Security Preparedness *Resource Toolkit*

How Does Your Plan Hold Up?

CHRISTIAN BROTHERS SERVICES

SORENSEN WILDER & Associates

Specializing in Safety & Security Solutions

Table of Contents

Introduction
How to Use this Toolkit 3
Section 1 - Threat Assessment Team
Assemble a Planning Team 4
Educate the Team 5
Determine Goals and Objectives 5
Identify Program Weakness and Threats 5
Develop a Plan of Action 6
Accomplish Goals and Objectives 6
Implement, Test and Maintain 6
Threat Assessment Team/Active Shooter Committee 7
Functions and Responsibilities of an Active Threat Team 8
Threat Assessment Team/Agenda 9
Objective and Goal Tracking Form 9
Section 2 - Security Preparedness Self-Assessment
How to Use and Complete the Assessment 10
Assemble your Review Team 10
Preparations 10
Assessment Scoring 11
Your Organization's Assessment 12
Hiring and Human Resources 13
Security and Identification 14
Staffing and Organizational Culture 15
Policy Review 16
Security Awareness Policies 17
Training: Security 17
Training: Physical Protection of People and Property 18
Training: Employees and Volunteers 19
Access Control 20
CCTV and Video Storage 21
Alarm Systems 22
Communication Systems 22
Lobby Management and ID Systems 23
Outside Grounds 23
Section 3 - Security Inspections
Introduction 24
Doors/Windows/Loading Docks/Skylights (checklist) 25
Outside Physical Security (checklist) 29
Inside Equipment/Lighting (checklist) 32
Section 4 - Staff Training and Awareness
Types of Training to Consider 33
The Four Outs for an Active Shooter 34
Ongoing Awareness Programs 35
Active Shooter Training and Awareness Schedule 36
Section 5 - Disaster Recovery Planning
Introduction 37
Section 6 - Sample Policies
Introduction 38
Active Shooter Response 39
Standard of Conduct and Work Rules 41
Physical Security 42
Whistleblowing 44
Workplace Violence 45
Workplace Security 46

How to Use this Toolkit

We developed this Toolkit to help your organization apply appropriate controls to manage workplace violence, security and active shooter/active threat situations. In addition, the documents aim to guide you in creating a threat assessment team and in providing your staff with training and awareness.

By using the Toolkit, you can create a planning process for your organization that will allow you to recognize and assess threats. An included self-assessment on security preparedness and a physical security self-inspection checklist will help you ensure your organization is taking the proper safety measures.

The Toolkit also contains sample documents that you can modify according to your needs, including sample policies for violence in the workplace, standard of conduct and work rules, whistleblowing, physical security, and active shooter response.

It is our goal that this Toolkit will provide the most up-to-date knowledge on security preparedness best practices to ensure your organization and its employees have a safe work environment.

Christian Brothers Risk Solutions would like to thank our consulting partners at Sorensen Wilder & Associates for their support and contributions to this resource tool kit. Sorensen Wilder & Associates provided consultation, materials, content and use of their trademarked terms; “Get Out, Hide Out, Keep Out, Take Out” highlighted in sections 4 and 6.

Section 1

Threat Assessment Team

Once your organization has committed itself to the development of an ongoing threat assessment program, logically, the next steps are to determine who will develop, implement and maintain the overall program. Some organizations may create a unique committee or team to manage the program. Other organizations look to assign this important function to the safety, risk management or business continuity committees. Whatever your organization decides, the steps involved with planning and developing a program to address this risk are the same.

The following seven steps will help your organization develop a threat assessment team and understand team-member functions:

1. Assemble a planning team:

Case studies find a team approach that includes interested representatives from across the organization to be a sound method. The team should be small enough to allow for good communication between team members but large enough so there is not too much burden placed on any one person. The following are suggestions of individuals to make up your team:

Internal Staff

- Individuals who are interested in participating (assigning staff who may not be interested could negatively affect the team)
- Individuals who have had experiences outside the organization, such as: military, law enforcement, firefighter, security, first aid responders, etc.
- Individuals who have been or are on other internal committees or teams such as a risk management team, safety committee, business continuity team, emergency operation planning team, etc.
- Representatives from various departments/divisions such as human resources, security, safety, information technology, facilities, operations, legal, media relations, finance, nursing, etc.
- Representative(s) from the religious community

External team members are usually members who will help advise and assist with the development of your organization's programs. These members rarely attend every meeting but rather the committee will reach out to them at times to get guidance throughout the process and various steps. Identify and introduce the following suggestions of external team members to the team:

External Team Members

- Security expert/consultant
- Local police
- Local fire department
- Local FBI
- Legal
- Trustee/Board member
- Community services
- Insurance representative
- Representatives from nearby organizations

As with any new team, a structured approach for running the team needs to be developed. This structure, at a minimum, should include roles and responsibilities such as chairperson or secretary, a meeting schedule, duration of meetings, etc. As the team grows, additional roles and responsibilities may be added, such as assigning someone to manage the training or someone to manage the ongoing awareness of how to identify potential threats and react during an active threat event.

2. Educate the team:
Each team member needs to understand the "who, what, where, when, why and how" of active threat incidents to help them see the larger picture. This step is important, though it should not slow the team down from moving on to the next step. You can find a variety of different types of training offered in many different formats. The committee should consider looking into the following types of programs offered: webinars, online training and even local live workshops. If the committee is just starting out, it might be beneficial to begin with a live webinar or workshop. These types of programs tend to be better as the audience gets the benefit of hearing questions asked and answers given by the presenting experts.

Unfortunately, not every team member may be able to attend a training session. To account for this, it is good practice to include an agenda item for each subsequent meeting covering what was learned from training and how this knowledge may apply to the team's development of the program.

Live on-site training is often the best, since the expert providing the training can actually customize the program to meet the organization's ministry and exposures existing at the program. Various divisions of the Department of Homeland Security offer training videos.

Before moving to the next step, the team might also want to do some additional research in obtaining sample plans, planning guides, checklists and other resources. Looking for and reviewing resources found is another good way to mentally help individuals understand their ultimate goal and slowly learn more about what organizations should do prior, during and after a threat event. Multiple, trusted governmental sites often offer free materials that are easily accessible online. For starters, check out the Department of Homeland Security at **www.dhs.gov**; Federal Bureau of Investigation (FBI) at **www.fbi.gov** or the Federal Emergency Management Agency at **www.fema.gov.**

3. Determine goals and objectives:
To begin, the team needs to develop a list of initial goals and objectives with target dates. These initial items usually will focus on the overall direction of the team. There also could be multiple goals developed to accomplish one objective. As meetings occur and activities of the team move forward, additional objectives and goals will be developed. Prioritize these additional items and the target dates assigned. We have developed a form and included it in this section to assist the team in tracking its objectives and goals.

4. Identify Program Weakness and Threats:
We have included a resource in this toolkit to help the team identify weakness within the organization's existing program and possible threats to the organization. However, this resource is not all inclusive. Outside team members, such as a security consultant may need to be brought in to develop a more comprehensive list of threats and offer suggestions on how to put these threats in check. Some local police departments even offer an active shooter physical security assessment service to community businesses free. **Caution** Free services can be very helpful but can be limited in nature. The free service might not include how best to manage residents within a nursing home, students within an educational ministry, sisters in a convent or evaluate an organization's technological programs/equipment maintained by the IT department. The team may need to turn to an outside security consultant to help them identify weaknesses and threats to these special concerns.

A free resource available to everyone is a FBI document on developing emergency operations plans. Use this document for not only active shooter program development, but for other program development, such as a gas leak or fire. Download the document at: **https://www.fbi.gov/file-repository/active-shooter-guide-for-businesses-march-2018.pdf/view**. This guide for business is an excellent resource to help walk the team through each step of this process. This document suggests identifying at least three goals to accomplish one objective.

Team brainstorming is another good method of identifying potential threats to the organization and should be used to help further develop the list of potential threats. Some examples of scenarios most commonly identified during this brainstorming session are:

- Employee's family member, divorcee, or significant other comes to the organization with intent to harm the employee and anyone else around
- Employee is terminated and comes back to the organization with intent to harm other employees

Keep in mind, as the team develops additional objectives and identifies additional threats, goals to address these concerns need to be prioritized and added to the overall master list of objectives.

5. Develop a plan of action:

A plan or process needs to be developed for each goal to accomplish each objective. These plans need to include the "who, what, where, when, why and how." Who is assigned to complete the goal and who does this goal affect? What resources are going to be needed? Where is this activity going to take place? When will the training be conducted? Why is this goal so important? How will this be communicated to other employees or how much will the new equipment cost? Some plans of actions might be put on hold for a later date so the team can focus on higher priority items or situations that are more likely to occur. If the team tries to address a long list of objectives all at once, the team can become overwhelmed and quickly burn out. These teams are very functional but everyone on the team also has other jobs. Developing an active threat program should not monopolize 100 percent of one's time.

6. Accomplish goals and objectives:

After a procedure or policy has been written, it then needs to be approved. Keep in mind some polices and some procedures may need to be looked at by an attorney to ensure it complies with local/state/federal law. This also may be the case for specific procedures involving vulnerable clientele like nursing home residents or students. For this situation, a security consultant may be needed to review the plan/procedure if they did not create it or help develop it. Unfortunately, this step could take some time as it depends on how the approval process is set up and to whom the team reports. Once the policy/procedure has been submitted for approval or the funding request has been submitted to purchase new security equipment, it should be tracked and followed up upon at the next meeting to check status. This activity should be documented in the Objective and Goal forms.

7. Implement, test and maintain:

After approval is received, it is time to implement. Implementation should begin with communication. Depending on what you are implementing, you may need to inform all employees as to the overall implementation plan. Communicate general guidelines for when and how implementation will begin and end. Example: If the organization is going to install security cameras, communicate with

employees when the project is going to start/end and promote how this new equipment is going to help better secure the organization, the employees and the overall ministry. Another example could be employee training. Provide communication to employees explaining why training is to be provided, who is to receive the training and when to expect training to start, etc. Remember, a good implementation strategy can help gain employee buy-in and make the implementation go smoothly.

After implementation of the policy, procedure or installation of equipment, the next steps are to test and then maintain the systems. Policies and procedures are only as good as the paper upon which they are printed. Without testing to see if they work or if they are being followed, an organization will not know if their hard work will pay off or if there are areas that need fixing. There are many ways to test the system whether it is a live test or a table-top exercise. These types of tests/drills/exercises should be done after any new change in the system and on a regular basis. Finally, once a year, the team should review the policy/procedures to see if any changes are needed to meet the demands of the organization.

Threat Assessment Team

The authority of the team will vary from one company to another and generally depends on its responsibilities. Much depends upon the size of the organization, the type of problems faced, and the quality of employer/employee relations. The following is presented as a suggested order of business that may be adopted for the Threat Assessment Team meetings in general:

1. **Call to Order** - The meeting should be called to order promptly at the appointed time.
2. **Roll Call by the Secretary** - Names of members and others present should be recorded. Members who cannot attend should notify the secretary in advance and the reasons for absence should be noted in the minutes and arrange for a substitute during absence.
3. **Introduction of Visitors**
4. **Minutes of the Previous Meeting** - should be read and corrections and/or additions made.
5. **Unfinished Business** - All matters on which definite decisions have not been made are brought up for needed action.
6. **Objectives and Goals –** The person assigned to accomplish the goal should review and summarize objectives and goals.
7. **Review of Policy and Procedure –** After an organization's active threat program has been implemented, policies and procedure should be reviewed on a regular basis. These can be done all at once or spread out over the course of a few meetings.
8. **Active Threat Education** - When desirable, the chairperson should request a member to speak at the next meeting. The subject to be discussed should be reviewed with the management and approved.

9. **Activities** - The chairperson may wish to appoint subcommittees to arrange for:
   a. Active threat employee awareness suggestions
   b. Development of table-top exercises
   c. Monitoring of changes in industry standards or watching for new products that could be beneficial to the organization's program
   d. Review of any active threat employee suggestions

10. **Adjournment** - Minutes should be taken, prepared and circulated by the secretary, after approval by the chairperson. The minutes are of great importance since they are often sent to others besides committee members, especially top management. The minutes must record accurately all decisions made and actions taken, since they serve to keep management informed of the group's work and as a follow-up tool.

The following is a typical active threat team structure and their functions:

A. Chairperson's Duties:

1. Notify members of meeting
2. Arrange meeting/program
3. Schedule and notify committee members of next meeting
4. Arrange for a meeting place
5. Review previous minutes and materials prior to meeting

B. Secretary's Duties:

1. Distribute minutes
2. Record status of objective and goals

C. Members' Duties:

1. Attend all meetings
2. Contribute ideas and suggestions for improvement of safety
3. Set a positive example in the workplace for others to see
4. Be observant of others actions as it relates to possible workplace violence

Functions and Responsibilities of an Active Threat Team

A. Discuss active threat related policies and recommend their adoption by management

B. Identify possible red flags to violence and report them to management

C. Assist management to implement recommendations or to improve enforcement of existing rules

D. Teach active threat awareness to all personnel by:

1. Generating and maintaining the interest of workers and convincing them that their cooperation is needed to prevent an incident
2. Providing employees an opportunity for free discussion of concerns and preventive measures
3. Helping management evaluate a variety of educational and communicative suggestions

Agenda

Date: _____

1. Roll Call and Introduce Visitors
2. Approval of Last Meeting Minutes
3. Review Unfinished Business
4. Review Status of Objectives and Goals
5. Review of Policies and Procedures for Revisions
6. Review of Any Inspection Reports
   - *Insurance*
   - *In-house Inspections*
   - *External Security Consultant*
7. New Business
8. Education
9. Adjournment

Objective and Goal Tracking Form

Objective Name: _____

Objective Description: _____

_____

(List goals below to accomplish the objective above)

	Description of Goal	Who is Responsible	Target Date	Cost	Priority: High Medium, Low	Status/Progress Summary
Goal 1						
Goal 2						
Goal 3						
Goal 4						
Goal 5						

Section 2

How to Use the Security Preparedness Self-Assessment

How to Use and Complete the Assessment:
This section will walk you through how to assess your organization's current level of preparedness should an active threat or workplace violence situation occur. This assessment should help you identify strengths and vulnerabilities as well as "chinks in the armor" that you should address as a preventative measure.

The assessment categories are assembled in the "P2T2"® format, which identifies security areas regarding **People, Policies, Training and Technology**. There are additional categories to help you assess areas of concern as it pertains to a building's physical facilities and preparations for a post-event.

Assemble your Review Team:
It is recommended that you use a team or committee approach to utilize this assessment. A team approach will provide more thorough background knowledge of the organization's overall security policies and procedures. Each person should be confident in their abilities and encouraged to be open and honest in their opinions during the process. Each person should be willing to embrace improvements and recommendations of the team. (See Section 1 for assistance with developing the review team or committee.)

Preparations:
To prepare for the review, identify the following items and bring them to the assessment meeting. These items will assist the team as they review and discuss each line item of the checklist. These items are:

- Organizational charts
- List of standard hiring questions and reference check procedures
- Policies and procedures
  - Security
  - Workplace violence
  - Weapons
  - Lockdown
  - Shelter in place
  - Visitor management
  - Essential emergency contacts
  - Emergency situations (such as fire, bomb threat, weather, etc.)
  - Use of force
  - Domestic violence
  - Key cards/keys/FOB distribution and control
  - Process for storing and retrieving security camera data
- Mass communication systems access management
- Security vendor contracts
- List of vendors
- List of standard employee training programs provided and their frequency

Section 2

How to Use the Security Preparedness Self-Assessment

Assessment Scoring:
Each question on the assessment is worth a maximum of five points and for each question's row there are two scoring columns. The first column is the possible score column. This column will have a score of five. However, if the question is one that may not be applicable, you can change the total points in this column to a zero. If you are unable to change this number then the question is applicable and would be five points. The second column will list your selected score from one through five. However, for some questions you may only be able to select a one or five. If the question in the row is not applicable to your facility, mark a zero for both the "Possible Score" and the "Actual Score." When selecting your score, use the scoring chart below as a guide:

Scoring Chart

Score	Represents
1	Never / Incomplete / Needs to be done
2	Rarely / In planning stages / Should be done
3	Infrequently / Not as often as necessary / Done, but not often
4	Completed, but needs improvement / Satisfactory
5	Point of focus / Important / Completed regularly / Excellent

The assessment on the following pages is only a sample. The actual fillable assessment is available upon request from Christian Brothers Risk Management Services by e-mailing Jeff Harrison, Director of Risk Control Services at jeff.harrison@cbservices.org.

Section 2

Security Preparedness Self-Assessment

Date: _____

Building/Site Name: _____

Building/Site Address: _____

Assessment Team Member Names: _____

_____

_____

Your Organization's Assessment

	Possible Score	Actual Score
Hiring and Human Resources	35	0
Security and Identification	35	0
Staffing and Organizational Culture	35	0
Policy Review	60	0
Security Awareness Policies	25	0
Training: Security	15	0
Training: Physical Protection of People and Property	40	0
Training: Employees and Volunteers	45	0
Access Control	35	0
CCTV and Video Storage	45	0
Alarm Systems	5	0
Communication Systems	20	0
Lobby Management and ID Systems	20	0
Outside Grounds	20	0
	435	0
	Total Possible Score	Total Actual Score

Section 2

Security Preparedness Self-Assessment

Hiring and Human Resources	Possible Scoring	Actual Scoring	Comments
Do you have a dedicated Human Resources Department?	5		
Past employer interview completed?	5		
Full criminal background check: Local/State/Federal on all employees and volunteers completed?	5		
Drug testing conducted on employees for pre-employment/ random/post-accident/reasonable suspicion?	5		
Psychological exam conducted during pre-employment?	5		
Neighbor/relative/domestic partner references checked?	5		
Do you have a team or committee that addresses workplace violence?	5		
Ministry- & State-Specific Questions *These questions are specific to healthcare and education ministries and may not pertain to your ministry.*			
Do initial hiring questions include domestic violence?			
Medical history absentee/illness/injury/claims reviewed?			
Sex-Child Abuse Registry checks conducted on volunteers if full criminal background checks not conducted?			
Total Possible Score ►	**35**	**0**	**◄ Total Actual Score**

Section 2

Security Preparedness Self-Assessment

Security and Identification	Possible Scoring	Actual Scoring	Comments
Is there an employee who is responsible for the facility's security program?	5		
Does the facility have a dedicated security staff?	5		
If security staff contracted, is there a formal contract with a security company that will indemnify the organization from the security staff's actions, along with requiring the contractor to have appropriate coverage limits?	5		
Is the security team armed and State-certified trained on the weapons they are using?			
Is it mandated that the security team wear bullet resistant vests?			
Are the security officers additionally equipped and certified on the use of that equipment?			
Do the security officers patrol the exterior?	5		
Are visitors required to display ID badges?	5		
Do all employees wear picture ID badges?	5		
Do employees register their vehicles for employee parking?	5		
Do visitors register their vehicles upon parking?			
Ministry- & State-Specific Questions *These questions are specific to healthcare and education ministries and may not pertain to your ministry.*			
Are residents/students/religious involved in the employee evaluation process?			
Do residents/students/religious have an established and scheduled residents/students/religious committee?			
Are students required to wear school ID badges?			
Total Possible Score ►	**35**	**0**	**◄ Total Actual Score**

Section 2

Security Preparedness Self-Assessment

Staffing and Organizational Culture	Possible Scoring	Actual Scoring	Comments
Is there a consistent concern for Workplace Safety and Security?	5		
Does administration share the appropriate awareness?	5		
Do employees have a means to report security concerns?	5		
Does consistent training and policy reflect the appropriate level of concern for workplace safety and security?	5		
Is there a formal process to report security issues?	5		
Is there a contingency plan for mass call-off?	5		
Are keys/ID/passwords returned at term/separation?	5		
Ministry- & State-Specific Questions *These questions are specific to healthcare and education ministries and may not pertain to your ministry.*			
Is there a formal process for residents/students/religious to report security issues?			
Total Possible Score ►	**35**	**0**	**◄ Total Actual Score**

Section 2

Security Preparedness Self-Assessment

Policy Review	Possible Scoring	Actual Scoring	Comments
Are all security, violence, and weapons policies reviewed by a committee annually?	5		
Has the Five Stage Development Process been identified? Stage One: Needs Analysis Stage Two: Research Stage Three: Drafting/Consultation Stage Four: Approval/Communication/Implementation Stage Five: Maintenance and Review	5		
Are there sufficient policies in place for emergency situations, e.g.,			
Fire?	5		
Bomb?	5		
Severe Weather?	5		
Hazardous Materials Leak?	5		
Utility Loss: Water/Gas/Power?	5		
Workplace Violence?	5		
Active Shooter?	5		
Domestic Violence Threat?	5		
Employee Illness Considerations?	5		
Written Visitor Management?	5		
Ministry- & State-Specific Questions *These questions are specific to healthcare and education ministries and may not pertain to your ministry.*			
Evacuation of Residents: MOU/Transfer Documentation?			
Shelter In-Place Considerations/Surge Evac. Acceptance?			
Elopement/Missing Person?			
Do residents/students/religious help provide comments to emergency situational procedures and policies?			
Total Possible Score ►	**60**	**0**	**◄ Total Actual Score**

Section 2

Security Preparedness Self-Assessment

Security Awareness Policies	Possible Scoring	Actual Scoring	Comments
Are there regularly scheduled committee meetings?	5		
Is there an Employee Domestic Violence Reporting Policy?	5		
Is there a "See Something, Hear Something, Say Something" Policy?	5		
Is there a Use of Force Training and Policy?	5		
Is there an Aggression Management/De-escalation Policy?	5		
Ministry- & State-Specific Questions *These questions are specific to healthcare and education ministries and may not pertain to your ministry.*			
Is there a "See Something, Hear Something, Say Something" Policy for residents/students/religious?			
Total Possible Score ►	**25**	**0**	**◄ Total Actual Score**

Training: Security	Possible Scoring	Actual Scoring	Comments
Are Security Officers certified in Verbal De-escalation?			
Are non-security staff utilized for security (Maintenance)?	5		
Have non-security staff been trained for security purposes?	5		
Are employees trained in what to look for (Security Awareness)?	5		
Ministry- & State-Specific Questions *These questions are specific to healthcare and education ministries and may not pertain to your ministry.*			
Have residents/students/religious been trained on facility security awareness?			
Total Possible Score ►	**15**	**0**	**◄ Total Actual Score**

Section 2

Security Preparedness Self-Assessment

Training: Physical Protection of People and Property	Possible Scoring	Actual Scoring	Comments
Are all employees trained in the following areas, e.g.,			
Bloodborne Pathogens?	5		
First Aid/CPR/Choking/AED?	5		
When and where to rapidly evacuate the facility depending on circumstance?	5		
When and where to hide in various locations?	5		
How to secure Hide Areas to keep the aggressor out?	5		
How to select and use weapons of opportunity?	5		
Avoid using the elevators during an active threat?	5		
Do NOT pull the fire alarms during an active threat?	5		
Ministry- & State-Specific Questions *These questions are specific to healthcare and education ministries and may not pertain to your ministry.*			
Are residents/students/religious trained on the same procedures as employees?			
Total Possible Score ►	**40**	**0**	**◄ Total Actual Score**

Section 2

Security Preparedness Self-Assessment

Training: Employees and Volunteers	Possible Scoring	Actual Scoring	Comments
Are all employees trained annually on various emergency drills and specific actions applicable to their job assignments, e.g.			
Severe Weather?	5		
Hurricane?			
Tornado?	5		
Flood/Mudslide?			
Earthquake/Volcano/Tsunami?			
Snow Storm?			
Fire/Evacuation?	5		
Active Shooter/Hostage?	5		
Are these trainings documented and signed off by employees?	5		
Are emergency drills conducted as a table-top exercise annually?	5		
Are employees trained on the media disclosure policy annually?	5		
Do the emergency trainings include the media spokesperson?	5		
Are all employees trained in the security awareness policy?	5		
Ministry- & State-Specific Questions *These questions are specific to healthcare and education ministries and may not pertain to your ministry.*			
Are lockdown drills conducted regularly?			
Are residents/students/religious trained on the same procedures as employees?			
Total Possible Score ►	**45**	**0**	**◄ Total Actual Score**

Section 2

Security Preparedness Self-Assessment

Access Control	Possible Scoring	Actual Scoring	Comments
Does the facility use any form of access control listed below, e.g.,			
Keyed locks (Proprietary/General)?	5		
Keypad Control?			
Electronic Access Control?			
Card/FOB/Biometric?			
Are all employees granted the same access levels?	5		
Are some employees on limited-hours access?	5		
Are the denied access logs reviewed daily?	5		
Are there separate entrances for employees?	5		
Are there procedures for deliveries, e.g., food, supplies, equipment, mail, etc.?	5		
Are there areas identified around the facility for authorized personnel only?	5		
Ministry- & State-Specific Questions *These questions are specific to healthcare and education ministries and may not pertain to your ministry.*			
Are residents/students/religious informed of the areas they are authorized to enter?			
Total Possible Score ►	**35**	**0**	**◄ Total Actual Score**

CCTV and Video Storage	Possible Scoring	Actual Scoring	Comments
Are there cameras placed throughout the facility at the following locations:			
Entrances/Exits?	5		
Strategic Exterior Locations?	5		
Loading/Receiving Docks?	5		
Reception Areas?	5		
Hallways?	5		
Storage Rooms?	5		
Are all cameras monitored by a person?	5		
Can live video feeds be viewed from outside the building via computer?	5		
Is there video storage available for:	5		
0 - 24 hours? = 1 point 1-7 day(s)? = 2 points 8-14 days? = 3 points 15-29 days? = 4 points 30 plus days? = 5 points			
Total Possible Score ►	**45**	**0**	**◄ Total Actual Score**

Section 2

Security Preparedness Self-Assessment

Alarm Systems	Possible Scoring	Actual Scoring	Comments
Are there exterior alarm stations in parking areas?			
Are there duress/panic alarms at strategic locations?			
Are there emergency alarms at strategic locations?			
Are all alarms tested and documented monthly?	5		
Ministry- & State-Specific Questions *These questions are specific to healthcare and education ministries and may not pertain to your ministry.*			
Are doors equipped with hold-open alarms?			
Total Possible Score ►	**5**	**0**	**◄ Total Actual Score**

Communication Systems	Possible Scoring	Actual Scoring	Comments
Does the facility have a mass communication system?	5		
Is the communication system updated monthly/ onboarding/termination?	5		
Is the communication system internet-based?	5		
Does the communication system include all employees/ Administration/Corporate?	5		
Ministry- & State-Specific Questions *These questions are specific to healthcare and education ministries and may not pertain to your ministry.*			
Does the communication system include resident family contacts?			
Does the communication system include residents/students/religious?			
Total Possible Score ►	**20**	**0**	**◄ Total Actual Score**

Lobby Management and ID Systems	Possible Scoring	Actual Scoring	Comments
Are visitors required to sign in?	5		
Are Government ID cards scanned?	5		
Is there a list of banned or potentially violent persons available?	5		
Are ID systems and picture name badges mandated for all employees?	5		
Total Possible Score ►	**20**	**0**	**◄ Total Actual Score**

Outside Grounds	Possible Scoring	Actual Scoring	Comments
Is there a procedure to inspect trees and shrubs for security concerns?	5		
Is there a procedure to inspect areas of concern lending opportunity to building access?	5		
Is outside lighting inspected for proper lighting of parking areas and walkways to building?	5		
Are the procedures to conduct security inspection at various times of the day at various times of the year?	5		
Total Possible Score ►	**20**	**0**	**◄ Total Actual Score**

Section 3

Security Inspections

Security inspections conducted on a regular basis will help your organization stay on top of possible occurring or reoccurring weaknesses. Over time trees and scrubs will grow, doorjambs will get loose, door hinges will bend, parking lot lights will burn out and equipment will eventually wear and slowly fail. Regularly conducted inspections can help identify these weaknesses before issues occur and allow the organization some time to repair and/or upgrade these broken systems to better protect the ministry.

It is recommended that you conduct a formal security inspection on a quarterly basis. This means a documented activity assigned to an individual or a committee held responsible for conducting and completing a final report for management. It does not mean these formal inspections should replace the everyday observations and reports made by any employee or volunteer working at your ministry.

Included in this toolkit (pages 25-32) is a sample "Security Self-Inspection Checklist." This resource is not all-inclusive but is rather a tool that can be customized by you to meet your organizational needs. The purpose of the checklist is to provide a starting place for organizations to begin in the development of a customized weekly/quarterly/semiannual/annual security inspection program for the facility and property. This checklist includes various physical security items requiring inspections. As an organization's buildings and property change, update the checklist at least annually to include any new facility features or activities.

Some organizations may have multiple buildings on one piece of property. If this is the case, you should consider developing customized checklists or a separate checklist for each building. Completing separate checklists for each building could help in the management of the formal documentation process/procedure.

Completing an inspection is only the first part of any inspection procedure. The second step of the process needs to include a formal follow-up that is tracked. You should not allow areas needing attention to fall through the cracks. Identifying a concern, but not correcting the problem, can put your organization at a security and liability risk. Set up every area that needs attention on a corrective plan and track each one until it has alleviated the concern.

Once you address the inspection and the areas of concern, you can provide a formal report to management.

Section 3

Security Inspections

The purpose of this checklist is for organizations to use this information to develop a customized weekly/quarterly/semiannual/annual security checklist for the facility and property. This checklist includes various physical security items requiring inspection, but we recommend reviewing your checklist annually to include new, potential security concerns.

Date: _____ Time: _____ ☐ A.M. ☐ P.M.

Weather Conditions: _____

Building/Site Name: _____

Building/Site Address: _____

Inspector's Name: _____

Inspector's Phone/Email: _____

Doors • Windows • Loading Docks • Skylights			
Are employee entrance and exit doors locked?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Is employee entrance and exit door panic-bar hardware in good repair and tested to be operable?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			

Doors • Windows • Loading Docks • Skylights *(continued)*			
Are other exit doors locked and panic hardware in good repair?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Do exit doors self-close to a locked position?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Have non-security door wedges been removed, or are not present?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Are there any signs of damage or forced entry on door locks, hinges, or any other part of the door?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Do all visitor/client entrance doors all clear visibility from the entrance to the parking lot/street?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Are doors on the loading docks locked when deliveries are not being unloaded?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			

Doors • Windows • Loading Docks • Skylights *(continued)*			
Are overhead garage doors locked when deliveries are not occurring?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Are window locks in good repair, and have they been tested to be operable?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Are window surfaces clear of coverings so as not to block the view to the outside or inside? (Coverings should not exceed more than 10% of the window surface.)			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
If the windows have closable blinds, do the blinds remain in the open position when the facility is closed?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Are windows locked, even windows that may be open for ventilation?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Are exterior window safety guards covering windows in good repair?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			

Doors • Windows • Loading Docks • Skylights *(continued)*			
Are skylights, roof hatches, ventilation grills secured to prevent unauthorized entrance?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Are roof access locks in place?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Have door-lock-proximity card readers been tested and confirmed to work properly?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Are custodial, mechanical rooms, and storage closets locked when unattended or not in use?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Are breaker panels locked?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			

Section 3

Security Inspections

Outside Physical Security			
Are shrubs and bushes maintained around 3 feet high to eliminate hiding places?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Are the lowest tree limbs no less than 7 feet high?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Are tree limbs maintained to prevent access to building vents, windows, or floors above the first level?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Are building lights operable above entrance/exit doors?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Are parking lot and walkway lights operable?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Are parking lot lights providing enough light to recognize a person from 25 feet away?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			

Section 3

Security Inspections

Outside Physical Security			
Are the outside garbage area lights operable, and are the dumpster covers in place?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Are outdoor valuable assets properly stored and secured?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Are fences in good repair, including locked fencing around property utilities?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Are exterior walls clear of foot/handholds from cables, utility items, downspouts, gutters, wires that could be used to climb to the roof?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Are all light fixtures operable and providing adequate light when dark so walkways, parking lots, and entrances can be seen at night?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			

Section 3

Security Inspections

Outside Physical Security				
Are protective light covers/wire cages in good condition?				
Acceptable		Needs Attention		Correction Completed (Date & Initials)
Concerns Found:				
Are security camera views clear of any foliage or other items placed in the way?				
Acceptable		Needs Attention		Correction Completed (Date & Initials)
Concerns Found:				
Have all 911/emergency call boxes been tested and found functioning?				
Acceptable		Needs Attention		Correction Completed (Date & Initials)
Concerns Found:				
Are mounted, communicative security signs in good repair and clearly visible to pedestrians, people in vehicles or on bicycles?				
Acceptable		Needs Attention		Correction Completed (Date & Initials)
Concerns Found:				
Is the entrance sign visible and easy to read?				
Acceptable		Needs Attention		Correction Completed (Date & Initials)
Concerns Found:				
Are flammable liquids, such as gasoline, properly secured from access when not in use?				
Acceptable		Needs Attention		Correction Completed (Date & Initials)
Concerns Found:				

Section 3

Security Inspections

Inside Equipment • Lighting			
Are 24/7 security lights operable?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Are light motion sensors operable?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Are assets securely locked when not in use, e.g., instruments, fine arts, sacred objects, computers rooms, chemical storage, etc.?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Are window blinds open at night?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Are the central station camera monitors in good working order, and can people and objects be seen clearly?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Did the security alarm test function as it should?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Did all door alarms function properly?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			
Are safes locked when not being used?			
Acceptable ☐	Needs Attention ☐	Correction Completed (Date & Initials)	
Concerns Found:			

Section 4

Staff Training and Awareness

Training and awareness activities are essential for preparing staff on the various ways to respond should an active threat event occur. This training should be ongoing and include not just employees, but volunteers and possibly the clients served by your ministries, such as students at educational facilities and residents at nursing homes. If your facility is a convent or monastery, the religious living on-site should also participate in any training and awareness activities. These activities will prepare those involved on how to think and react wherever they are, whether or not they are at work.

Initially, if your organization has had no type of active threat awareness training, consider working with an outside consultant to help set up and provide the initial training. This initial training can help properly set the stage for ongoing awareness programs and additional reminder training sessions throughout the year. This training also should include a review of specific and applicable organizational policies/procedures and any type of warning/communication systems the organization will be using. A variety of ongoing awareness programs also should be utilized to help encourage employees to think daily about what they will do should an incident occur.

Schedule and coordinate training and awareness for your organization. Depending on how you set up the risk management programs, you may have an active threat team, workplace violence committee, safety committee, risk management team, or you may even have an organizational trainer. These functions need to be assigned and managed by someone or some group within your organization.

Types of Training to Consider

Live Training:
Providing live training is a high priority in coordinating training. It is recommended that live training should occur every couple of years, and initially for all staff. There are two types of live training: Presentation and Hands-on. Live training is important since it allows participants to ask specific questions of the presenters. Formal organizational policy and procedures also can be reviewed and discussed in live training. Also, the hands-on portion of the training usually can be customized and conducted within individual departments. This will allow staff to practice their reactions to an event in the same areas they normally perform their work. This helps them to visualize what they might actually need to do.

There is a variety of options when it comes to coordinating live training. You may have security on staff who can perform this type of training. If not, the organization may consider sending security personnel or someone else to become trainers. You also can identify outside security consultants to perform the needed training or steer your organization toward where to find quality trainers. You might also identify a local community resource that can provide you with a live trainer. Some communities have trainers on their police force that specifically assist organizations with this type of training.

Online Training:
Online training is a great way to continue with ongoing awareness. Online training usually can be done quickly and the user can coordinate their time to take the programs when it is convenient for them. It is also a good method for organizations to consider using to provide basic awareness of the topic for new employees.

Table-Top Exercise:

"Table-Top" training exercises are also a good method to train specific individuals on formal policies/procedures and to test the preparedness of current systems and protocols. This type of training also helps those individuals responsible for managing a simulated emergency situation to identify weakness in the existing programs.
After reviewing your training options, investigate a little further as to what these programs will offer and what content will be presented. Do these steps before you schedule the training so there are no surprises as to the content being presented. Some facilities such as retirement communities or schools need very specific training depending on their ministries and the services they provide. Active shooter training should also include a process for staff to follow that is easy to remember. We list one of these processes below:

The Four Outs for an Active Shooter™

In the event of an active shooter in the facility, there are four options available, called The Four Outs:

Get Out

- Exit the facility as quickly as possible.
- Leave personal belongings behind.
- Encourage others to go with you, but do not delay. Evacuate as many residents as possible.
- Any and all employees with cell phones should call 9-1-1.
- Follow police directions.

Hide Out

- If you are unable to safely leave the facility, attempt to seek shelter in an inconspicuous place; lock doors if possible.
- Turn off lights. Make every attempt to give the appearance of an empty room. Each unit/floor/wing should make a list of rooms in their areas that have locking doors that can be used to hide and secure residents and staff.
- Be aware of any sounds that would help you know the location and direction of the threat.
- Plan an escape route.
- Use stairwells as opposed to elevators if moving to an area of shelter.
- Hide in plain sight (as a last resort)
- Remain quiet and hidden until the "ALL-CLEAR" is given by the person in charge or local authorities.

Keep Out

- Lock/deadbolt doors, if doors do not have locks on them, try to secure the doors as much as possible by tightening a belt around the closer cross arms; door stops under the doors, or however possible.
- Use large, heavy items (furniture, resident beds, copy machines, desks, etc.) to barricade doors. Remember to lock the wheels on anything with rollers or casters.
- Stack smaller things in front of doors to create a "wall of obstruction" that will delay the shooter's entry to the room or area, or will discourage him from attempting entry.
- Remain quiet and still.
- Start thinking about self-protection and what things you can use to attack the assailant.

Take Out

- TAKE OUT means to fight back. This is a last resort. It must be recognized…this is the fight of your life…FOR your life.
- There is strength in numbers. All occupants of the room who can physically fight back should arm themselves with some type of "weapon of opportunity" and be prepared to incapacitate the shooter as soon as he enters the room.
- Use anything available (fire extinguishers, stethoscopes, chairs, coffee cups, staplers, cellphones, letter openers, belts, pictures, chairs, etc.), to "take out" the threat and defend yourself.
- Take a position of tactical advantage; do not position yourself right in front of the door. Position yourself to the side of the door. If you are in a group, position members on both sides of the door.
- Use a diversionary tactic to distract the shooter or cause him to look away momentarily. Use a three-step attack: surprise…aggression…speed.

Ongoing Awareness Programs:

There are many ways organizations can increase staff awareness of a variety of topics. You can rotate these topics in and out with other company news, activities or programs. However, keep in mind, you need to manage and coordinate these activities. Usually a committee or team prepares the necessary communication. Below are a few examples that can be used to increase staff awareness:

- ***Bulletin Boards:*** If you have bulletin boards, attach and switch out the old awareness bulletins monthly. It is suggested that the coordinating group of this program develop an annual topic schedule to help provide ongoing direction as to what needs to be developed for the next month.
- ***Hallway Posters:*** Not all organizations have wall mounted poster units where posters can be switched out monthly or quarterly. Usually organizations that have these types of poster holders, mount motivational-type posters. You can also use these units to increase awareness to active shooters and other topics.
- ***Weekly/Monthly Company Newsletters/ eNewsletters:*** If your organization uses newsletters in any format, consider developing a column to address active shooter concerns and/or add active shooter as a rotating topic if there is a section for safety.
- ***Staff Meetings:*** You can develop topics for the staff meetings. These topics should be short and discussions should not last more than five to 10 minutes. When developing the topics, try to give your speakers a short outline as to what to cover. A descriptive narrative and maybe a few discussion questions to ask the group will help walk them through the five to 10 minute discussion they are to present.

Active Shooter Training and Awareness Schedule

(Sample Calendar Year Schedule)

	Training (Topics/Dates)	Awareness Activities
January	Assign New Employees online training	Update Poster Holder Monthly Topic in eNewsletter
February	Assign New Employees online training Options Based Training All Divisions week	Monthly Topic in eNewsletter
March	Assign New Employees online training	Monthly Topic in eNewsletter Post Topic on Bulletin Board
April	Assign New Employees online training Assign Employees Part 1 online training	Monthly Topic in eNewsletter
May	Assign New Employees online training Departmental 5-10 min. Topic	Monthly Topic in eNewsletter
June	Assign New Employees online training	Monthly Topic in eNewsletter Safety Month: Work on Topic with Safety Committee
July	Assign New Employees online training	Updated Poster Holder Monthly Topic in eNewsletter
August	Assign New Employees online training Options Based Training Make-up week	Monthly Topic in eNewsletter
September	Assign New Employees online training	Monthly Topic in eNewsletter Post Topic on Bulletin Board
October	Assign New Employees online training Assign Employees Part 2 online training	Monthly Topic in eNewsletter
November	Assign New Employees online training Departmental 5-10 min. Topic	Monthly Topic in eNewsletter
December	Assign New Employees online training	Monthly Topic in eNewsletter

Section 5

Disaster Recovery Planning

As with all plans, it is critical for organizations to develop and test their plan before it is actually needed. Organizations do not want to get caught without a plan after an active threat event occurs at their facility. Does your organization have a plan if the police department tells you no one at the organization is allowed to enter your property for the next week? This could happen. Organizations can be shut down for a week or more, during the time the crime scene is being investigated. What about employees? After an event, employees may physically be able to come to work and work in the same area doing the same job; however, psychologically they may not be ready to engage in normal work activities in a building they have experienced the most life changing event of their life. How about one year after the event? This could be traumatic for people reliving the event on its anniversary.

Disaster recovery planning is essential to assist the organization in picking up the pieces and moving on after a traumatic event. These types of plans, whether it is for an active shooter event or a gas leak from one of your neighboring businesses, are normally developed and tested by the organization's "Business Continuity Planning Team." The purpose of this section is not to walk you through step-by-step, how to develop a disaster recovery plan, but rather to highlight areas of consideration your organization and its "Business Continuity Planning Team" should consider. The following is list of these considerations:

1. Assign leadership responsibilities and what their responses should be.
2. Have access to emergency supplies that includes a number of tourniquets that would be accessible where people will assemble.
3. Identify and confirm there is a backup facility/building or work-from-home possibilities identified with agreements already in place.
4. Identify the types and the amounts of equipment/computers/software that may be needed, where this equipment can be acquired and a plan to set up and roll out the equipment/hardware quickly so that it can be used immediately upon its configuration.
5. Determine how electronic data is going to be stored, protected and recovered.
6. Determine how paper documents are going to be stored, protected and recovered.
7. Develop a communication plan that helps employees communicate easily with other employees and mission critical functions.
8. Develop a plan for the media, vendors and the customers you serve.
9. Have contracts in place with vendors to help with cleanup of the facility and possible board up to prevent further damage to the property.
10. Develop human recovery plan that would address the physical and mental needs of all employees, victims, and family members whether they are at home or at work. This plan should include the initial short-term needs, such as reporting to family members and long-term needs that go out past a one-year anniversary date and include ongoing help such as the use of an "Employee Assistance Program" (EAP) or other behavioral health support services. It is important to include all members of staff's family in this plan.
11. Determine how positions will be filled for injured or deceased employees.
12. Evaluate and test these individual plans initially and periodically to adjust for any changes in the organization.
13. Check with your insurance carriers to identify what is and what is not covered. Also identify if there is any assistance with the disaster recovery process and what that assistance will include.

Recovering after an event can be a continuous process that occurs not just during the short term, but is rather a long-term healing process. Ensuring you have a plan in place before an event occurs will help your organization bounce back quicker and hopefully prevent your ministry from having to close its doors permanently.

The following links can assist with further research and identifying additional material on disaster recovery and business continuity planning:

dhs.gov	Department of Homeland Security
ready.gov	Department of Homeland Security - Disaster Emergency Information
fema.gov	Federal Emergency Management Agency

Section 6

Sample Policies

When developing and implementing employment policies for any organization, it is always essential to ensure these policies comply with federal, state and local laws. They should also meet any requirements spelled out by licensing/accrediting agencies with which the organization must comply. This section provides several sample security policies to be considered and can be customized to be included within your organization's employment handbook. When using sample policies to create your own organizational polices, remember, they are sample polices. All policies need to be customized to reflect the organization's mission and operations for the specific facility in which it will use the policy. "Specific" means what might be good for a school, most likely will not be good for a nursing home, retreat center or religious community, so the policy needs to be customized.

As with all employment policies, you should conduct a legal review by an employment attorney before the organization moves forward with a policy roll out. This will help eliminate any wording that could have legal ramifications should an event occur. For policies and procedures involving security, you also should consider having a security expert provide suggestions on these documents. A security expert's review will help to provide a risk management approach to the documents whereas a legal review normally focuses on meeting the needs of the required laws.

The following pages are sample polices to be considered.

These policies are intended to serve only as a basic example and should be added to and/or revised to fit each individual organization or institution.

Section 6

Sample Policies - Active Shooter Response

This policy is to provide guidance for an employee response during an active shooter situation to help limit injury and maximize survivability. The term "active shooter," as it applies to this policy, is an assailant(s) actively engaged in killing or attempting to kill people at the workplace with weapons to include, but not limited to, those from firearms, vehicles, explosives and knives. If an active shooter event is occurring, it is important for employees quickly to determine the most reasonable way to protect their own lives and to assist others as appropriate. Remembering and using the **"Get Out" "Hide Out" "Keep Out" "Take Out" ™** method can assist with directing potential employee actions during an active shooter situation. These steps are described below:

Get Out: Determine where the threat is located and evacuate the premises immediately through the closest exits. While evacuating communicate with other employees of the threat and encourage them to evacuate with you. Leave all your belongings behind. Keep your hands visible and up in the air so it is clear you have no weapons. Emergency responders could misinterpret belongings or items in your hands as weapons such as a black cell phone or small purse. All employees with cell phones should call 9-1-1 once in a secure area. (During this initial reactionary step, staff needs to know where to go after vacating the building. An assembly area(s) should be identified that is not too close to the building and large enough for numerous staff to gather.) After vacating the building, staff should not get into their vehicles and leave the property. This can be an added danger for individuals fleeing from the building and can cause confusion and problems as emergency vehicles are rushing to the facility.

Hide Out: If you are unable to evacuate, find a place to hide. Look for areas that are out of the active shooter's view and provide protection if shots are fired in your direction. Lock the door if possible. Turn off the lights. Make every attempt to give the appearance of an empty room. Silence your cell phone, close room blinds and try to remain calm and quiet. (Identify locations in the facility that could allow for a place to "Hide Out." These places can be listed here.)

Keep Out: Lock/deadbolt doors, if doors do not have locks on them, try to secure the doors as much as possible such as with door stops. If the door has a closer mechanism (located at the top of the door that closes the door shut when not in use) tighten a belt around the closer cross arms to help prevent the door from being opened. Use large heavy items (furniture, resident beds, copy machines, desks, etc.) to barricade doors. Stack smaller things in front of doors to create a "wall of obstruction" that will delay the shooter's entry to the room or area, or will discourage him from attempting entry. Remain quiet and still. Start thinking about self-protection and what things you can use to attack the assailant. (Identify locations in the facility that could allow for a place to "Keep Out." These places can be listed here.)

Take Out: Fight back if your life is in imminent danger and as a last resort. There is strength in numbers. All occupants of the room who can physically fight back should arm themselves with some type of "weapon of opportunity" and be prepared to incapacitate the shooter as soon as he enters the room. Use anything available (fire extinguisher, chairs, coffee cups, stapler, cellphones, letter openers, belts, pictures, etc.), to "take out" the threat and defend yourself.

(Once we discuss communications, we might want to include possible notification systems and how they might work at the onset of an active shooter or give the "all-clear." Usually, the all-clear means officers clearing the building room by room, but we can discuss this policy element.)

Some additional thoughts to consider:

- Elevators are usually locked down during an incident so do not hide out in an elevator.
- Never pull the fire alarm. Doing so can provide the shooter with loud audio cover as the shooter moves about the building and can possibly drive employees and visitors to know evacuation routes in the shooter's path. People might not even know there is an active shooter event going on.
- Most attempts to negotiate with an active shooter will probably be futile. The shooter has already in their head dehumanized people and will not think twice to shoot. Keep in mind they are trying to hurt/kill as many people as possible.
- **"Get Out" "Hide Out" "Keep Out" "Take Out" ™** are possible steps to follow during an active shooter event. However, these steps are not to be followed in order, rather they are opportunities for consideration depending on the circumstances of the situation. In fact, multiple steps could be used during an event. If an individual is using the "Hide Out" method and if the situation then allows for an opportunity to "Get Out," then this step would be used. Or if the active shooter is in front of you, your best opportunity at the time could be to use the "Take Out" method.
- **Depending on the organization's ministry, additional plans may need to be developed for communications and assistance for those the ministry serves.**

Section 6

Sample Policies - Standard of Conduct and Work Rules

The Company has a responsibility to establish rules and regulations regarding employee behavior necessary for an efficient operation, and for the benefit and protection of the rights and safety of all. We will not tolerate conduct that interferes with operations, discredits the Company, or is offensive to customers or fellow employees. For these reasons, the following sets forth the Company's expectations of employee conduct.

1. All employees are expected to conduct themselves in a manner conducive to the efficient operation of the Company. Such conduct includes:
   a. Reporting to work as scheduled and being at the workstation, ready for work, at the assigned starting time.
   b. Performing assigned job responsibilities effectively and efficiently.
   c. Treating all employees, customers and visitors with respect and professionalism.
   d. Refraining from behavior or conduct deemed offensive or undesirable, or subject to disciplinary action.
   e. Adhering to the Company-wide dress code policy.
2. The following conduct is prohibited and will subject the individual involved to disciplinary action up to and including dismissal:
   a. Insubordination, including improper conduct toward a supervisor or refusal to perform tasks assigned by a supervisor, either in writing or verbally, in the appropriate manner.
   b. Possessing, consuming, or distributing alcohol or illegal drugs or substances on Company grounds, or reporting to work or performing duties under the influence of alcohol or with illegal drugs or substances present in his/her system. Reasonable consumption of alcohol at Company-authorized functions is permitted.
   c. Failure to maintain confidential information.
   d. Theft, misuse of, or damage to Company property or of another employee's property.
   e. Falsifying Company records or reports, such as an application for employment, a production record, a time record, financial or expense.
   f. Fighting, assault, or the use of abusive or threatening language or gestures on Company property.
   g. Bringing dangerous or unauthorized material such as explosives, firearms, and other such items on Company property.
   h. Unsatisfactory work performance.
   i. Failure to notify a supervisor of absence from work in accordance with policy.
   j. Unexcused excessive tardiness or absenteeism and/or abuse of vacation benefits or sick days.
   k. Unauthorized or excessive personal telephone, email, copy machine, fax or internet usage.
   l. Sleeping on the job.
   m. Violation of policies and procedures relative to the safety and security of Company employees, visitors, and customers.
   n. Failure to cooperate with Company investigation of insurance, discrimination, harassment or disciplinary matters.
   o. Failure to accept required training.
   p. Violation of the Company's policy prohibiting discrimination, harassment and retaliation.
   q. Violation of any company policies, rules, regulations, or practices.

Listed above are some Company conduct and work rules. The list includes types of behavior and conduct that the Company considers inappropriate and which could lead to disciplinary action up to and including dismissal from employment without prior warning. Employees should not view this list as being all-inclusive. Additionally, the Company reserves the right to impose discipline up to and including dismissal for other inappropriate or dangerous actions or misconduct.

Section 6

Sample Policies - Physical Security

The physical security of all Company employees and assets–equipment and information–is very important. Each employee is responsible for adhering to the methods of physical security detailed below.

1. Employee Identification Badge

The Company issues all employees a plastic identification (ID) badge when hired. For protection purposes, should the card be misplaced, the badge does not include specific information identifying the employee or the company. We advise employees to wear their name badge. Clips and lanyards are available from ITS upon request.

The badge, when worn and visible, provides identification as an employee and as an access card for any door with a card reader and according to the employee's security level.

Missing, stolen or damaged ID badges are to be reported promptly for a replacement. Cards no longer in the company's possession must be disabled immediately so they cannot be used to access secure doors. If an employee's need for replacement badges is excessive, the Company may charge a fee.

2. Building Card Access System

The building is equipped with a key card access system that controls the operation of all external doors and several internal doors—identifiable by the keycard sensor mounted on the door.

External doors are locked at all times. The employee ID badge also serves as a door key card. Employees can "swipe" their key card to access the building during regular business hours.

Usage Procedures:

- Employees leaving the building will need their ID badge to re-enter.
- Only authorized employees have access to the building outside business hours and have been instructed in the use of the alarm system. All other employees must be accompanied by an employee authorized for access outside business hours.
- Employees are not to prop doors open.

3. Visitor Check-In and Deliveries

The receptionist and Mail Room have responsibility for processing all visitors and deliveries.

Visitors

- Employees are not to give anyone access to the building and should be on alert for anyone who attempts to "tailgate"—enter behind an employee/group of employees without using an access badge. Employees have ID badges, so do not need to be let in by other employees. Also, former employees, including retirees, are visitors and are not to be given access to the building by anyone other than the receptionist.
- Visitors must enter and exit the building through the main lobby.
- Employees are to notify the receptionist of expected visitors. The receptionist is responsible for giving access to the building to expected visitors only.
- Visitors are required to sign in to the log book upon entrance and to sign out when exiting the building. Visitors are issued a visitors' ID badge that must be worn throughout their visit and returned to the receptionist when they sign out and exit the building.
- Employees expecting a group of visitors are to provide the receptionist with a checklist of the group ahead of time. This will expedite the check-in process. Likewise, employees expecting a visitor who will arrive before or after business hours are to obtain a visitor's badge from the receptionist ahead of time.

- Visitors are not permitted beyond the lobby without an escort unless that visitor is a frequent and well-known visitor. A visitor must have an escort at all times while in the building, including if the visitor wishes to visit employees in another division.
- Employees are to report any unfamiliar person without a name badge to their supervisor.

Deliveries

- Except for floral deliveries, all deliveries are to be directed to the dock. This includes food deliveries.
- Delivery hours are 7:00 a.m.–3:30 p.m., Monday – Friday and are posted on the door. Any delivery before or after the posted hours will be turned away. Anyone accepting a delivery before or after the posted hours will be held accountable for the items and paperwork.
- Office Services and Facilities are the only employees authorized to sign for packages and to collect packing slips. When a delivery is scheduled, the vendor needs to be made aware of delivery hours, which differ from business hours. Arrangements must be made with Office Services for deliveries outside the posted hours.

4. Building Alarm System

The building is equipped with an alarm system to help protect the building during non-business hours. There are many sensors throughout the building. The company distributes the building alarm code to authorized personnel, as determined by the Human Resources Manager in consultation with the senior level managers.

We may provide the building alarm code to others upon request and review by Human Resources. Access will be provided only for the specific time period necessary (e.g. weekend work) and revoked immediately afterward.

The Company provides the building alarm code and building access procedures to authorized personnel on a semi-annual basis.

5. Building Video Surveillance System

The building is equipped with an external video surveillance system consisting of a network of cameras installed on and around the building to capture images of the parking lot entrances/exits, building entrances/exits and much of the grounds and parking lots. Signs are posted at the driveway entrances to inform visitors of the existence of the video surveillance system. All employees and visitors consent to being recorded on video by entering company property.

The building is also equipped with several internal cameras.

These policy and security measures are in place to protect all employees and property. Each employee is responsible for following the policy and to report any observed violations. Employees who violate the Physical Security policy may be subject to disciplinary action up to and including dismissal.

Questions, comments, and observed violations are to be reported to Human Resources.

Section 6

Sample Policies - Whistleblowing

An employee at one time or another may have a concern about something happening within the Company. Usually, such a concern is easily resolved. However, when the concern is observed conduct that may violate a Company policy or may be unlawful, it can be difficult to know what to do.

It is understandable that employees may be worried about raising such issues. They may want to keep the concerns to themselves, perhaps feeling this is none of their business, only a suspicion or that this is not important enough to report. Employees may also feel that raising the matter would be disloyal to colleagues, managers, or to the Company itself. However, employees must report all improper conduct. The Company takes seriously any form of conduct in violation of a Company policy or this Code. The Company would prefer that the matter be raised when it is just a concern rather than have the employee wait for the situation to develop. It is not the employee's responsibility to investigate the matter; rather, the matter should be turned over to someone who has that responsibility, releasing the employee from the burden of the concern raised.

Typically, concerns of a financial nature need to be reported to the Chief Financial Officer or the Controller, and all other concerns are to be reported to the Human Resources Office or the HR Manager. The Company encourages employees to report their concern of wrongdoing immediately to any manager who is then responsible for referring the matter to the appropriate senior level manager.

An employee who raises a genuine concern under this standard will not be at risk of retaliation. Provided the employee is acting in good faith, it will not matter if she/he is mistaken. Retaliation for reporting any violations of this Code of Values, Standards and Conduct, or participating with an investigation is strictly prohibited. If we substantiate a complaint of retaliation, appropriate disciplinary action, which may include dismissal, will be taken.

Sample Policies - Workplace Violence

Workplace violence of any kind will not be tolerated. Workplace violence includes threats, intimidation, verbal and physical aggression, and other conduct that could reasonably cause fear in another person. Firearms, other weapons, or any dangerous materials are not permitted at any time while on Company premises or elsewhere while conducting business on behalf of the Company. An employee who observes a weapon and/or experiences or witnesses any form of violence at the Company is to immediately report the incident to their supervisor or to Human Resources.

In addition, the Company will not condone any acts or threats of violence against employees, vendors, clients or visitors on the Company's premises at any time or while they are engaged in business on behalf of the Company, whether on or off the Company's premises.

Policy

It is the policy of the Company and the responsibility of its managers and all of its employees to maintain a workplace free from threats and acts of violence. The Company will work to provide a safe workplace for employees and for visitors to the workplace. The Company does not tolerate any type of workplace violence committed by or against employees. The Company prohibits employees from making threats or engaging in violent activities.

Prohibited Conduct

The list below provides examples of conduct that is prohibited, albeit not exhaustive:

- Causing physical injury to another person
- Making threatening remarks
- Acting out aggressively, including aggressive language, that creates a reasonable fear of injury to another person or subjects another individual to emotional distress
- Intentionally damaging employer property or property of another employee
- Possessing a weapon while on Company property or while on Company business
- Committing acts motivated by, or related to, sexual harassment or domestic violence

Reporting Procedures

You must immediately report any potentially dangerous situations to your supervisor or Human Resources. Reports of workplace violence may be made anonymously and investigated accordingly. Reports or incidents warranting confidentiality will be handled appropriately and we will disclose information to others only on a need-to-know basis. The Company will speak to all parties involved in a situation and we will discuss the results of investigations with them. The Company will take appropriate action at any indication of a potentially hostile or violent situation.

Risk Reduction Measures

While the Company does not expect employees to be skilled at identifying potentially dangerous persons, we expect employees to exercise good judgment and to inform the Human Resources Department if any employee, claimant or customer exhibits behavior which could lead to a potentially dangerous situation. Such behavior includes, but is not limited to:

- Discussing dangerous weapons and/or bringing such weapons into the workplace
- Displaying overt signs or extreme stress, resentment, hostility, or anger
- Making threatening remarks
- Exhibiting sudden or significant deterioration of performance
- Displaying irrational or inappropriate behavior

Enforcement

Threats, threatening conduct, or any other acts of aggression or violence in the workplace will not be tolerated. Any employee determined to have committed such acts will be subject to disciplinary action, up to and including termination.

Non-employees engaged in violent acts on the employer's premises will be reported to the proper authorities and fully prosecuted.

Sample Policies - Workplace Security

The Company is concerned about the increased violence in our society, including its entry into the many workplaces throughout the country. With this concern in mind, the Company has taken steps to help maintain safe working conditions. It is the policy of the Company to expressly prohibit any actions or threats of violence by any employee against any other employee in or about the Company's premises. In addition, the Company will not condone any acts or threats of violence against employees or visitors on the Company's premises at any time or while they are engaged in business with or on behalf of the Company, on or off the Company's premises. The Company is committed to prohibiting employees and visitors from bringing unauthorized firearms or other weapons onto the Company's premises.

All visitors, including former employees and the friends and family members of employees, are to enter the building through the main lobby entrance only. All visitors are required to sign in, receive and wear a visitor security badge at all times while in the building.

In keeping with the spirit and intent of this policy, and to ensure that the Company's objectives are attained, the Company is committed to the following:

1. To take prompt and remedial action, up to and including immediate dismissal of employment, against any employee who engages in any threatening behavior or acts of violence or who uses any obscene, abusive, or threatening language or gestures.
2. To take appropriate action when dealing with visitors who engage in such behavior. Such action may include notifying local law enforcement personnel and prosecuting violators of this policy to the maximum extent of the law.
3. To establish viable security measures to ensure that the Company's premises are safe and secure to the maximum extent possible and properly control access to the building by visitors.

Any employee who engages in or displays a tendency to engage in violent, abusive, or threatening behavior, or who otherwise engages in behavior that the Company, in its sole discretion, deems offensive or inappropriate will be referred to Human Resources, which will address the matter in conjunction with the appropriate manager/supervisor.

This guide can be used to assist your team in developing regular reminders, drafting protocols and practicing procedures effectively, keeping life-saving tactics top of mind. Preparation can be the key to survival. Having a practiced plan in place can mean the difference in ensuring your employees a safe working environment.

Risk Solutions
1205 Windham Parkway • Romeoville, IL 60446
Jeff Harrison (*Director of Risk Control Services*)
630.378.2543 • jeff.harrison@cbservices.org