on an annual basis.	YES	NO
4.2			
4.2.9	School conducts regular exercises/drills of emergency	YES	NO
4.2.9	plans.		

THREAT ASSESSMENT TEAM				
1. Does your school have a threat assessment team? (If no, please skip the questions in this section)	YE:	SS NO		
2. Who is on the threat assessment team? (Check all that apply)	o Memio Memio Investo office school of the s	tal health professional(s) (e.g., school hologist, clinical psychologist, asic psychologist) lance counselor(s) hers		

3. Do members of the threat assessment team rotate?	YES □	NO
3a. If yes, how often do they rotate? (Check all that apply)	 Weekly Monthly Quarterly Yearly Other (please spectrum) 	cify)
4. Does the threat assessment team receive training?	YES	NO
4a. If yes, how often do they receive training? (Check one)	 Weekly Monthly Quarterly Yearly Other (please special)	cify)
4b. What topics are covered in threat assessment team trainings (Check all that apply)	o Public Awareness o Threat Manageme o Threat Investigati o Prevention o Mental Health Co o Legal/Policy Con o Privacy Concerns o Other (please spec	ent ons oncerns cerns
4c. How are threat assessment trainings conducted? (Check all that apply)	 Presentations Hands on experience/role playing/scenarios Other (please specify) 	
5. Does your school have a single point of contact (phone number, email address, etc.) for reporting threats, threatening behavior, or concerning behavior?	YES	NO
5a. If yes, is this point of contact for reporting potential threats available 24/7?	YES	NO
5b. What are the ways someone can reach the point of contact for reporting potential threats? (Check all that apply)	 Email Telephone In person Online Other (please spector) 	cify)

6. If there is a central point of contact for reporting potential threats, does one person manage this point of contact or does a group manage it? (Check one)	 One person manages the point of contact A group manages the point of contact (If a group manages the point of contact, skip to question 7.) There is no central point of contact (If there is no central point of contact, skip to question 7.)
6a. If one person manages the point of contact for reporting potential threats, does this person rotate?	YES NO
6b. If yes, how often does this person rotate? (Check one)	 Weekly Monthly Quarterly Yearly Other (please specify)
7. Does the threat assessment team have clear policies in place for collecting and acting on information about a threatening or potentially threatening situation (If no, skip to question 10.)	YES NO
8. Does the policy about threat assessment inquiries include information on the following: (Check all that apply)	 Purpose and scope of the policy Role of educators and threat assessment in relation to the role of law enforcement officials Identity of and delegation of authority to school officials concerning determination that a threat assessment inquiry or investigation should be pursued Definition of the threshold of concern for initiating inquiry or investigation Types of information that can/should be gathered during a threat assessment inquiry or investigation Designation of an individual or group responsible for gathering and analyzing information on groups/individuals Steps or procedures that should be followed from initiation to completion of the threat assessment inquiry
9. Does the policy specify certain behaviors of concern or provide examples of behaviors that would merit a referral to the threat assessment team?	YES NO

9a. If yes, list those behaviors that would merit a referral to the threat assessment team	
10. What types of information are generally gathered during an inquiry: (Check all that apply)	 Facts that drew attention to the student, situation, or target Information about the student Identifying information Background information Current life information Information about attack related behaviors in which the student has engaged The student's motives The targets that are in danger of violence None of the above Other (please specify)
11. How does the threat assessment team actively encourage school community members (students, parents, faculty, staff, administrators, etc.) to report knowledge of potential threats? (Check all that apply)	 Public awareness campaigns (posters, announcements) Student assemblies In-class lectures/presentations Student-teacher conferences Parent-teacher conferences Newsletters Other (please specify)
12. How does the threat assessment team make school community members (students, parents, faculty, staff, administrators, etc.) aware of the general steps and timeline of the inquiry process? (Check all that apply)	 Public awareness campaigns (posters, announcements) Student assemblies In-class lectures/presentations Student-teacher conferences Parent-teacher conferences Newsletters Other (please specify)
13. Does the threat assessment team explain how information will be handled confidentially and appropriately?	YES NO

Photo Sources

Picture 1: Brach, Patricia, FEMA Photographer. Houston, Texas. March, 9, 2009. http://www.fema.gov/photodata/original/40283.jpg.

Picture 2: Risk Management Series: Design Guide for Improving School Safety in Earthquakes, Floods, and High Winds, FEMA P-424 / December 2012, Federal Emergency Management Agency, page 151. http://www.fema.gov/library/viewRecord.do?id=1986

Picture 3: Safe Havens International http://www.safehavensinternational.org/

Picture 4: Jun, Elissa, FEMA Photographer. Joplin, Missouri. August 19, 2011. http://www.fema.gov/photodata/original/50245.jpg.

This document was developed by the Office of Infrastructure Protection, DHS, to provide information to K-12 school personnel assigned with the responsibility of assessing school security practices to foster safer and more secure school communities. The information herein is not all inclusive. This guide presents an overview of K-12 school security practices. School administrators and legal counsel should work together to ensure that these practices are employed in a manner consistent with legal requirements.

Note: Information presented here is subject to copyright laws and other terms of use as set forth in the respective references