

# **Security Principles**



**This e-manual is the product of  
Learning Shop USA  
and is available to our clients free of charge**

## **Part One**

### **Introduction to Private Security**

**Role of Private Security**

**Private Security and the Criminal Justice System**

**Awareness and Prevention of Crime**

**Observe and Report**

**Ethics and Professionalism**

# The Role of Private Security

In the United States today a private security officer is a person employed by a private party to protect the employing party's assets (such as people, equipment and money) from a variety of hazards (such as waste, careless or unsafe worker behavior and criminal activity) by using preventive measures.

Security guards do this by maintaining a high-visibility presence to deter illegal and inappropriate actions, looking (either directly, through patrols, or indirectly, by monitoring alarm systems or video surveillance cameras) for signs of crime or other hazards (such as a fire), taking action to minimize damage (such as warning and escorting trespassers off property), and reporting incidents to their clients.



**The private security industry is a crucial component of security and safety in the United States and abroad. Today, private security is responsible not only for protecting many of the nation's institutions and critical infrastructure systems, but also for protecting intellectual property and sensitive corporate information. U.S. companies also rely heavily on private security for a wide range of functions, including protecting employees and property, conducting investigations, performing pre-employment screening, providing information technology security, and many other functions.**

# Private Security and the Criminal Justice System



**The criminal justice system consists of three main parts:**

**Police**

**Courts**

**Corrections**

**The police enforce laws and maintain public order and public safety by preventing, detecting and investigating crime, and apprehending and detaining individuals suspected of violating laws.**

**Courts determine if charges alleged by the police merit trial and when trial is appropriate a court oversees proceedings to ensure fairness and compliance with the law.**

**Corrections incarcerates convicted persons.**

**The role of private security in the operation of the criminal justice system is limited to assisting the police.**

# Awareness and Prevention of Crime

Prevention of loss or damage is proportional to the degree of awareness exercised by security officers performing their assigned duties. It is clear that loss and damage occur at a higher level of cost and with great frequency when there is no protective shield such as a security officer force comprised of officers that are aware and able to protect a client's property. If there is a single word in a security officer's vocabulary, it has to be prevention. Prevention is the end goal. It is reached by being aware, alert, observing, reporting and responding.



Prevention activities include:

- Staying current with crime trends, especially those that could impact the property you are hired to protect.
- Maintaining positive relations with external resources such as police and fire departments, emergency medical agencies and hazardous material disposal organizations.
- Controlling property entering and leaving the protected facility such as inspecting packages and purses, vehicles, and supplies/equipment delivered by vendors.
- Assisting mail room personnel determine if a suspicious item deserves further examination by qualified persons.
- Controlling access to the facility and areas within the facility.
- Operating security-related equipment such as CCTV and night lighting.
- Patrolling the facility to look for suspicious activities and hazards.
- By personal example, educating employees as to the importance of security in protecting them and their employer's property.

## **Awareness and Prevention of Crime (Continued)**

- **Conducting random inspections, particularly public areas that are accessible to outsiders.**
- **Reporting security deficiencies such as burned out security lights, holes in a perimeter fence and malfunctioning CCTV cameras.**
- **Assisting employees evacuate the premises during emergency situations.**
- **Knowing how to handle bomb threats made by telephone.**
- **Escorting visitors.**
- **Operating a reception desk to issue visitor passes.**
- **Escorting people who are delivering money and other valuables to a bank and other places of secure storage.**
- **Maintaining communication with the security control center.**
- **Responding to serious incidents such as a person threatening to hurt another person.**
- **Knowing post orders, special operating procedures and other forms of guidance such as a temporary access list.**





## Observe and Report



To observe requires awareness. Awareness is the state or ability to be conscious of events, conditions, or objects. Awareness, then, is the stock and trade of security officers. The word "alertness" is an associated word but connotes a higher degree of awareness. Being aware is a continuous process, while being alert can be temporary such as being alert following a bomb threat. When the threat is over, alertness declines but awareness continues.

Being aware is more than just being observant. A security officer who observes a situation in progress may not be aware of its

meaning. For example, a security officer might see men loading a truck at the loading dock and think it is perfectly alright. However, if he or she were aware that the loading dock had been used in the past to load stolen goods into a truck, the officer would want to check out the situation.

To observe and not report can be a serious mistake. Every unusual activity or event must be reported. Two kinds of reporting apply: immediately notifying a person above you in the chain of command, and then making a written report at the first moment time allows.

### Maintain Order

A security officer maintains order by his or her presence. Appearance of authority, which is essential to maintaining order, is demonstrated by alertness and vigilance. A good way of stating this simple idea is, "He looks like he knows what he is doing."

### Serve as a Deterrent

To deter is to discourage, and in this case it means discourage activity that damages the client's interest. A person that would commit an offense will do it elsewhere if there is an appearance the person will be caught. Projecting an image of professionalism is a strong deterrent.

# Ethics and Professionalism



Ethics are the standards of conduct and judgment in respect to what is perceived as right and wrong. A key element of ethics is the specification of responsibility for human actions. Ethical standards go beyond merely describing conduct that we habitually accept; they seek to define higher goals and the means for attaining them.

We should keep in mind that people in general have always shown an interest in the

security profession and are quick to make negative judgments even when there is the smallest hint of wrongdoing. A relatively minor offense in the grand scheme of things is often sensationalized by the press and television media. There should be no doubt in anyone's mind that security officers are held to high standards and essentially operate in a kind of fishbowl that magnifies minor shortcomings.

As a result, a security officer's conduct, both on and off the job, has to be exemplary. Any behavior that shows a disregard for what is correct and proper has to be avoided. The worst examples of unacceptable behavior on the job are the use of unnecessary force, preparing false reports and sleeping while on post.

Because security officers are the custodians of company and employee property, honesty is an absolute must. Courtesy and efficiency are essential qualities of a security officer. They are frequently the first to contact a visitor, customer, vendor, or employee. The manner in which the officer deals with people will have a marked positive or negative effect on the initial impression made by the security organization.

A security officer who is officious or careless in the performance of duties, or otherwise gives a bad impression, can have an adverse effect on the total protection program.



## A CODE OF ETHICS FOR SECURITY OFFICERS

*As a security officer I pledge:*

To accept the responsibilities and fulfill the obligations of my role: protecting life and property; preventing and reducing losses and crimes against my employer's business, or other organizations and institutions to which I am assigned; upholding the law; and respecting the constitutional rights of all persons.

To conduct myself with honesty and to adhere to the highest moral principles in the performance of my security duties.

To be diligent and dependable in discharging my duties and to uphold at all times the laws, policies and procedures that protect the rights of others.

To observe the precepts of truth, accuracy and discretion without allowing personal feelings, prejudices, and animosities or friendships to influence my judgments.

To report to my supervisor, without hesitation, any violation of the law or of my employer or client's regulations.

To respect and protect the confidential and privileged information of my employer or client beyond the term of my employment, except where their interests are contrary to law or to this Code of Ethics.

To cooperate with all recognized and responsible law enforcement and government agencies in matters within their jurisdiction.

To accept no commissions, gratuity or other advantage without the knowledge and consent of my employer.

To conduct myself professionally at all times and to perform my duties in a manner that reflects credit upon me, my employer, and the security profession.

To strive continually to improve my performance by seeking training and educational opportunities that will better prepare me for my security duties.

## **Part Two**

### **Legal Aspects**

**Arrest**

**False Arrest**

**False Imprisonment**

**Search Incidental to Arrest**

**Police Notification**

**Dealing with Violence**

**Necessary Force Only**

**Civil Liability**

**Physical Evidence**

# Arrest

## Arrest is Risky

Making an arrest is more prone to problems than that of any other task performed by a security officer. There are several reasons this is the case. First, the laws that regulate arrest are strictly enforced. Second, it is in the nature of the American culture to prize freedom so highly that when an improper arrest is made, public opinion falls heavily in favor of the arrested person.



If the law is clear on arrest and if society is disapproving of bad arrests, why do bad arrests occur? They occur because the person making the bad arrest lacks good judgment and/or does not understand the law in the first place.

### Arrest, According to Wikipedia

Arrest is the act of depriving people of their liberty, usually in relation to an investigation or prevention of a crime, and thus detaining the arrested person in a procedure as part of the criminal justice system.

Police and various other officers have powers of arrest. In some places, the power is more general; for example in England and Wales, any person can arrest "anyone whom he has reasonable grounds for suspecting to be committing, have committed or be guilty of committing an indictable offence," although certain conditions must be met before taking such action. Similar powers exist in France, Italy, Germany, Austria and Switzerland if a person is caught in an act of crime and not willing or able to produce valid ID.

## **False Arrest**



**False arrest is the detention of a person by another who claims to have official authority to make arrests when in fact he does not have that authority. Imagine a security officer whose only authority to make an arrest happens to be based on the private person arrest authority. He makes an arrest while telling or leading the arrested person to believe that he is a police officer or has the same arrest authority as a police officer. In addition to being charged with false arrest, the security**

**officer may be charged with impersonation of a police officer.**

**False arrest also occurs when an arrest is made absent a reasonable belief that the arrested person committed an offense for which an arrest can be made. Imagine a security officer hired to keep unauthorized people out of a gated community. The security officer sees a person get out of a car that does not bear a sticker that identifies the car as the property of a resident. The officer arrests the person for trespass even though the arrested person produced identification showing him to be a resident. In this example, the officer did not have facts that would cause a person of prudent judgment to believe that the arrested person had committed a crime.**

## **False Imprisonment**



**False imprisonment has nothing to do with prison. It is the unlawful restraint of a person's freedom of movement. False arrest and false imprisonment often occur together. A security officer could be charged with false imprisonment if he required a falsely arrested person to remain in a certain place or prevented the person from leaving.**

**False imprisonment is frequently an issue in the retail business when a security officer detains a suspected shoplifter.**

**If the detention is not based on a reasonable belief that the suspect shoplifted and the suspect is detained against his or her will, the security officer can be charged with false imprisonment, as well as false arrest.**





## Police Notification

**A security officer who makes an arrest is required to deliver or turn the offender over to the police with no unnecessary delay.**

**After the offender is in police custody, the security officer or the client (e.g., the owner or manager of a store) must sign a formal complaint. A follow-up procedure by the police may be to take a sworn written statement from the security officer.**



**A final duty is to testify at the offender's trial.**

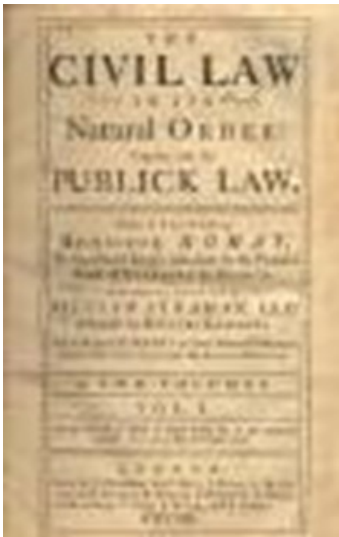
False imprisonment, also known as unlawful detention, occurs when a person is improperly restrained from leaving a location due to the improper actions of another person. In broad terms, false imprisonment occurs when one person intentionally restricts the freedom of movement of another person without their consent and without legal privilege. It is not necessary that the person be physically restrained.

Questions of false imprisonment often arise when a person is detained by a store security officer on suspicion of shoplifting and it is later shown there was insufficient evidence that shoplifting actually occurred.

The gravity of the error is greatly increased if the security officer failed to immediately call the police.



# Civil Liability



Civil liability occurs when one party (the plaintiff) has been injured, damaged, or wronged by another party (the defendant). A party can be a person, company, or organization. The plaintiff sues the defendant in a civil court where both parties explain their positions to a judge or jury. If the plaintiff prevails, the defendant may be ordered to compensate the plaintiff and also to pay punitive damages.

In civil law, your client and employer can be held responsible as well. A civil suit will almost always name the party with the "deep pockets" (i.e., the financial ability to make recompense). This is usually the client or employer. In defending the suit, the client or employer may choose to not stand by you, meaning that you must defend yourself alone and at your own expense. No matter what happens, substantial legal costs can be sustained by any or all of the defendants.

The central point: a security officer who commits a wrong against another can be tried in both a criminal court and a civil court. The civil trial, and any monetary payments ordered, can occur in addition to jail time and fines imposed by a criminal court.

## Something to Think About

- Fact 1. A security officer detained a shopper on suspicion of shoplifting.
- Fact 2. The suspicion was shown to be unreasonable.
- Fact 3. The female shopper sued the security officer.
- Fact 4. A civil court jury found the security officer negligent in his duties.
- Fact 5. The jury awarded \$100,000 punitive damages.
- Fact 6. The security officer mortgaged his home and settled out of court with a payment to the shopper in the amount of \$45,000.

## **Part Three**

### **Security Operations and Practices**

#### **Fire Prevention**

**Inspections**

**Response**

**Control**

**The Triangle Theory**

#### **Patrol Procedures**

**Foot Patrol**

**Mobile Patrol**

#### **Bomb Threats**

**Anti-Terrorism**



# Fire Prevention

---

## Response

Fire is the greatest cause of accidental injury, death and property destruction. The most common origin of fire is electrical origin.

During a fire emergency, a public- address system should communicate one of three messages:

- Evacuate
- Stand by for further instructions
- Return to normal work activities

Security officers should be skilled in:

- Detecting and correcting fire hazards
- Reporting fire conditions
- Notifying and assisting fire responders as needed
- Directing traffic to allow unhampered access of firefighting vehicles and equipment

## Control



**A slogan appropriate for a fire prevention program would be, “There are fire-resistant buildings but there is no such thing as a fire-proof building.” But fire prevention is more than a slogan; it is an integral part of your job. When practiced, it places into the center of your mind a permanent reminder to always be on the watch for fire hazards.**

**Fire control consists of the activities that occur when prevention fails. Unlike prevention, which relies on a mindset, control involves motor skills, stamina, and a good deal of common sense.**

**The security officer practices fire prevention every minute he or she is on the job. Certain patrol duties are exclusively aimed at detecting and correcting fire hazards such as looking for overloaded electric circuits, cooking appliances left on, and blocked fire escape routes.**

**These inspecting activities are planned and carried out purposefully, but the process does not end there. Keeping an eye out for hazards is a continuous, non-stop activity that should be as natural as breathing the air around you.**

## **Control (Continued)**



Prevention is also practiced when you inspect fire equipment such as to see if there is sufficient pressure in a hand-held fire extinguisher or that a piece of hose attached to a standpipe is not rotted. It is also present when you test the alarm system or participate in fire drills.

Fire control begins the instant fire is detected. The detection might occur as the result of an alarm sounding or of a person spotting fire or smoke and setting off the alarm manually. In either case, the security officer performs two actions: he or she calls 911 to report the fire, and then clears the area of people. A third action is called containment and it is possible if the fire is not fully out of control. Containment actions include using fire extinguishing equipment, moving flammable material away from the path of the fire, and closing doors to impede the spread of the fire.

The three important control functions of the security officer are:

- Ensure that the fire department has been notified.
- Evacuate people
- Contain the fire, if feasible

A modern building will have automatic fire controls such as heat and smoke detectors, a sprinkler system, louvers that expel smoke and noxious fumes, pressurized stairwells, and emergency lighting. The security officer should be trained in how these automatic controls function.

# The Triangle Theory



The law of physics requires that for fire to exist there must be:

- Heat
- Fuel
- Oxygen

Remove any of the three, and fire cannot exist. The methods used to prevent fire rely on this theory. In fire prevention, for example, we work against heat by keeping electrical wires from being overloaded or we turn off coffee pots that are not in use. We work against fuel by keeping volatile substances, such as gasoline and paint thinner, away from heat sources. In fire control, we fight against oxygen when we use a hand-held fire extinguisher that removes oxygen by dousing the fuel of the fire with a dry chemical.

## The Four Stages of Fire

Fire can be thought of as having a life of its own. In this life, fire goes through four stages:

- Incipient: There is no flame or smoke but the fire is alive, just waiting for more oxygen or fuel or heat.
- Smoldering: The fire has smoke but no flame.
- Flame: Smoke and flame appear together. This may be the last chance to bring the fire under control.
- Heat: Smoke, flame and intense heat appear together. At this point, the fire is raging.





## **Foot Patrol**

Foot patrol has all of the characteristics of mobile patrol except the use of a vehicle. The only obvious difference is that a walking patrol usually patrols indoors, except in circumstances such as checking a parking lot, monitoring deliveries and shipments at a loading dock, or directing employee traffic at morning and afternoon rush hours.

An active patrol is more likely to spot hazards before they become harmful such as a fire in the incipient stage.

Among the important duties of a security officer on walking patrol are:

- Looking for safety hazards such as coffee machines not turned off, overloaded wall plugs, and fire escape routes blocked with boxes and the like
- Looking for vehicles that are improperly parked such as a van left unattended close to the office building or vehicles that violate parking and speeding rules
- Monitoring work performed by a janitorial crew to prevent theft and compromise of sensitive information
- Looking for sensitive documents left unattended
- Looking for doors left open where they should be closed
- Looking for doors left unlocked where they should be locked
- Looking for suspicious activity such as a stranger, especially when the stranger is in an area where valuable assets are kept
- Reporting unusual conditions to the security center
- Checking louvers, valves and similar pieces of fire control equipment
- Checking the expiration dates of hand-held fire extinguishers
- Looking for burned out lights, especially in fire stairwells
- Testing emergency generators to make sure they are in operating condition
- Escorting visitors
- Escorting client employees when they are making bank deposits
- Using an electronic wand or similar device to clock-in at points along an established patrol route

## **Foot Patrol (Continued)**



**A patrol officer familiar with the layout of the protected property will know how to get to one place by the fastest route possible. The officer will:**

- Personally know employees working in the area and use them as a source of information as to suspicious activities**
- Be able to recognize strangers that need to be checked**
- Cover enough territory so that a lesser number of officers will be required to provide the same level of coverage**

**None of these techniques are possible without a patrol officer who:**

- Is mentally alert**
- Is dedicated to the work**
- Is knowledgeable about business operations on the protected site**
- Is knowledgeable about past crimes and how they have occurred**
- Is knowledgeable about current crime trends that could affect the property under protection**
- Is flexible in the nature of the patrol**
- Communicates clearly while on patrol, keeping the supervisor well informed of the patrol activity**
- Carefully inspects the patrol vehicle before going on shift**
- Prepares reports that can be helpful in a post-investigation or in the training of inexperienced patrol officers**
- Maintains good working relationships with law enforcement officers that patrol the area around the protected site and being proficient in contacting them when a crime occurs or a criminal flees from the protected site**
- Reports breaches in security such as a blown-out security lights or a hole in a perimeter fence**

# Mobile Patrol



There are two forms of mobile patrol: deterrent and aggressive. The objective of deterrent patrol is to discourage a potential criminal from attempting to commit an offense in the patrol's territory. The determined intruder is usually professional and relies on stealth to enter the protected area.

Direct attempts to penetrate the perimeter can be prevented by patrolling areas nearby the perimeter. And by ensuring that security lighting is working, the viewing distance of the patrolman is greatly increased. If the targets covered by a deterrent patrol are in a public area, such as a convenience store that operates 24 hours a day or a storage warehouse under lock during non-duty hours, the patrol officer should dismount, check with the cashier at the convenience store and rattle the lock on the storage warehouse doors and check windows for broken glass. An opportunistic criminal watching from a covert location may decide to concentrate his or her attentions at another company's location. This is called displacement of crime.

## **Mobile Patrol (Continued)**



**Mobile patrol, whether in the deterrent or aggressive modes, can be carried out in other vehicle types such as bicycle, motor scooter and golf cart.**

**A security officer on deterrent patrol should:**

- **Know the times of past security-related incidents**
- **Patrol randomly**
- **Be on the alert for suspicious persons**
- **Be prepared to encounter violence and know how to summon law enforcement without delay**
- **Know the names of persons operating law enforcement patrols and the boundaries of their patrol activities**
- **At the earliest possible moment, even during the “suspicion” stage, contact the base station and ask for a standby unit to respond if needed**

**Aggressive patrol is appropriate when criminal actions are frequent. This does not mean speeding or engaging in reckless driving. It means:**

- **Being extra alert**
- **Anticipating that a criminal attempt will be made and knowing where**
- **Patrolling with higher frequency in the areas where crimes have occurred**
- **Asking for a patrol rider to assist in case a crime in progress is spotted**

# Bomb Threats

The proposition is well accepted that security officers are vested with responsibility for responding to bomb threats. Even when there has been no history of threats and no reason to believe the organization has become a target, security officers must anticipate the possibility.

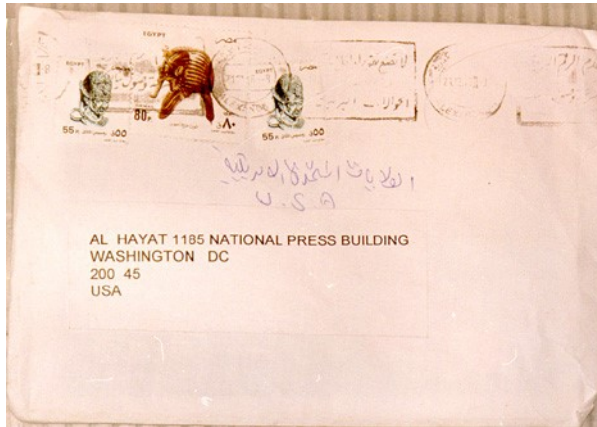
The security officer force can:

- Control suspect packages entering the workplace.
- Conduct periodic inspections of the workplace to identify areas where a bomb could be planted with minimum chance of detection and at the same time cause major property damage or personal injuries. The areas to think about are the facility's power plant, flammable storage rooms, telephone switching center, computer room, and executive offices.
- Be alert for suspicious persons and activities in areas that are accessible to the public, offer bomb concealment opportunities, and are sensitive in terms of damage and/or injury.
- During each tour of duty make random checks of public areas to look for unauthorized persons who may be hiding in or reconnoitering the facility





## Bomb Threats (Continued)



**An intelligent and determined adversary is likely to find a chink in even the best defensive armor. Without considering the elaborate schemes, some of the readily available means for introducing a bomb into a workplace are: on the person of an employee, by postal or commercial delivery service, and by motor vehicle into the facility's garage.**

**Once inside, placement of a bomb is mainly a matter of the attacker's nerve and knowledge of the premises. The attacker might choose to place the bomb in a rest room, janitor's closet, stairwell, receiving platform, lobby, or elevator.**

**A bomb threat is rarely made in person and sometimes is transmitted in writing. A bomb threat in writing should be handled carefully, touched by as few persons as possible and the envelope or any other accompanying materials preserved as evidence. Observing these simple precautions can be extremely helpful to a post-incident investigation.**





**As a general rule, material greed and unmet psychological needs are not motivators for ideological groups, although groups have a history of resorting to robbery and kidnapping to acquire operating revenue.**

**Group tactics can range from highly terroristic acts, such as bombings and assassination, to purely symbolic acts, such as splashing blood on walls or burning a flag in a very public place.**

**The ideologue may or may not be skilled, is likely to be intelligent, very likely to be strongly committed and dedicated, and willing to take chances and suffer the consequences of being caught.**

There is no universal agreement on the **definition of terrorism**. Various legal systems and government agencies use different definitions. Moreover, governments have been reluctant to formulate an agreed upon and legally binding definition. These difficulties arise from the fact that the term is politically and emotionally charged. In the United States of America, for example, Terrorism is defined in Title 22 Chapter 38 U.S. Code § 2656f as "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents." According to some:

- It is the use of violence or threat of violence in the pursuit of political, religious, ideological or social objectives.
- It can be committed by governments, non-state actors, or undercover personnel serving on the behalf of their respective governments.



## **Terrorism (Continued)**

**Terrorists, whether domestic, international or motivated by religion, regard senior business executives as logical targets. A person, deranged or motivated by revenge and/or the desire to gain attention to a cause, may attempt to place a bomb aboard or otherwise sabotage the plane or automobile used to transport an organization's top management.**

**U.S. businesses, both at home and overseas, are targets for kidnapping and other acts of violence. Terrorists use vi-**

**olent methods to force changes to business practices, to shape public opinion, and to bargain with governments for relief from prosecution and incarceration of their brothers-in-arms. Terrorists, as well as ordinary criminals, also use kidnapping as a means for acquiring money.**

## **Part Four**

### **Security Operations and Practices (Continued)**

#### **Medical Emergencies**

- CPR**

- Loss of Consciousness and Asphyxiation**

- Severe Bleeding**

- Burns**

- Electric Shock**

#### **Crowd Control**

- Channeling**

- Multiple Venues**

- Site-Specific Tasks**

#### **Systems and Equipment**

- Access Control**

- CCTV**

- Alarms**

- Fire Detection**

- Security Lighting and Fencing**

- Locks**



# Medical Emergencies

## CPR



Cardiopulmonary resuscitation is used to restore the heartbeat in a victim whose heart has stopped. CPR combines artificial respiration with external heart massage to keep blood flowing through the victim's body. The responder positions the victim face up on a firm surface and clears the airway.

The victim's head is tilted back and the chin lifted forward. The responder then gives the victim two breaths by mouth. If no pulse is detected at the carotid artery (located in a groove beside the windpipe in the neck), the responder kneels next to the victim and places the heel of one hand on top of the other over the lower half of the sternum. The responder depresses the chest about 2 inches, which forces blood from the heart into the victim's arteries. When the pressure is released, blood flows back into the heart. The responder applies the pressure in short, rhythmic thrusts about 15 times every 10 seconds. Two breaths followed by 15 chest compressions is repeated until the victim revives or medical help arrives.



# **Medical Emergencies (Continued)**

## **Loss of Consciousness**

**This condition occurs when the brain does not receive enough blood. In restoring blood flow to the brain, the responder elevates the unconscious person's feet or lowers the head below the height of the heart. The victim is also kept warm to prevent shock. Loss of consciousness may result from a variety of causes, including head injury and epilepsy. If the victim is breathing, the assistance is limited to providing comfort until medical help arrives. If the victim is not breathing, the responder administers artificial respiration.**

## **Asphyxiation**



**Cessation of breathing can cause brain death within 4 to 6 minutes unless relief is administered. Asphyxiation occurs when air cannot reach the lungs, cutting off the supply of oxygen to circulating blood. Among the causes of asphyxiation are drowning, gas poisoning, overdose of narcotics, electrocution, choking, and**

**strangulation. Victims may collapse, be unable to speak or breathe, and have bluish skin.**

**The most common technique for preventing asphyxiation is artificial respiration (the mouth-to-mouth technique) in which the first-responder forcefully exhales air into the victim's lungs after first clearing the airway. In a case of drowning, artificial respiration should be attempted even if the victim appears dead. People submerged in cold water for more than 30 minutes have responded to artificial respiration and recovered with no brain damage.**

## Medical Emergencies (Continued)

### Severe Bleeding

The mere presence of blood does not always indicate severe bleeding. Well-ing or spurting blood is a clear sign of severe bleeding. If a major artery ruptures, a person may bleed to death within a minute. Injuries to veins and minor arteries bleed more slowly but may also be fatal if left unattended.



Shock usually follows loss of blood, and must be prevented as soon as the bleeding has been stopped. Bleeding is stopped by applying pressure directly over the wound and, when possible, elevating the bleeding body part. The responder should hold a sterile dressing or clean cloth firmly over the wound.

If the bleeding is from an arm or leg, the responder can reduce blood loss by applying pressure at a point adjacent to the bleeding called the pressure point. Arteries pass close to the skin at these points and can be compressed against underlying bone to reduce bleeding.

### Signs of Shock

Agitation, restlessness and anxiety	Nausea or vomiting
Altered mental status	Change in pallor, cyanosis
Clammy skin	Thirst
Weak, thready or absent pulse	Narrowing pulse pressure



# Medical Emergencies (Continued)

## Burn

A burn is an injury to the skin caused by exposure to fire, hot liquids or metals, radiation, chemicals, electricity, or the sun's ultraviolet rays. Burns are classified according to the depth of tissue damage and extent of the burn. A first-degree, or superficial, burn, which involves only the surface of the skin, is characterized by reddening. A second-degree burn extends beneath skin surface and causes blistering and severe pain. A third-degree burn causes charring and destruction of the cell-producing layer of skin.



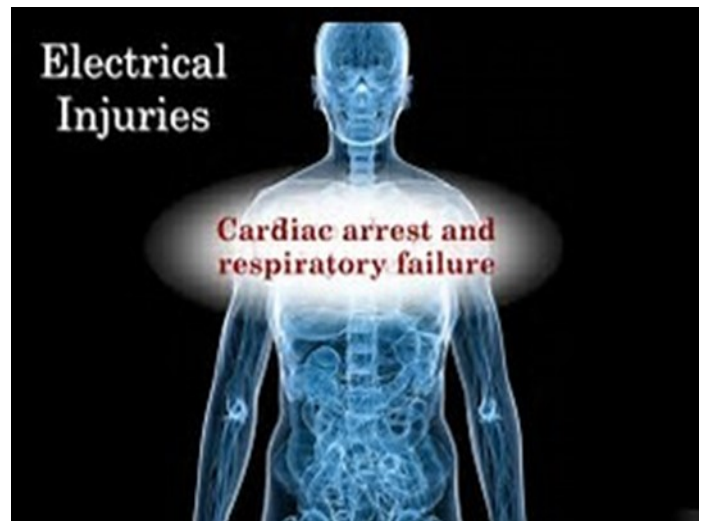
First-response actions are:

- Remove the source of the burn as quickly as possible.
- Immediately cool the burn with cold water.
- On less serious burns apply a clean, cold wet towel or dressing to ease pain and protect against contamination.
- Treat a chemical burn by continuously bathing it with running water for at least 20 minutes. Do not use wet dressings and ointments.
- Apply dry, sterile dressings held in place by bandages.

# Medical Emergencies (Continued)

## Electric Shock

Contact with electrical current is often fatal. Electricity passing through the body can cause serious injury to internal organs. If electricity passes through the heart, the heart's muscle may be damaged and its rhythm interrupted, leading to cardiac arrest. The severity of the injury depends on the strength of the current and the path it takes through the body.



The responder to a victim of electric shock should not touch the victim's body before the source of the shock is turned off. If the victim has stopped breathing and has no pulse, CPR should be administered.

Electric shock occurs upon contact of a body part with any source of electricity that causes a sufficient magnitude of current to pass through the victim's flesh, viscera or hair. Physical contact with energized wiring or devices is the most common cause of an electric shock. In cases of exposure to high voltages, such as on a power transmission tower, physical contact with energized wiring or objects may not be necessary to cause electric shock, as the voltage may be sufficient to "jump" the air gap between the electrical device and the victim.

Some of the causes of electric shock include:

- Faulty appliances
- Damaged or frayed cords or extension leads
- Electrical appliances coming in contact with water
- Incorrect or deteriorated household wiring
- Downed powerlines
- Lightning strike.

# Crowd Control



# Channeling

In emergency situations, a common procedure in crowd control is channeling people in safe directions such as away from the center of a fire or explosion. In protest marches, crowd control is focused on controlling people inclined to attack the marchers. In a riot situation the objectives may be to identify the leaders, photograph them for post-incident investigation, not escalate the situation, not directly engage the rioters, wear protective gear, and try to split the crowd by channeling some rioters down one street and others down another street.



**Riot control** refers to the measures used by police, military, or other security forces to control, disperse, and arrest people who are involved in a riot, demonstration, or protest. If a riot is spontaneous and irrational, actions which cause people to stop and think for a moment (e.g. loud noises or issuing instructions in a calm tone) can be enough to stop it. However, these methods usually fail when there is severe anger with a legitimate cause, or the riot was planned or organized.

Officers performing riot control typically wear protective equipment such as riot helmets, face visors, body armor (vests, neck protectors, knee pads, etc.), gas masks and riot shields.



# Multiple Venues

The need for crowd control exists in many circumstances.

- Sporting events
- Concerts
- Parades
- Speeches
- Political rallies
- Religious gatherings
- Protest marches
- Riots
- Civil disturbances



A problem in achieving effective crowd control is that every event will have its own set of problems and procedures to follow. For example, controlling a crowd watching the Pope pass by in a slow-moving limousine will confront risks that require protective procedures distinctly different than controlling a crowd leaving a Kiss concert.

## Research into Riot Control Weapons

- Netguns are non-lethal weapons designed to fire a **net** which entangles the target. Netguns have a long history of being used to capture wildlife, without injury, for research purposes.
- Pepper-spray projectile launchers fire a fragile ball which breaks upon impact and releases an irritant pepper.
- Stink bombs create an extremely unpleasant smell. They are believed to be less dangerous than other riot control chemicals.
- Sticky foam weapons immobilize rioters with a gooey foam.<sup>[9]</sup>
- Low frequency sound cannons incapacitate subjects using a focused beam of sound.
- Dazzler lasers use intense light to cause temporary blindness or disorientation of rioters.

## Special Equipment



Some security guard companies specialize in crowd control. They possess communication equipment, a mobile control center, portable CCTV systems for monitoring crowd movements, electronic wands for identifying persons carrying concealed weapons, bull horns, stanchions, and other equipment and devices. They also employ security guards that have been trained and are experienced in controlling crowds.





# Site-Specific Tasks

A first step for the security officer after going on the job is to learn the:

- Geographic layout of the site
- External and internal features of structures
- Nature of business operations at various locations within the site
- Entry and departure points
- Location and functions of physical security equipment such as:
  - Perimeter fencing
  - Lighting
  - Intrusion detection sensors
  - CCTV.
- Names and physical appearances of the client's key persons



## Property and Persons to Be Protected

The client's property you are responsible to protect can be almost anything: money, jewelry, merchandise, gold, stocks and bonds, sensitive information, real estate, physical structures and their contents, people, etc. Some assets are more valuable than others. The very valuable assets are called critical assets. A critical asset is one in which the loss of the asset will have serious negative consequences such as delay, interruption or cessation of business operations. Therefore, the higher the criticality, the higher the

protective shield must be.

An employer may identify employees as the company's most critical asset. Without them, the company cannot operate. This explains the importance of hazards detection, fire and accident prevention, medical emergency response and violence directed at persons.

# Site-Specific Tasks (Continued)

## Policies, Plans and Procedures

Site specific tasks are set out in writing in the form of security operating procedures, policies, and plans. Such tasks can include:

- Becoming familiar with the layout of the protected premises and key persons working for the client
- Controlling the movement of persons, property and vehicles that are within, leaving and entering the protected premises
- Operating a visitor reception desk
- Patrolling on foot and by vehicle
- Controlling entrance to sensitive areas
- Identifying and correcting hazards
- Escorting such as escorting client employees to a bank
- Examining suspicious packages
- Searching for dangerous items such as a bomb
- Notifying and assisting emergency response agencies such as police, fire fighters, EMT specialists and hazardous material specialist
- Suppressing and extinguishing fire in the incipient stage
- Maintaining incident logs and writing incident reports

### Policies, Plans and Procedures: What are They?

Policies are created at the upper levels of an organization. They give broad direction. For example, a security policy might say, "It is our policy to maintain a workplace free of drug and alcohol abuse." This policy would require the organization's security manager to develop, in coordination with other managers, a plan that meets the intent of the policy. The plan could include background checking of job applicants, pre-hire and random drug testing. Supervisors who report to the plan managers would write procedures that carry out the plan. Procedures that apply to guard operations might instruct security officers to be on the lookout for drugs and alcohol on the premises, among many other instructions.

## Systems and Equipment



# Identification, Detection and Control Equipment

The most basic method of access control is personal recognition, i.e., recognizing the personal features of persons as a means of allowing them entry. This method is limited to no more than about 50 persons and is generally unreliable.

Next is the use of badges or identification cards. Badges are typically worn on an outer garment. The badge for a permanent employee typically has a photo on it and is laminated. A visitor badge is typically dated for use within a limited time frame.



Card keys can serve as both a form of personal identification and a tool for passing through a door controlled by an electronic reader. Card keys are of different types: stripe or magnetic card that works like a credit card; the proximity card is passed in front of a reader; the Weigand card contains dots inside layers of lamination; bar code card; and punched hole card.





# Physical Security



Guard operations are augmented by physical safeguards such as fences, lighting, sensors, CCTV and signage.

The most common form of perimeter protection is the chain link fence. The fence is 7 feet high; has three strands of barbed wire or razor ribbon at the top and facing outward.

The bottom of the fence is beneath the soil. In sandy soil the bottom of the fence must be sufficiently deep to prevent crawling under. Where a fence crosses a culvert, the open space below the fence must be enclosed with heavy wire mesh or closely spaced bars.

Fence posts are ten feet apart with a horizontal post connecting the posts at the mid-height of the fence.

Perimeter fences are often augmented with sensors and lamps.



# Security Lighting

Lighting on a perimeter is directed outward to make visible an approaching intruder. Glare lights can make it difficult for an intruder to see what is ahead.

Lighting on a building illuminates entry points such as doors and windows.

Lighting is used in support of closed circuit television cameras.

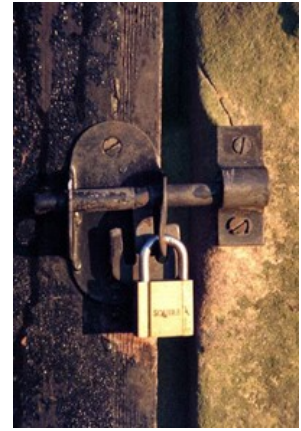
Roadway and parking lot lights are elevated and light poles are spaced so that cones of illumination overlap to eliminate shadow areas.

Offices, factories, warehouses and other structures of a critical nature are protected by security lights. They are physically resistant to brute force entry such as breaking down a door or smashing through an exterior wall. Within the outer sheath of the structure can be sensors that react to movement or sound.

Within structures are access-controlled areas which have lights that go on and alarms that activate when unauthorized entry is detected.



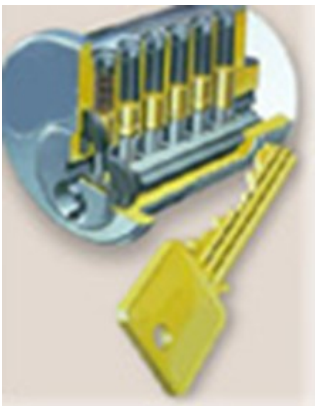




## Locks

**Locks are nothing more than delay devices. Types of locks include key locks, pad locks, combination locks, cypher locks and electronic bolt release lock. A cypher lock looks like the press pad on a burglar alarm system. Pressing the correct numbers on the pad releases a door lock. The electronic bolt release lock allows a person behind a locked door to press a button that disengages the lock bolt.**

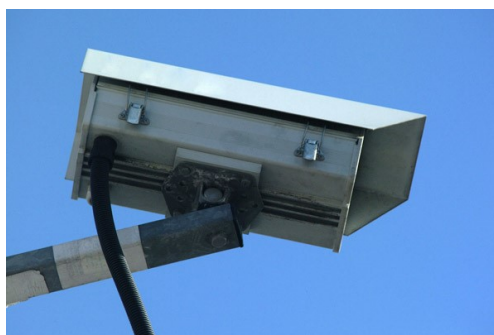
**The fact is that a lock can be defeated in one way or another--but time is a factor. A lock that delays entry for a long period of time (such as a minute) is considered a high-security lock. Locks are used to prevent opening of doors, windows and containers. Keys to locks are often kept in a security center for emergency use.**



# Defense in Depth



To understand this concept it helps to think of an onion. Getting to the center of the onion requires removing one layer at a time. In security work, the layers are detection and delaying safeguards. The first safeguard could be underground (seismic) sensors that react to pressure on the surface of the ground; motion (capacitance) sensors that react to touching a chain link fence; barbed wire atop a 7-foot high fence; double fences erected parallel to create a “dead man zone” between them; CCTV cameras that react to movement in a field of view and transmit a signal and an image to the security center; microwave beams that activate when a beam is interrupted; lights on the outside of a structure; locked exterior doors and windows; locks on interior doors; and locked file containers, safes and vaults, augmented with sensors. To be successful, the intruder would have to get by a series of safeguards--like the layers of an onion.



## **Part Five**

### **Interpersonal Communication**

**Spoken Words and Body Language**

**Interpersonal Dynamics**

**Modes of Communication**

**Courtesy, Tact, Diplomacy and Patience**

# Interpersonal Communications





# Spoken Words and Body Language



Interpersonal communication relates to participants who are dependent upon one another and have a shared responsibility such as security officers dependent on each other to effectively carry out their duties. There are two forms of interpersonal communications: spoken words and body language. The first is the normal form, assuming of course that the sender and receiver speak the same language. The second form, body language, is less obvious. Body language includes facial expressions, eye movements, gestures, and the like.

Body language is usually recognized subconsciously by the receiver, and is not always under direct control of the sender. The sender may inadvertently reveal one's true feelings toward the receiver unintentionally and thereby either taint or bolster the believability of a verbal message. Subconscious reception and interpretation of these signals is often described with arbitrary terms like gut-feeling, hunch, or premonition.



# Interpersonal Dynamics

There is a natural interplay between people on a day-to-day basis. For example, security officers interact with:

- Each other in the performance of their tasks
- Persons
- Employees of the client
- Visitors, guests and vendors that enter, move within, and depart the protected premises
- Police officers, firefighters, emergency medical technicians and other people associated with the security program
- Lawyers and judicial officers in matters of crime and restitution
- Religious figures





# Communication Modes

The modes of communication between security officers and their normal contacts include:

- Face-to-face
- Radio
- Telephone
- Voice mail
- E-mail



Each of these modes has a set of protocols. In the face-to-face mode the security officer is expected to be neat in appearance, professional in demeanor, tactful, knowledgeable, and responsive.

Talking by radio requires the operator to use short and plain sentences. Depending on the preferences of the employer and/or client, a code system, such as the Ten Series, can be a protocol.

Telephone protocol requires answering calls with a polite statement such as, "This is the security center. May I help you?" Other requirements are taking messages, passing them to the correct persons, and making return calls promptly.

Voice mail, whether sending or responding, requires clear and concise language, and a tone of voice that conveys a professional interest in the matter at hand.

E-mail messages should be written without shortcuts such as writing in lower case only and using a combination of letters in lieu of the words they represent.

Sending and receiving personal e-mail is also prohibited, and with some employers is an offense that can result in disciplinary action, including termination.

**Courtesy**

**Tact**

**Diplomacy**

**Patience**

**A stand-out characteristic of the professional security officer is the manner in which he or she deals with other persons, whether the client, the client's employees, guests, visitors and vendors, and coworkers.**



+++++

**Courtesy is simply a matter of showing respect such as by saying “sir,” “ma’am,” and “thank you.” It is also showing respect with actions such as opening doors for females and offering help to others.**

**Tact is not arguing with someone, even when you know you are right. Tact requires a little bit of cleverness because it means thinking ahead of a situation and acting in a way that makes the other person believe he or she is in the right, although you know better.**

**Diplomacy is tact by another name. It is the final and unwelcome stage that precedes disagreement. Diplomacy is non-threatening behavior for keeping a bad situation from getting out of control.**

**Patience is sometimes called a “virtue,” and rightly so because it comes from inside you. Not rushing ahead without thinking; being able to put off what you’d like to do; and waiting for the right moment to act.**



**This e-manual is the product of Learning Shop USA, a school that provides online training for security officers, process servers and private investigators.**

**For information on how to acquire this and other LSUSA publications and how to enroll in online courses acceptable to state regulatory boards for license issuance or renewal please feel free to visit our website at [www.learningshopusa.com](http://www.learningshopusa.com) or make contact with us via [learningshopusa@gmail.com](mailto:learningshopusa@gmail.com) or 706 268 2221.**

(Copyright, 2018)