

## MODULE 3: BASIC SECURITY PROCEDURES

- **Preview** Security Guards should be familiar with site procedures to handle diverse situations they encounter during performance of their duties. Normally, all sites have comprehensive guidelines reflected in the 'site orders'. All security officers must read these orders and follow them in letter and spirit. This chapter will cover general aspects to facilitate new security guards to perform their duties efficiently. The subject will be covered in following parts :-
  - **Part I** Professional Conduct
  - **Part II** Procedure for Shift Take over/ Handover
  - **Part III** Key Control Procedures
  - **Part IV** Access Control Procedures
  - **Part V** Patrolling and Surveillance

### Part I Professional Conduct

- **General** *A security guard is expected to project an image of professionalism at all times. During the course of his/her duties, a security guard will often be visible to, and interact with, a variety of persons, including customers, visitors, employees, tenants, and the general public. Because they constitute by far the largest segment of the security industry, and because of their visibility and interaction with the public, the conduct of security guards is vital to the maintenance of a professional image for the industry as a whole. This Part will review the general personal qualities and human relations skills required of a security guard in performing his/her duties.* With the recent growth in the security industry, the tasks that have been assigned to security have significantly changed. Government regulation of the security industry has introduced not only a screening mechanism to control who may become a security guard, but also to investigate complaints about individuals and companies that have been licensed by the program. Liability concerns (both criminal and civil liability for excessive use of force and other errors) and the fear that legitimate users will be reluctant to patronize premises ruled by an aggressive security force have further changed the attitudes of many clients.
- **Expectations from Security Officers** The Security guards are expected to perform a variety of complex functions with discretion, diplomacy and tact. Guards are expected not only to look more professional, but also to have a greater knowledge of the laws and policies related to their industry. Some of these expectations are :
  - Acting in an honest and ethical manner at all times
  - Being sensitive to people with special needs, different backgrounds, communities and cultures
  - Possessing knowledge of criminal law, and their powers and responsibilities under it
  - Possessing knowledge of their employer's policies, and the policies of the client, in order to act in accordance with them;
  - Being well-trained and able to respond quickly and appropriately to the routine situations they will encounter every day on the work site.

- If emergencies arise, security will not panic but provide assistance to those in need
- Being properly attired and neat and clean in appearance
- Acting in a disciplined and professional manner, even when encountering difficult people or when placed in difficult situations, treating all people with respect and dignity.
- **Security Guard's Conduct, Deportment and Attitude** Security guards are the first point of contact for any visitor on the site. They must reflect a positive body language to create favorable impressions on visitors. Following guidelines are recommended to achieve this aim :
  - **Tone and Volume** These factors are often as important as what is said. Think, for example, of the variety of inflections that can be placed on the words "Thank You." Sarcasm can turn words that would diffuse a situation into an insult designed to inflame. While loudness may be one of the verbal cues that we may use to emphasize a point, often it is interpreted as aggression. Tone and volume are especially important when dealing with people over the telephone where nonverbal cues are not available to help them interpret your reaction to the situation.
  - **Stance and Posture** Unless guarded carefully, the body is often a reflection of what is in one's mind. For example, imagine a situation in which a Security Guard has encountered a person who wishes access to a site. During the encounter, the guard has blocked access by placing his or her back to the gate or doorway and stands erect, arms crossed, and legs firmly set. The body language of the guard clearly states, "You will have to go through me to get onto this site." The visual messages being communicated here are much different from a picture in which the same uniformed officer is having a conversation with the same person, sitting on a chair at the side of the doorway, with legs crossed and arms relaxed. The point is that our body language says as much as our words do, and a guard must recognize that he or she may be communicating in ways that they he may not be even aware .
  - **Facial Expression** The face also often provides a window to what a person is thinking. A person who has lips pressed together, brows furrowed, and is wearing a scowl or frown on his or her face presents a much different picture than the person who smiles, and whose face is relaxed and open. The guards should be aware of the messages they are presenting and be able to read the messages of a person they are dealing or communicating with.
- **Obstacles to Good Public Relations** There are common obstacles confronting the average security guard in his or her daily work that make for poor security public relations. Many Security Guards fail to recognize these factors in advance, and as a result, either fail to provide an adequate level of service or make their jobs more difficult than they have to be. Some of the barriers to good public relations are:
  - **Suspicion** A security guard is employed for one purpose – to protect people and/or property. The nature of the job or the personality of the guard may make a Security Guard act in a suspicious manner. While this may seem to be desirable – at face value, it seems to make for a good Security Guard – in the long run, it can become an obstacle to the ability of a Security Guard to get along with people. Suspicion can cause the guard to distrust everything and everybody. The people with whom the security guard deals will be able to see this attitude clearly, making interaction difficult. This quality, manifested in an obvious way, presents an obstacle in good relationships with the people the guard encounters.

- **Negative Thinking** Looking for things that may be wrong is a part of a Security Guard's job. This may, unless controlled, become an obstacle to better public relations. It is our business to be critical, but we may tend to find ourselves always looking for things that are not right. We overlook things upon which we can compliment in our search for things to criticize. If a security guard has to say "No", it should be communicated in a dignified, polite and professional manner rather than being offensive or belligerent.
- **Temper** One of the main reasons some Security Guards fail to get along with people is that they get angry – and show it. It is the cardinal rule of salesmanship that you never get mad at the customer. "**customer is never wrong**" Remember that the best weapon you can hold, when you are angry, is your tongue. If you show your anger, you have lost the argument.
- **Lack of faith** Security Guards must have faith in their superiors, the people who, to some degree, control their future. Security Guards must also have faith in them self and faith in what they are doing. There will be times when they will question if the work is worthwhile – is it being appreciated. They will need to reaffirm their faith in the mind of the public. When you build faith in the mind of the public, you give people good reason to pay you what you deserve. You can only build faith in the public mind when you have faith in yourself.
- **Prejudice/Discrimination** A Security Guard like anyone else is a human being. He/she possesses his/her own natural likes and dislikes. Unfortunately, from a security public relations point of view, these decisions are seldom based on the impression that the person has made at the moment, but is usually based on some past experience, bias or attitude. This seems to be a human trait and there is little we can do about our immediate reaction to people. But we can discipline ourselves to be fair and just in our dealings with people in spite of our personal prejudice, and if you can start off by trying to like the person you will do a better job in public relations.
- **Lack of Pride** Pride is defined as having a sense of personal dignity and worth, having honorable self-respect. *Esprit de Corps or pride in the Guard Force* is the common pride of individuals to a group. A Security Guard fails his/her other colleagues if he/she does not have pride and shows it. A Security Guard has the right to be proud to be a Security Guard, pride in himself and pride in his/her force. A Security Guard who becomes slovenly in dress, sloppy in reporting or unkempt in personal hygiene is demonstrating to everyone a lack of pride in himself/herself. An officer who shows that he/she has pride in his/her appearance will also have pride in person and outfit. He/she will create a better impression and do a better public relations job.
- **Lack of flexibility** A Security Guard should be a diplomat in uniform. A diplomat must be flexible, tactful and quick to adjust to changing conditions. The work of a Security Guard ranges from challenging or detaining possible thieves to relaying messages for a company president. It requires constant physical and mental effort on the part of the Security Guard to be flexible enough to fluctuate between these two extremes. A Security Guard on one day may be guarding an individual gem show, open only to the elite of society; the next day he or she may be guarding heavy equipment or a worksite. The Security Guard must be able to change procedures and attitudes as the clientele changes. It takes a flexible, easily

adaptable person to become a diplomat; it takes the same thing to become a good Security Guard. It requires constant self-discipline.

- **Abuse of Power (or Position)** Imagined power can be a very dangerous weapon. By the very nature of the work and the uniform, the Security Guard appears to many to have power and authority. What power and authority a Security Guard has must be used sparingly, carefully and judiciously. Unfortunately, some Security Guards forget that even the limited powers they have apply only under certain circumstances. At all other times they are governed by the same rules and regulations as other employees and members of the public.

## **Part II Procedure for Shift Take Over/ Handover**

- **Shift Takeover Procedure** Arrive at least fifteen minutes prior to the start of the shift so that you can:
  - Obtain keys and check equipment like Cell phone, Radio, Memo book/Post orders/Daily log book
  - Receive verbal briefing from the outgoing staff or client contact and read his report
  - Understand pending jobs like visitors in, tele-requests, maintenance requests, emergency procedures in progress etc
  - Check in with security office (dispatch) and report to designated supervisors of client and the security company
- **Shift Handover Procedure** At the end of your shift, be sure to:
  - Complete all reports
  - Provide briefing to the oncoming staff or client contact
  - Check out with Security Company dispatch.
  - Hand over all equipment in good order to the oncoming staff and have the individual inspect and sign your report that they received it in good order
- **Who to Call for Support During Emergencies** It is imperative that each security officer knows who to call and for what reason. This information is available from the client either written in the duty brief or post orders that are normally kept on the site. When in doubt... Call supervisor/ dispatch to clarify rather than initiating a doubtful response to manage the situation.
  - **When to call Police** It is recommended to call Police whenever you observe criminal activity, encounter refusal to take directions, detection that a crime has occurred such as a car break in, vandalism, etc. or when anyone threatens you in any manner - verbally, with gestures or use of any object or threat with an animal/pet.
  - **When to call Security Company** Whenever in doubt, you must call your company for guidance. You can call them upon arrival and completion of each shift ,when requested to perform hourly call-ins, when someone is late to relieve you, when any Special Occurrence Report is generated for any incident, if any equipment is lost, stolen or broken, to receive and confirm schedules, to order equipment or to report any concerns.

### Part III Key Control Procedures

- **Trust and Responsibility of Security** Normally, security has the master key and access to the entire building in off hours. All the values and valuables of clients are in 'trust of security' The key control and access card control are the backbone of security procedures. All security guards must know key control procedures to honor this 'trust and responsibility'
- **Key Control Procedures** Normally, the key control guidelines are available in site orders. However, it is recommended to follow these general guidelines :
  - Record in logbook and sign for the keys received at the start of shift. Have your relief sign for them when you go off duty.
  - Keys must always be accounted for. All key transfers must be recorded for time and place and signed for.
  - Always read orders for key handling and follow them in letter and spirit.
  - Carry and handle keys with utmost care. They should always be secure and never removed from the key ring.
  - Never lend keys even for a few minutes. If a person needs the key, escort him to location and record in log book.
  - Report any key related problems in daily/special occurrence reports.
  - Any keys that are lost must be reported immediately. There is heavy liability for loss of key/master key wherein client has the option to change the entire access control system and bill it to the security company.
  - Security guard must watch for persons issued with keys in off hours. A vendor may have an official access to facility but can misuse access control authority. All vendors, even if they have authorized access, must be escorted when they visit on site in off hours for any reason like overtime or to retrieve their tools etc.
  - Access control card should be treated at par with key control procedures.

### Part IV Access Control Procedures

- **Aim of Access Control** The aim of access control is to control the movement of people, materials, and vehicles into, out of, and within an area to ensure that right person/material is allowed into the right area at the right time. Access control is one of the primary functions of security. Security needs access control systems to control traffic into, within, and out of an area, whether it is a building, a parking area, a residential complex, or other facility.
- **Access Control Levels** There are three levels of access control :
  - **Minimum Access Control** This type of control is used at sites that allow general admission, such as malls. It assumes everyone is entering for lawful purposes. People are only denied entry by the security guard if rules are not followed or the law is broken.
  - **Medium Access Control** This type of control is often used at office or residential buildings. The security guard or someone in the building may use an intercom to allow access to the property. The intercom system may discourage someone from coming in, but if they really want to get in they can enter behind someone who has authority to enter the building.

- **Maximum Access Control** This type of control is found at sites with high security, such as some government offices, labs, military bases, software manufacturers, etc. Sites like these use a combination of security personnel and alarm systems to have total access control in all parts of the property.
- **Types of Protection Systems**
  - **Point of Entry Protection System or Perimeter Protection System** The goal of introducing a perimeter protection system is to ensure that an intruder is detected immediately upon entering the property. It acts as first line of defense to regulate access. e.g. Access booths, gates, fences and walls
    - ✓ **Partial Perimeter System** If the outer perimeter has detection devices on only the accessible openings – like windows, doors, and gates – it is termed a partial protection system.
    - ✓ **Complete Perimeter System** *a complete system, in contrast, includes detection devices in these areas as well as in the walls, floors and ceilings.*
  - **Area Protection System** Area protection systems are more commonly found in the inner perimeter and central core areas of premises. They act as the second line of defense against intruders. Instead of detecting the opening of a door, window or gate, an area system detects intruders once they have actually entered the premises. Examples - motion detectors, pressure plates, audio detectors and photoelectric cells.
  - **Point or Spot Protection System** They are used to monitor access to specific valuable objects in the premises. They act as the third line of defense in a layered protection system. Bank vaults, paintings in art museums, and so on, are objects that may have sensors attached, or may be surrounded by audio and infrared detectors and other security mechanisms.
- **Access control Areas**
  - **Outer Perimeter** Access control generally starts with the **outside perimeter or property perimeter** of the premises, where the property that is being guarded begins. As one progresses from the outer perimeter to the centre of the protected site, access control mechanisms generally are harder to breach.
  - **Inner Perimeter** Once inside the outer perimeter, one finds the **inner perimeter or building perimeter** and the **central core or interior of the building**. The inner perimeter consists of all common areas within the entire protected property, while the central core represents the central area that the property owner wishes to be protected.
- **Methods and Technology Used to Control Access/Egress**
  - **Entry Through Security Guard or Manned Access** Security takes post on main entrance to check identification and decide if people are authorized to enter. Following options exist:
    - ✓ **Personnel Recognition** This is often used at small sites. You let in only people who you recognize. Staff tells you if they are expecting any visitors. You use a special form to write down information about visitors. This method only works if you know each person who enters and if you see each person enter. If your attention is

somewhere else or you don't have time to identify everyone, unauthorized people may enter.

- ✓ **ID Systems** Many government offices use this method. All employees show their ID card before entering. Insist on Govt Issued ID. Security checks each ID card carefully. Things to look for are: Photo and physical description of the holder, Full name and signature of the holder, The Company's name and an issuing authority's signature, expiry date and Serial number (for the card itself or an employee number).
  - ✓ **Special Passes** In high security areas, security may allow only people with special passes or badges to enter. Such passes may be specially designed for a particular event or may be used to access high security zones in a premise. Always maintain proper record of issue of passes. In sites with maximum access control, visitors may have their picture taken and be given a temporary ID card that they must wear until they leave the property.
- **Entry through Mechanical / Electronic Device**
- ✓ **Keys** Some employees are given a building master key that allows them to enter the building and most areas inside. This is the most common and cheap method of physical access control to premises.
  - ✓ **Touch keypads** A keypad is on the wall at the entrance. Users are given passwords, codes, or personal identification numbers (PIN) that they must punch in order to enter.
  - ✓ **ID Card Tags** Some cards have a magnetic strip like you see on the back of a debit card. Other cards have a bar code like you see on a store product. The user swipes the card or puts it in a slot in the reader. The reader is mounted on the wall or door. It checks the code on the card. If the card is authorized, the door is unlocked for a short period of time.
  - ✓ **Proximity Cards** These cards work in the same as cards with stripes or bar codes, but they do not have to touch the reader. Someone can unlock the door by passing their card near the reader. These cards may show only an identification number or one side may include photo ID. A key fob is a device that acts the same way as a proximity card. It is a small plastic device that can be attached to a key ring.
  - ✓ **Biometric Identification** Biographical information about individual employees is stored in a data bank. This could include fingerprints, palm prints, retina patterns (blood vessel patterns in the eye) or face recognition information. If an employee wants to enter an area, they must pass their hand, eye, or face by a reader. If the reader matches this information with the stored data bank, the door is unlocked. Because biometric data is unique to each person, this system can be used to prevent theft or fraud. Unlike a password or PIN, a biometric trait cannot be forgotten or lost.
  - ✓ **Radio Frequency Identification (RFID)** Tags the size of a grain of rice can be embedded in access cards or other security devices that would allow authorized

personnel access to areas within a facility and would also allow Security to 'track' the individuals as they move throughout the facility. RFID technology is being used in airports in the new e-passport system to help identify legitimate personnel, and distinguish them from possible security risks.

- **Access Control Guidelines** The Security Guard has to receive the visitor, escort/monitor him/her through the premises and ensure his/her satisfactory departure. Security is recommended to follow these guidelines :
  - **At Reception Stage to Provide Site Access**
    - ✓ Verbally greet individual(s) entering premises/site/facility
    - ✓ Verify Identification- use Govt issued Photo ID
    - ✓ Checking identification against access list
    - ✓ Examining/searching individual(s)/property/vehicle (as necessary)
    - ✓ Confirm purpose of visit asking questions
    - ✓ Writing/logging in person/vehicle in entry
    - ✓ Brief visitor of site restrictions (e.g., no phones or cameras)
    - ✓ Granting access to facility (e.g., issuing key card/key chain, open gate or arrange escort)
  - **During Movement Within Site/Premises**
    - ✓ **Escort visitor(s)** or follow visitor escort policy on site
    - ✓ **Monitor visitor.** Observe visitor/employees' behaviour, looking for irregularities / unexpected events (e.g., unauthorized entry to part of building)
    - ✓ Report irregularities or unexpected events to management/supervisor/dispatch
  - **Control Egress / Exit of Visitors**
    - ✓ Greet individual(s) leaving site
    - ✓ Examine/Search Personal property/possessions (as necessary)
    - ✓ Comparing entry data to egress/exit observations/data
    - ✓ Redirecting individual(s) to permitted area (as necessary) or using physical force (if necessary)
    - ✓ Reporting incidences to others (e.g., dispatch, police, as necessary)
    - ✓ Collecting access cards/keys
    - ✓ Allowing egress/exit of site (e.g., open/unlock door) (as necessary)

### **Part V Patrolling and Surveillance**

- **Patrolling** Patrolling is one of the fundamental method by which the security guard performs the function of protecting people, property and information. A security guard deters crime just by being present in a particular area or site. But when he moves on a patrol, his area of coverage widens. The patrolling also helps in apprehension of individuals committing crimes and preservation of peace.
- **Aim of Patrolling.** Patrolling is one of the most complex and difficult tasks performed by security guards. The aim of patrolling could be any or all of the following:
  - Detect hazards and emergencies.
  - Help employees and visitors to the site



- Check for damage or equipments which are not working properly.
  - Detect crimes.
  - Protect confidential information
  - Generate a feeling of secure environment in community living
  
- **Preparation for Patrolling.** Normally, a security guard is expected to patrol the site every hour or every alternate hour. The tasks for each patrol may vary depending on the level and types of threat and the type of response to be generated. Irrespective of the task, a security guard must always plan and prepare for the patrol. Some of the factors that must be considered for planning a patrol are:
  - **Purpose of Patrol** The purpose like general patrol, investigation patrol etc has great bearing on planning and preparation for patrol
  - Based on the purpose, plan for timing, duration, route, geography of the area, emergency and routine equipment required, radio communications especially in the dead zones like basements etc, writing material, any constraints /restrictions during the patrol like using radio, flash lights, access restrictions etc.
  - For effective patrolling, always study and follow post orders, seek advice from other guards who have been on such duties before, have detailed knowledge of layout of site and keep other guards/ supervisors informed of the plan and progress of the patrol.
  
- **Recommended Methodology for Patrolling a High rise Building.** When patrolling a multi-storey building, start from the perimeter and there-after monitor security of all the ground level access points of the building. Pay particular attention to ground floor windows. Starting from top floor, patrol floor by floor checking for deficiencies, garbage, open apartment/office doors, bicycles or carts and persons loitering in halls, laundry rooms, and underground and above ground parking areas. Preferably, go up the lift and come down the stairwells. Note any cigarette butts, drug paraphernalia, graffiti, broken locks or windows, garbage, property damage, lights out etc. Move any individual loitering in stairwells but do not engage on same level, but instead stay a half level higher for easy escape. Should situation become volatile, call for assistance immediately.
  
- **Types of Patrol** The patrol may be conducted on foot or vehicle.
  - **Foot Patrol** In this method, the security guard moves on foot and covers the given area. He checks access points, doors and windows, locks, machinery and equipment, alarms etc on each floor of building or condominium. Security Guard should ensure that he patrols at random times so that patrolling patterns are not formed.
    - ✓ **Advantages of Foot Patrol** The foot patrol is highly visible and deterrent for crime prevention. It has more person to person contact and improves community relations. It also helps in developing more sources of information due to direct contact with residents/locals. Security guard has the ability to access smaller spaces and restricted areas thus detecting emergency situations using all his sensory organs and generate suitable responses.

- ✓ **Disadvantages** Some of the disadvantages of the foot patrol are limited range, time consuming, limited equipment carrying capability, vulnerability of the security guard in confined areas and adverse impact of the inclement weather.
  - **Mobile/ Vehicle Patrol** Mobile patrolling is done by using vehicle or by bicycle. It can be done any time of day or night and same tasks can be done by this patrol which was being done by foot patrol. The area coverage can be much large and heavy surveillance equipments can be carried along in the vehicle. It improves reaction capability of the patrol and diverse types of equipment can be carried depending on the requirements.
- **Surveillance** It is also known as fixed or static patrol wherein a security guard keeps an access point or large areas under observation relying on technology like CCTV, night vision devices and surveillance cameras. Its aim is to keep a continuous and systematic watch over given area with specific purpose of threat identification and response generation.
- **Duties from Static Post** Some of the duties that security guard performs while doing surveillance from the static post are : access control and escorts, CCTV monitoring, data entry, enforcing permission protocols and search programmes or monitoring trespass to property and generating emergency responses
- **Surveillance Procedures** A security guard must observe changes in physical environment and suspicious behavior, recognize patterns and be aware of environment/ situation around him and always be conscious of any breaks/ changes in routine patterns on the site. He should endeavor to improve his responses by interpreting and adapting to events, decision making and action plans and prioritizing actions. Security guard is placed on site to use his intelligence and judgment to respond to situations. He must rely on his sensory organs 'eyes- to see, ears- for sound detection, nose- to smell, touch –to feel and finally brain- to perceive and assess the situation'. He should exploit technology as supplement to sensory organs and not vice versa.
- **Keeping Yourself Safe** Always ensure your personal safety during surveillance or patrolling. Some of the guidelines are : never approach a suspect alone- call for back up, use your flashlight effectively, use caution with windows and glass doors, use the shadows to observe, be silent on patrol, don't smoke, watch where you walk and know when to be seen.