xemana

Workplace Training and Management Systems

Building Security

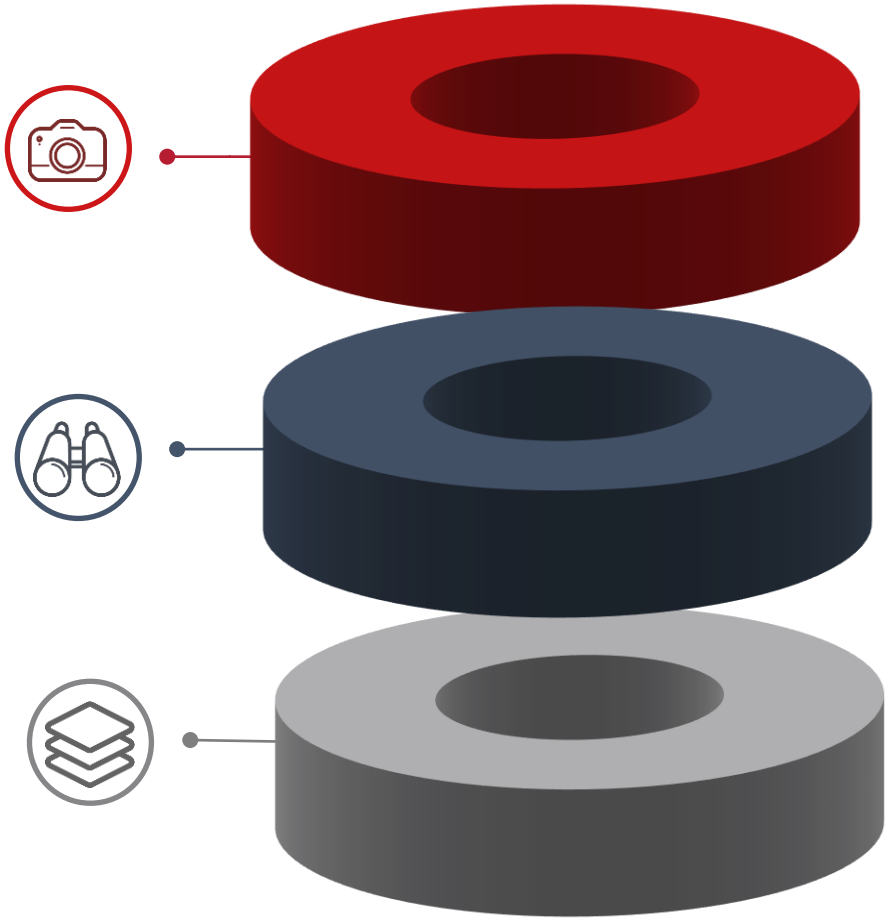
Powered by B.E.S.T.
Building Effective Safety Teams™
Auburn Services ,LLC

Security Begins With You

We are faced with increased risks that threaten :

- Employee Safety and Morale
- Guests Safety
- Economic Livelihood

Building Security –
Risk Management



Threat
A natural or manmade occurrence, individual, entity or action that has or indicates the potential to harm life, information, operations, the environment and or property.

Vulnerability
Physical features or operational attributes that render an entity open to exploitation, or susceptible to a given hazard. Vulnerabilities may be associated with physical factors such as human factors, cyber factors, or untrained guards or personnel.

Consequence (Impact)
The effect of an event, incident, or occurrence.

ID Badges

Many facilities have systems for access control and visitor management deployed throughout the property. These systems grant access to individuals based on their function at the workplace.

Facilities may use ID badges or picture IDs for quick identification of personnel while providing the appropriate level of access control. Many badge types work with proximity readers, allowing individuals to use their badge as a key.

Typical Badge Requirements

If your workplace uses ID badges or other ID security measures, remember that you should:

- Wear your badge on the outermost garment at all times while in the workplace.
- Never allow “piggybacking”—letting an individual follow you through access doors.
- Never lend or borrow badges when an employee has forgotten his or her badge.
- Never allow visitors to share your badge. Only one person should be cleared through an entry point on a given badge.
- Report a lost badge to the appropriate security personnel, manager, or human resources representative immediately.

Sources: Chemical Security Awareness Training/Protect Your Workplace Campaign: Report Suspicious Behavior and Activity Poster

Access & Security Control Threats

Non-employees should wear a visitor's badge and should be escorted at all times.

For more information on the specific security policies for your workplace, please refer to your organization's security officer or management representative.

If your workplace does not use an ID badge system, follow your appropriate recognition methods (for example, vest, hat, or uniform) and apply the recognition procedures and reporting requirements as established in your workplace.

Access & Security Control Threats

Unknown Individuals

You should challenge unknown or suspiciously behaving people that you encounter within a secured area if they:

- Are not accompanied by someone you recognize.
- Are not wearing appropriate identification.
- Have an appearance that is inconsistent with the workplace dress code.
- Seem lost or are asking for directions to specific areas.

Challenging Unknown Individuals

If you approach an unknown individual:

- Maintain a safe distance of at least three steps (10 feet) between yourself and the person you are challenging.
- Be persistent in your questioning.
- Do not be easily dismissed. An intruder may give you a brief explanation and just keep on going. (For example: "Sir, may I help you?" "No thanks, I'm fine.")

Note: These standard access security control procedures are based on industry best practices. However, they may not reflect your organization's policy. Please contact your manager or designated security personnel professional for your specific workplace policy on approaching such individuals.

Criminal & Terrorist Threats

Suspicious Behaviors

It is important to be alert for the following suspicious behaviors:

- Nervous behavior, evasive attitudes, or undue concern with privacy by guests or visitors.
- Attempts to gain access to restricted areas.
- Individuals taking notes, pictures, or videos of facility.

Reporting Suspicious Behaviors

- Note the time and place of the incident.
- Report the incident to the appropriate supervisor or security personnel immediately.

When you see someone engaged in suspicious activities such as taking pictures of security cameras or guard posts, you should report it to the appropriate supervisor or security personnel. However, you should never be confrontational or attempt to restrain the person physically

Criminal & Terrorist Threats

Unusual Events or Suspicious Items

Be alert for:

- Changed or unusual situations around your workplace such as tampered HVAC units, abandoned vehicles, damaged fence line, or missing property.
- Suspicious packages or items, especially:
  Large amounts of unusual substances (e.g., acetone, peroxide, or drain cleaner).

- Fumes, odors, or liquids coming from the package.
- Disassembled electrical components such as wires, circuit boards, or batteries.
- Plans, drawings, schematics, or maps.

Immediately report the situation to appropriate security or management personnel. Do not go near the area or attempt to open or inspect suspicious items.

Criminal & Terrorist Threats

Perimeter Breaches / Suspicious Packages

Employees should immediately notify a supervisor or security person of the following:

- A breach in the security perimeter, such as a door that is propped open
- A suspicious package or item

Employees should never approach or attempt to open or inspect suspicious packages.

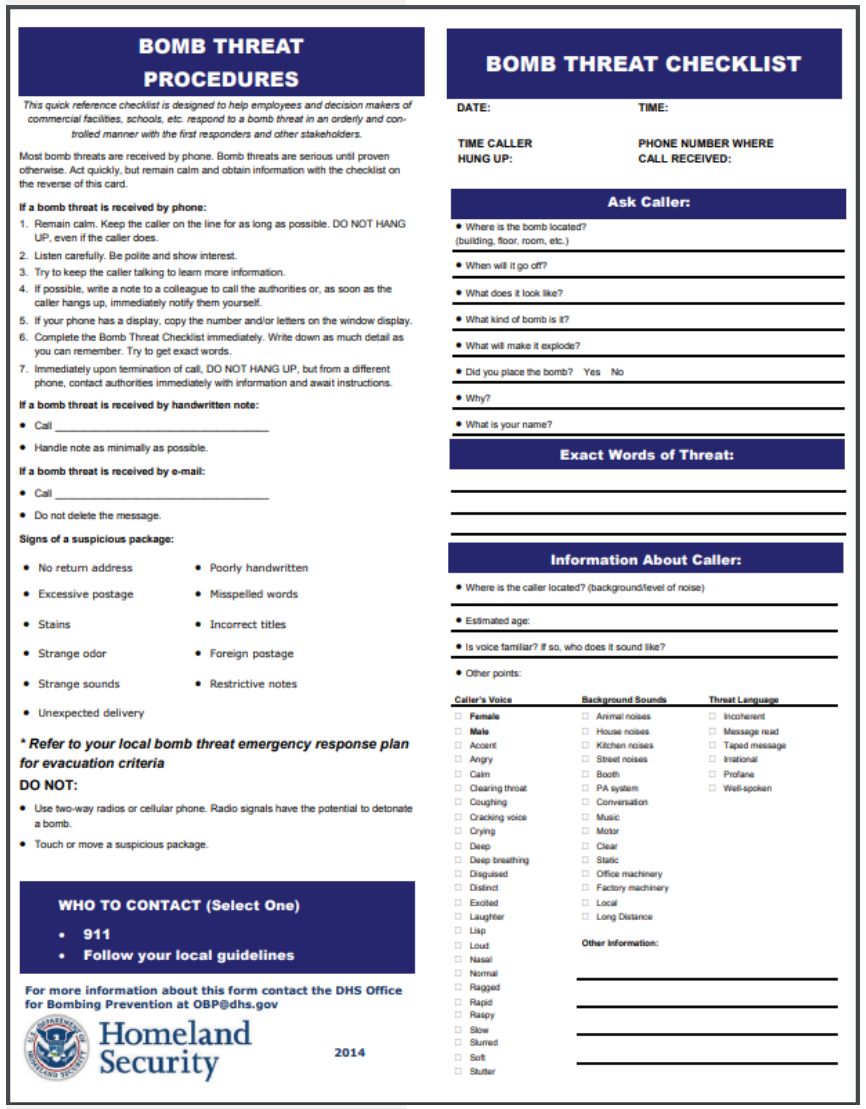
Criminal & Terrorist Threats

Employees should:

- Report abandoned vehicles parked on the property or adjacent to the workplace.
- Be on the lookout for private vehicles loading or unloading unusual or suspicious items on or around the property.
- Be alert for familiar vehicles arriving at unusual, unscheduled, or inappropriate times.

- Report observations to security personnel or an appropriate supervisor immediately.
- Observe and, if possible, write down a suspicious vehicle's license plate number and description (make, model, color, body damage, bumper stickers, and accessories).
- Not take any other action except to observe and report the vehicle.
- As a secondary means of reporting, notify local law enforcement.

Criminal & Terrorist Threats



BOMB THREAT PROCEDURES

This quick reference checklist is designed to help employees and decision makers of commercial facilities, schools, etc. respond to a bomb threat in an orderly and controlled manner with the first responders and other stakeholders.

Most bomb threats are received by phone. Bomb threats are serious until proven otherwise. Act quickly, but remain calm and obtain information with the checklist on the reverse of this card.

If a bomb threat is received by phone:

1. Remain calm. Keep the caller on the line for as long as possible. DO NOT HANG UP, even if the caller does.
2. Listen carefully. Be polite and show interest.
3. Try to keep the caller talking to learn more information.
4. If possible, write a note to a colleague to call the authorities or, as soon as the caller hangs up, immediately notify them yourself.
5. If your phone has a display, copy the number and/or letters on the window display.
6. Complete the Bomb Threat Checklist immediately. Write down as much detail as you can remember. Try to get exact words.
7. Immediately upon termination of call, DO NOT HANG UP, but from a different phone, contact authorities immediately with information and await instructions.

If a bomb threat is received by handwritten note:

- Call _____
- Handle note as minimally as possible.

If a bomb threat is received by e-mail:

- Call _____
- Do not delete the message.

Signs of a suspicious package:

- No return address
- Excessive postage
- Stains
- Strange odor
- Strange sounds
- Unexpected delivery
- Poorly handwritten
- Misspelled words
- Incorrect titles
- Foreign postage
- Restrictive notes

Refer to your local bomb threat emergency response plan for evacuation criteria

DO NOT:

- Use two-way radios or cellular phone. Radio signals have the potential to detonate a bomb.
- Touch or move a suspicious package.

WHO TO CONTACT (Select One)

- **911**
- **Follow your local guidelines**

For more information about this form contact the DHS Office for Bombing Prevention at OBP@dhs.gov

Homeland Security

2014

BOMB THREAT CHECKLIST

DATE: **TIME:**

TIME CALLER HUNG UP: **PHONE NUMBER WHERE CALL RECEIVED:**

Ask Caller:

- Where is the bomb located? (building, floor, room, etc.)
- When will it go off?
- What does it look like?
- What kind of bomb is it?
- What will make it explode?
- Did you place the bomb? Yes No
- Why?
- What is your name?

Exact Words of Threat:

Information About Caller:

- Where is the caller located? (background/level of noise)
- Estimated age:
- Is voice familiar? If so, who does it sound like?
- Other points:

Caller's Voice	Background Sounds	Threat Language
☐ Female	☐ Animal noises	☐ Incoherent
☐ Male	☐ House noises	☐ Message read
☐ Accent	☐ Kitchen noises	☐ Taped message
☐ Angry	☐ Street noises	☐ Irrational
☐ Calm	☐ Booth	☐ Profane
☐ Clearing throat	☐ PA system	☐ Well-spoken
☐ Coughing	☐ Conversation	
☐ Cracking voice	☐ Music	
☐ Crying	☐ Motor	
☐ Deep	☐ Clear	
☐ Deep breathing	☐ Static	
☐ Disguised	☐ Office machinery	
☐ Distinct	☐ Factory machinery	
☐ Excited	☐ Local	
☐ Laughter	☐ Long Distance	
☐ Lisp		
☐ Loud	**Other Information:**	
☐ Nasal		
☐ Normal		
☐ Ragged		
☐ Rapid		
☐ Raspy		
☐ Slow		
☐ Slurred		
☐ Soft		
☐ Stutter		

Bomb threat calls should be taken seriously. Use the following procedures:

- Keep calm.
- Keep the caller on the line as long as possible.
- Record every word spoken by the caller on a form such as a bomb threat checklist (sample provided on the following page).
- Obtain as much information as possible about the threat without antagonizing or threatening the caller.
- Pay particular attention to peculiar background noises and to anything that can be gleaned from the caller's voice, such as gender, accent, and speech pattern.
- Report the incident immediately to a security officer, a manager, and/or a supervisor.

Employees should talk to a supervisor or security representative about the organization's bomb threat policy.
Bomb threat checklists are extremely valuable and should be made available at all workstations.

Criminal & Terrorist Threats

Employees should be alert for threatening or suspicious mail or packages that might contain a bomb or hazardous substance. This includes:

- Letters or packages with suspicious contents such as white powder or photographs of the workplace.
- Letters or packages with oil or grease spots, an inaccurate address, or excessive postage and/or packaging.

Participants who encounter a suspicious mail item or package should:

- Isolate the item. Do not open or handle it.
- If a letter or package contains a suspicious substance, evacuate the area and immediately wash affected body parts (such as hands) with soap and water.
- Contact a manager or security.
- Retain written threats and associated packaging/envelopes unless directed to destroy them by management or security procedures.

Criminal & Terrorist Threats

Theft & Diversion

Employees should be aware of **both** potential theft and diversion.

Theft is an unlawful or unauthorized acquisition by force or stealth:

- By an insider (member of staff), or
- By an outsider (someone who is not a member of the staff).

Diversion is an unlawful or unauthorized acquisition by fraud or deceit.

The type of deception can vary. Diversion may include payment, but there is fraud or deceit involved, such as the improper purchase of items that are restricted.

Workplace Violence Threats

A current employee, a former employee, or an acquaintance of a current or former employee may have the potential to carry out violent behavior at the workplace.

Intuitive managers and coworkers may notice indicators of potentially violent behavior in an employee.

HOW TO RESPOND WHEN AN ACTIVE SHOOTER IS IN YOUR VICINITY

Quickly determine the most reasonable way to protect your own life. Remember that customers and clients are likely to follow the lead of employees and managers during an active shooter situation.

1. ***Evacuate***

   If there is an accessible escape path, attempt to evacuate the premises. Be sure to:

- Have an escape route and plan in mind
- Evacuate regardless of whether others agree to follow
- Leave your belongings behind
- Help others escape, if possible
- Prevent individuals from entering an area where the active shooter may be
- Keep your hands visible
- Follow the instructions of any police officers
- Do not attempt to move wounded people
- Call 911 when you are safe

Workplace Violence Threats

2. Hide out

If evacuation is not possible, find a place to hide where the active shooter is less likely to find you.

Your hiding place should:

- Be out of the active shooter's view
- Provide protection if shots are fired in your direction (i.e., an office with a closed and locked door)
- Not trap you or restrict your options for movement To prevent an active shooter from entering your hiding place:
- Lock the door
- Blockade the door with heavy furniture

If the active shooter is nearby:

- Lock the door
- Silence your cell phone and/or pager
- Turn off any source of noise (i.e., radios, televisions)
- Hide behind large items (i.e., cabinets, desks)
- Remain quiet If evacuation and hiding out are not possible:
- Remain calm
- Dial 911, if possible, to alert police to the active shooter's location
- If you cannot speak, leave the line open and allow the dispatcher to listen

SCAN ME

3. Take action against the active shooter

As a last resort, and only when your life is in imminent danger, attempt to disrupt and/or incapacitate the active shooter by:

- Acting as aggressively as possible against him/her
- Throwing items and improvising weapons
- Yelling
- Committing to your actions

Information & Cyber Threats

Types of PII

To safeguard PII or confidential information, employees should:

- Store sensitive information in a designated room or area that has access control measures to prevent unauthorized access by visitors or members of the public (e.g., locked desk drawers, offices, and file cabinets).
- Destroy all sensitive information by the appropriate methods (e.g., burn bag or paper shredder) when it is no longer needed.
- Never email sensitive information to unauthorized individuals.
- Never leave sensitive information on community printers.
- Take precautions to avoid the loss or theft of computer devices and removable storage media.
- Notify an immediate supervisor if a privacy incident has occurred.

Information & Cyber Threats

Be suspicious of anyone requesting information, especially by phone, Web, or email, and always verify the identity of the person or organization making the request.

- Before entering personal information online, verify that the URL starts with https:// and that you see a closed padlock icon in your browser (often found in the lower right-hand corner of your screen).
- Contact the organization by telephone if there is any doubt as to the authenticity of an email or Web site.
- Contact security if anyone requests your account name or password(s).

Information & Cyber Threats

- **Malicious Code:** Malicious code is any software or program designed to disrupt the normal operation of a computer by allowing an unauthorized process to occur or by granting unauthorized access. Often, the term “virus” is used to refer to all types of malicious code, but malicious code comes in many forms, including:

o Viruses
o Worms
o Trojan horses
o Adware
o Spyware

• **Information Gathering:** Terrorists and other criminals use cyber tools as part of their information-gathering and espionage activities.

• **Identity Theft:** Identity theft occurs when someone uses your personal identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes.

Information & Cyber Threats

Employees should never give their user names or passwords to anyone and should create a strong password that:

- Includes a minimum of eight characters with a combination of:
  - o Alpha characters in both uppercase and lowercase;
  - o Numbers; and
  - o Special characters (- ! @ # $ % ^ & * ( ){ } [ ] | + \ - < > ? /) or alternate alpha characters.

- Does not consist solely of a dictionary word in any language, proper noun, name of person/child, pet, or fictional character.

- Does not use information that a hacker could easily obtain or guess about you, such as a Social Security number, address, birth date, or telephone number.

Information & Cyber Threats

DHS launched the **“If You See Something, Say Something™”** (http://www.dhs.gov/files/reportincidents/see-something-say-something.shtm) campaign as part of the national Suspicious Activity Reporting initiative. The campaign is a simple and effective program to raise public awareness of indicators of terrorism, crime, and other threats and emphasize the importance of reporting suspicious activity to the proper transportation and law enforcement authorities.

The campaign emphasizes that everyone should:

- Be vigilant.
- Take notice of surroundings.
- Report suspicious items or activities to local authorities immediately.

Note: The “If You See Something, Say Something™” campaign was originally used by New York’s Metropolitan Transportation Authority (MTA), which licensed the use of the trademarked slogan to DHS to help with antiterrorism and anticrime efforts.

Information & Cyber Threats

Actions taken at the workplace will be dependent upon circumstances. However, all employees can contribute to workplace security by:

- Identifying threats and vulnerabilities that affect workplace security.
- Avoiding complacency.
- Observing with all senses.
- Being aware of unusual events and activities.
- Noticing unusual or suspicious behavior.
- Knowing whom to call if something is not right.
- Getting assistance—NOT attempting to handle a potential situation alone.

Remember, security is everyone's job. Take it seriously.

References

https://www.fema.gov

Photos courtesy of 123rf.com

Workplace Training and Management Systems

Xemana LLC
David Braun
CEO/Co-Founder
310.200.4184
Email: dbraun@xemana.net