Access Control

Access Control

Security Guards are responsible for managing the movement of people and materials in, out of, and within a facility. This role is crucial for maintaining normal operations and preventing unauthorized access and exit. Guards must be knowledgeable about access control measures, which involve the coordination of human resources with other security components such as electronic systems and physical barriers. – *Canadian General Standards Board Standard 133.1 Paragraph A8.1*

Responding to Alarms

Security Guards also respond to alarms. This section will equip candidates with a foundational understanding of protective and fire alarm systems, which they are likely to encounter. It will include information on how these systems operate. – *Canadian General Standards Board Standard 133.1 Paragraph A5.1*

Access Control Systems

Access control encompasses any mechanism designed to ensure that the right person accesses the right area at the right time. While this might seem complex, it's quite straightforward. Consider everyday examples: you secure your home by locking it when you leave, you protect your vehicle by locking its doors or using anti-theft devices, and you lock your office door each night to prevent unauthorized entry. These are all forms of access control. Access to these places and devices is managed by not distributing keys or combinations to everyone, but rather only to those you trust.

Though these methods are not foolproof—thieves can steal keys, break doors or windows, pick locks, or hot-wire cars—additional security measures can enhance access control. One effective method is employing Security Guards. A primary function of security personnel is to manage the movement of people, materials, and vehicles in, out of, and within an area. By controlling access, they ensure that authorized individuals can enter specific areas at appropriate times, thus maintaining security.

Access control can vary in its intensity, from minimal to extensive, based on the security needs of the site. Whether it's a building, a parking lot, a residential complex, or another facility, controlling access is crucial for protecting the property and ensuring the safety of authorized individuals.

Levels of Access Control

Minimum Access Control: This level of control is implemented at sites that allow general admission, such as shopping malls. It operates on the assumption that everyone entering is doing so for lawful purposes. Entry is only denied by the Security Guard if individuals fail to follow rules or break the law.

Medium Access Control: This type of control is common in office or residential buildings. Access is typically managed using an intercom system, which allows a Security Guard or someone inside the building to grant entry. While the intercom can deter unauthorized entry, determined individuals might still gain access by following someone with legitimate entry rights.

Maximum Access Control: High-security sites, such as certain government offices, laboratories, military bases, and software manufacturing facilities, employ maximum access control. These locations use a combination of security personnel and alarm systems to ensure total control over access to all parts of the property. This comprehensive approach is designed to prevent any unauthorized entry.

Rules for Access

Access rules vary for each building, facility, or work site. Public admittance may be permitted to some, all, or none of the premises, and these rules can change based on the time of day. For instance, an office tower's lobby might be open to the public during normal working hours but locked and restricted after hours. Similarly, a parking lot closed to the public from 7 a.m. to 5 p.m. might allow unrestricted access after those hours.

Access rules may not only restrict public entry but also limit access for employees working on the site. For example, a large pharmaceutical plant with different branches working on various projects within the same building might implement access controls to ensure employees remain within their designated areas for security reasons.

The client’s specific needs determine the access control mechanisms at a job site. Since the client is more familiar with the site’s requirements and sensitive areas (e.g., tenants in an office tower who might object to certain security measures like physical searches), they are responsible for deciding which access control mechanisms to use.

Property owners set all access rules, including who is granted access and under what conditions; when bags and briefcases will be searched; and when individuals will be stopped, questioned, or allowed free access to the property. It is the security team’s role to ensure compliance with these rules.

Elevator and Escalator Operation

When Security Guards are responsible for supervising elevator operations, they should follow these procedures:

1. **Verify Load Maximums**: Ensure that the maximum load capacity is clearly posted.
2. **Encourage Proper Positioning**: Advise passengers to move to the rear of the elevator and face the front.
3. **Keep Clear of Doors**: Ensure people, clothing, and personal belongings are kept away from the doors when they are closing.
4. **Familiarize with Emergency Systems**: Know the emergency systems on board, including the stop button, bells, and the telephone system if available.

For escalator operation, similar procedures apply:

1. **Prevent Crowding**: Do not allow overcrowding on the escalator.
2. **Encourage Proper Direction**: Advise people to face the direction of travel and to remain stationary while on the escalator.
3. **Know Emergency Stops**: Be familiar with the location of emergency stop buttons, which are at the top and bottom of escalators.

In case of an accident on an escalator, the emergency stop button should be pressed immediately. If the issue is resolved and the escalator needs to be restarted, ensure no one is on the escalator before it starts moving. If an escalator malfunctions, ensure it is turned off and not restarted until it has been properly repaired by qualified service personnel.

Methods of Controlling Access to Property

Access control mechanisms are essential for regulating the entry and exit of individuals onto a property or into specific areas. Various devices are used as access control mechanisms, including card readers, touch keys, ID cards, badges, and fingerprint identification.

In smaller work sites, a Security Guard may recognize individuals, which serves as an effective but limited method of access control. This method's effectiveness depends on the memory of the Security Guard, which can vary significantly between individuals. The larger the number of people granted access, the higher the chance of mistakes, allowing unauthorized individuals to slip inside.

To enhance this method, photo badges can be used as identification at manual checkpoints. Keys and locks are another common method for controlling access to the entire property or specific sections. However, keys can be lost or stolen, and locks can be picked. Additionally, locks are ineffective if doors or windows are not consistently secured.

Ticket machines provide another access control method by only granting access to those who obtain a ticket.

Access control typically starts with the property's outer perimeter and becomes more stringent towards the central core of the protected site. The outer perimeter marks the property boundary, the inner perimeter includes all common areas within the property, and the central core is the primary area to be protected.

Access Control Area Examples

Shopping Centre

- **Outer Perimeter**: Outside edges of the parking lot.
- **Inner Perimeter**: Sidewalks, parking lot around the building.
- **Central Core**: The shopping centre itself.

Building Construction Site

- **Outer Perimeter**: Outside edges of the parking lot, starting with the fence keeping the public out.
- **Inner Perimeter**: Ground inside the fence, surrounding the building under construction, road in, parking area for equipment, tool shed, etc.
- **Central Core**: The building structure itself.

Bank

- **Outer Perimeter**: Outside edges of the bank property, the front where the bank's storefront contacts the sidewalk, and the rear parking lot available to the public.
- **Inner Perimeter**: Walls of the bank building itself; doors and windows are areas of concern.
- **Central Core**: The bank vault.

Perimeter, Area, Building, and Point of Object Protection Systems

Security systems can protect various areas of a property, including the inside and outside perimeters, the central core, or specific spots within these areas. Specific security devices can also safeguard objects like safes and vaults.

Perimeter Protection Systems

The first line of defense in protecting property involves control mechanisms around the outside perimeter. These can include access booths, gates, fences, and walls. These systems aim to detect intruders immediately upon entering the property and are also known as point of entry protection systems. A "complete" system protects the entire outer perimeter, including walls,

floors, and ceilings, while a "partial" system protects only accessible openings such as windows, doors, and gates.

Area Systems

More commonly found in inner perimeter and central core areas, area systems serve as the second line of defense. They detect intruders once they have entered the premises. Examples include motion detectors, pressure plates, audio detectors, and photoelectric cells.

Point or Spot Systems

The third line of defense involves point or spot systems, used to protect specific objects like bank vaults and paintings in art museums. These objects may have sensors attached or be surrounded by audio and infrared detectors and other security mechanisms.

Fences and Walls

Made of wood, wire, or other solid materials, fences and walls control access by surrounding the property. Natural barriers like rivers, cliffs, and ravines can provide similar protection. However, these barriers are not foolproof as they can be cut through, knocked down, tunneled under, or climbed over. Regular maintenance and patrols are essential to maintain their effectiveness. Any materials stacked against fences and walls that might enable intruders to enter should be reported immediately.

Gates and Other Openings

Gates or other openings are used for entrance and exit. Security personnel, access booths, keys, and other mechanisms can manage access at these points.

Infrared Beam Perimeter Security Systems

These systems use poles or columns around the premises to create an infrared curtain. An alarm is triggered if any of the infrared beams are interrupted. Each column typically has an anti-tamper/anti-climbing device that activates an alarm if tampered with. These electronic devices require backup power to operate during power failures.

Cameras

Cameras, mounted at strategic points, provide additional security. They can be fixed, movable, or activated by movement, and can monitor the outer perimeter, inner perimeter, or central core areas. However, cameras do not automatically raise alarms or open gates; they require continuous monitoring by security personnel. Backup power is necessary to ensure functionality during power failures.

Lighting

Proper illumination can significantly enhance property security. Well-lit premises make it easier for security personnel, passersby, and workers to spot potential problems and reduce the risk of ambush attacks on guards. Lights should be placed along the outer perimeter, inner perimeter, and within the inner core. Lighting controls should be situated out of reach of potential intruders. Backup power is crucial to maintain lighting during power outages.

By implementing these various protection systems and maintaining vigilance, security personnel can effectively safeguard property and individuals.

Technology Used to Control Access/Egress

Access control typically happens in two ways: through a Security Guard or via mechanical or electronic devices.

1. Entry Through Security Guard

As a Security Guard, you may be stationed at the main entrance of a site with the primary tasks of checking identification and determining if individuals are authorized to enter.

Personnel Recognition:

- This method is often used at smaller sites where you admit only recognized individuals. Staff will inform you of expected visitors, and you will record visitor information using a special form. This method is effective only if you know every person entering and can monitor each entry. If your attention is diverted or you cannot identify everyone, unauthorized individuals may gain access.

ID Systems:

- Commonly used in government offices, where all employees present an ID card before entering. When checking ID cards, look for:
    - A colored photo and physical description of the holder.
    - The full name and signature of the holder.
    - The company's name and an issuing authority’s signature.
    - An expiry date.
    - A serial number (either for the card or an employee number).

Special Passes:

- In high-security areas, entry may be restricted to individuals with special passes or badges. Familiarize yourself with the specific access control criteria. Visitors and short-term workers might need to provide a piece of ID, such as a driver's license, to receive a

pass. Record their names in a logbook and return their ID when they return the pass upon leaving. In maximum access control sites, visitors may have their picture taken and be issued a temporary ID card to wear until they leave the property.

Access control is only effective if rules are consistently followed for everyone. Long-term employees might become frustrated by daily ID checks, but it is essential to adhere to protocol. If you are new to the site and do not recognize all employees, check ID cards even for known individuals, as their cards may no longer be valid. If challenged, remain calm, explain the security procedures, record the information in a logbook or report sheet, and follow your post orders.

Security Guards may sometimes be tasked with receiving, storing, or delivering mail, messages, or parcels. These duties are not typically a Security Guard's responsibility and should only be performed if explicitly instructed in your post orders. Postal or special delivery messengers should wear special badges and have proper identification. Your responsibility is to verify their ID, record their entry, and provide directions for their delivery.

Entry Through Mechanical / Electronic Device

At medium access sites, employees often use various mechanical or electronic devices to control access without the direct intervention of a Security Guard. Here are the common methods:

Keys:

- Some employees are provided with a building master key, allowing them to access the building and most areas inside. However, new technologies are increasingly replacing traditional metal keys.

Touch Keypads:

- A keypad is installed at the entrance. Users are assigned passwords, codes, or personal identification numbers (PINs) that they must enter to gain access.

ID Card Tags:

- These cards may have a magnetic strip, like a debit card, or a barcode, like a store product. Users swipe the card or insert it into a reader mounted on the wall or door. The reader verifies the card and unlocks the door for a brief period if the card is authorized.

Proximity Cards:

- Similar to magnetic strip or barcode cards, proximity cards do not need to touch the reader. Simply passing the card near the reader unlocks the door. Some proximity cards also feature photo ID. Key fobs work similarly and can be attached to key rings.

Biometric Identification:

- This technology stores biographical data, such as fingerprints, palm prints, retina patterns, or facial recognition, in a database. Employees must scan their biometric data to gain access. This system is highly secure as biometric traits are unique and cannot be forgotten or lost, preventing theft or fraud.

Radio Frequency Identification (RFID):

- RFID tags, which are very small, can be embedded in access cards or other security devices. They allow authorized personnel to access various facility areas and enable security to track individuals as they move throughout the facility. RFID technology is used in e-passport systems in airports to identify legitimate personnel and distinguish them from potential security risks.

While these systems provide significant advantages, they also rely on the honesty of visitors and the ability of security personnel to detect false identification when ID is required.

Keys and Locking Systems:

- Locks prevent unauthorized access to property. Security personnel may be provided with keys to access the property.
    - **Building Master Key**: Opens all doors within a building except those "keyed off the master."
    - **Sub-Master Key**: Opens a group of doors within a specific area. For example, a "department master" may access all spaces held by one department, while a Sub-Master key might access only a particular section.
    - **Security Protected Keys**: These keys are engraved or stamped with specific insignia or numbers that locksmiths and key copying services recognize and refuse to copy.
    - **Push-Button Combination Locks**: These locks require a code for access and are used in areas where higher security is needed. Distribution of master keys, sub-master keys, and push-button codes is usually controlled carefully.

Timed Locks:

- Common in banks and similar institutions, these locks are set on timers. At a preset date and time, using a key or code will unlock the protected area. Access outside regular business hours may require special overrides, and some systems may not allow overrides at all.

Ticket Machines:

- Tickets are issued to individuals accessing the premises, providing proof of granted access. This method offers limited security as it typically restricts access to those who can pay a fee but does not ensure the conduct or safety of users or property.

Implementing these technologies enhances security by providing various access control mechanisms suitable for different security levels and needs.

Limitations on Access Control Mechanisms and Techniques

Technical access control mechanisms largely depend on electricity to function, making backup or emergency power and manual overrides crucial components of a robust security system. Here are some common limitations and vulnerabilities of access control systems:

1. **Electricity Dependency**: Many access control mechanisms cease to function during power outages unless backup power or manual overrides are available.
2. **Loss, Theft, or Duplication of Keys/Cards**: Keys, cards, or passes can be lost, stolen, or duplicated. Programmable cards and similar devices can be obtained by illegitimate users with sufficient resources.
3. **Vulnerability to Physical Breach**: Locks can be picked, and doors, gates, and windows can be smashed open.
4. **Static Passwords and Codes**: Passwords and pass codes that are not changed regularly can be discovered or sold, compromising security.

No security system is foolproof; it is designed to minimize the risks of unlawful access, not eliminate them entirely. Security Guards play a vital role in mitigating these weaknesses by providing supplementary protection to the persons and property they are assigned to guard.

Case Study: Legal Liability and Responsibilities

A notable case in Texas highlighted the critical importance of proper management of access devices. A security firm was held liable for $18 million in damages after a woman was sexually assaulted and abducted by a man who used a backup key to enter her apartment. The offender had broken into the security firm's office and stolen the labeled key, which had the victim's correct address. The jury found the security firm liable because it had assumed responsibility for the safe storage and foreseeable unlawful use of the key. The court ruled that the firm had a duty to protect the homeowner from unlawful actions enabled by such a powerful access tool.

Best Practices for Security Guards

1. **Awareness and Vigilance**: Always be mindful of the inherent weaknesses in the security systems you work with.

2. **Regular Updates**: Ensure that passwords and pass codes are changed regularly to minimize the risk of unauthorized access.
3. **Secure Storage**: Maintain strict protocols for the storage and handling of keys, cards, and other access devices.
4. **Supplementing Technology**: Use your presence and vigilance to complement and enhance the effectiveness of electronic security systems.
5. **Emergency Preparedness**: Be familiar with manual overrides and backup power systems to ensure continuous security during power outages.

By understanding and addressing these limitations, Security Guards can provide more comprehensive protection and enhance the overall security of the sites they are assigned to.

Materials Access

One of the most sensitive tasks for Security Guards is handling the removal of materials from a work site. Employees routinely leave the site with items like computers, computer disks, boxes, briefcases, vehicles, and other company possessions. While industrial espionage may be a concern, overly restrictive measures can also create problems if legitimate access is hindered. It is the client's responsibility to determine the appropriate security measures. Clients provide directions formally or informally, usually in written form. Security Guards must stay informed about any changes to security operations, policies, and procedures, and discuss them with a supervisor.

Shipping and Receiving Controls: Clients may ask security to handle documents, packages, and other deliveries. Security Guards should follow clear instructions or post orders to comply with the client's requirements. Clients may need:

- Special forms prepared by recipients of packages.
- Logbooks detailing the receipt of goods.
- Deliveries signed for.
- Arrangements for the delivery to the ultimate recipient on the site.

Gate Duty Responsibilities: Guards stationed at gates are typically expected to:

1. **Check Vehicle and Driver Information**:
    - Verify vehicle license numbers and driver's names.
2. **Ensure Authorized Deliveries**:
    - Confirm that deliveries are expected or have proper authorization.
3. **Receive Deliveries per Post Orders**:
    - Follow post orders when receiving deliveries.
4. **Verify Seals on Vehicles**:
    - Ensure that seals on incoming or outgoing vehicles, if used, are intact and untampered.
5. **Confirm Outgoing Loads**:

    - Use waybills or other supporting documentation to authorize the removal of property when vehicles leave the premises.
6. **Search Vehicle Cabs**:
    - If required by the client and specified in post orders, search the cabs of vehicles entering or leaving for articles.

By adhering to these procedures, Security Guards can effectively manage materials access while balancing security concerns with operational efficiency.

The Security of Information

Confidentiality of Information

Maintaining the confidentiality of critical information is a fundamental responsibility of Security Guards. Confidentiality involves keeping sensitive information secret to prevent "information leaks." As a Security Guard, you are placed in a position of trust and must always act to uphold that trust.

Due to their job duties, Security Guards often become some of the most informed employees within a company. They are privy to a wide range of sensitive information, including details about criminal acts, financial affairs, personal activities, and classified work. Guards also frequently carry keys that grant access to areas restricted to others, further emphasizing the need for discretion.

Security Guards must ensure that confidential and classified information remains within the workplace and is shared only with authorized personnel within the security department or designated company members. Discussing or showing this information to outsiders is strictly prohibited.

Classification of Information

The Canadian Government classifies information into several categories based on the potential impact of unauthorized disclosure:

- **Top Secret**: Unauthorized disclosure would cause exceptionally grave damage to the nation.
- **Secret**: Unauthorized disclosure would endanger national security, cause serious injury to the nation's interests or prestige, or significantly benefit a foreign nation.
- **Confidential**: Unauthorized disclosure would harm the nation's interests or prestige, or provide an advantage to a foreign power. Individual personal files may also fall under this classification.
- **Restricted**: Information should not be published or communicated except for official purposes. In the industrial context, similar classifications protect information from competitors and the public.

Security Guards must understand and adhere to these classifications to ensure that sensitive information is appropriately safeguarded. By doing so, they help maintain the trust placed in them and protect the interests of their employer and the nation.

Computer Crime

Computer crime involves stealing or damaging computer information. There are various methods by which computer crimes can occur. Stolen data can be used to obtain goods and services or sold for profit. Intruders might acquire confidential information, such as passwords or special codes, by searching through desks or garbage cans. If employees fail to log off their computers properly, unauthorized individuals can access private information or alter files.

Both external and internal individuals can perpetrate computer crimes at your site. As a Security Guard, one of your responsibilities may be to escort people through restricted areas to ensure they do not access confidential information. Detecting computer crime can be challenging, but there are some signs that might indicate its occurrence:

1. **Unusual Access Patterns**: Unexpected or irregular access to sensitive information or systems by employees or visitors.
2. **Unattended Computers**: Computers left logged on and unattended, providing potential access to unauthorized users.
3. **Tampering with Equipment**: Signs of physical tampering with computers or network equipment.
4. **Strange Software or Files**: The presence of unfamiliar software or files on a company computer.
5. **Suspicious Behavior**: Individuals showing undue interest in restricted areas or confidential information.

As a Security Guard, remain vigilant for these signs and report any suspicious activity to your supervisor or the appropriate department. Ensuring computer systems' security is crucial in preventing data theft and maintaining the integrity of company information.

Watch for Any of the Following:

Be alert for the following signs that may indicate someone is involved in computer crimes:

- **Disgruntled Employees**: Employees who are angry at the company or have been recently fired.
- **Exposed Private Information**: Pass codes or other private information left out in easily visible areas.
- **Unauthorized Computer Use**: Individuals using computers that belong to someone else.
- **Odd Work Hours**: Employees who work from home frequently and come into the office at unusual hours or times when they are not expected.

- **Unproductive Extended Hours**: Employees who arrive early or leave late but appear to do little company work during these times.
- **Loose Talk**: Employees who discuss confidential matters too freely.

Use your common sense when assessing whether something you observe may indicate involvement in computer crimes. If you notice anything suspicious, take detailed notes and report your concerns.

Regardless of your work location or client, your assignment will fall under specific classifications. To be effective, a good Security Guard must be thoroughly familiar with the physical layout of the building, plant, facility, or area they are guarding. This knowledge is essential to detect when something is wrong and respond quickly when necessary. Without this understanding, you will not be able to perform your duties with pride and confidence or react appropriately in emergencies.

Always remember, the primary function of a Security Guard is to provide protection. Specific duties for each assignment will usually be detailed in orders and instructions issued by management. Stay informed and vigilant to ensure you can fulfill your responsibilities effectively.

Computer Security

Protecting computers and the programs they contain presents unique challenges. Each technological advancement brings new threats, including:

- **Theft of Computers**: Physical theft of computer hardware.
- **Theft or Piracy of Software**: Unauthorized copying or use of software, violating copyright laws.
- **Industrial Espionage**: Theft of ideas, products, or trade secrets.
- **Mischief or Damage**: Actions that harm computers or their functionality, including introducing viruses or modifying data.

Challenges in Detecting Computer Theft: Computer theft can range from blatant to subtle. For instance, a person stealing a computer by physically removing it is easy to identify. However, distinguishing between a legitimate employee taking work home and someone stealing a laptop or software can be challenging, especially if the person appears authorized and is in business attire.

Piracy of Software: Software is protected by copyright, and unauthorized use or copying is illegal. Both individuals and employers can be held liable for software piracy.

Industrial Espionage: This specialized form of theft involves stealing industrial secrets, such as proprietary recipes or processes. It is difficult to differentiate between employees taking home legitimate work and those removing confidential information.

Non-Legitimate Use of Company Equipment: Some companies prohibit personal use of company equipment. Security Guards may find it challenging to determine if such policies are being violated. These issues should be discussed with a supervisor, who can then consult the client to establish appropriate measures.

Mischief or Damage to Computers: This includes physical damage and actions that reduce computer functionality, such as infecting them with viruses, deleting or modifying data, or introducing malicious software.

Common Computer Threats:

- **Virus**: A program that infects other programs by modifying them to include a copy of itself.
- **Worm**: A program that spreads copies of itself through a network and connected computers.
- **Trojan Horse**: A program with hidden instructions that perform unintended actions.

Effects of Computer Viruses and Worms: These self-propagating programs can destroy data, consume resources, and spread to other programs. Trojan horses can insert harmful instructions into programs, causing unintended and potentially damaging actions.

By understanding these threats and maintaining vigilance, Security Guards can better protect computers and sensitive information from various forms of computer crime.

Conducting Security Checks and Searches

While the client determines the rules of access at a work site, a Security Guard is responsible for ensuring compliance with these rules. It is essential for Security Guards to be fully aware of the specific access rules they will be enforcing. Security firms should provide thorough training and discussions about the rules of access and protocols when introducing Security Guards to a new site.

Ensuring Compliance with Access Rules

- **Familiarization**: Security Guards must become familiar with the access requirements of the particular site they are assigned to.
- **Detailed Training**: Security firms should discuss access rules and protocols in detail with Security Guards before they begin their duties at a new site.

Conducting Searches

- **Potential for Inconvenience and Insult**: Searches can be highly inconvenient and potentially insulting to individuals. It is crucial that Security Guards comply with the client's instructions regarding when such actions are necessary.

- **Clear Instructions**: If the client's instructions are unclear, Security Guards should consult with their supervisor to avoid misunderstandings.
- **Documentation**: Security Guards should document suspicious behavior and items removed from the site in an official report. Detailed notes should be recorded in the guard's notebook, including a full description of what transpired.

Consulting with Supervisors and Clients

- **Discussing Difficulties**: Security policies that present challenges should be discussed with a supervisor. The supervisor can then consult with the client to determine an appropriate approach.
- **Management Decisions**: It is easier for a Security Guard to explain the necessity of searching an employee's briefcase if the management has clearly determined that such searches are necessary.

Key Points for Security Guards

1. **Understand Site-Specific Rules**: Be clear on the specific rules and protocols of the site you are assigned to.
2. **Respect Client Wishes**: Ensure searches and checks comply with the client's instructions to avoid unnecessary inconvenience or insult to individuals.
3. **Consult Supervisors**: When in doubt or faced with ambiguous instructions, consult your supervisor for clarification.
4. **Document Incidents**: Keep detailed records of suspicious behavior and incidents in an official report and your notebook.
5. **Communicate Clearly**: Explain the necessity of security actions based on clear instructions from management.

By following these guidelines, Security Guards can effectively enforce access rules and conduct security checks and searches in a manner that respects the client's wishes and minimizes inconvenience to individuals.

Alarm Systems

Purpose of an Alarm System

An alarm system is any mechanism designed to provide immediate notification of a condition requiring urgent attention or response.

Historical Overview

- **Primitive Alarm Systems**:
    - **Dogs**: Barking at potential intruders.
    - **Bells and Noisemakers**: Strategically placed on strings to alert people.

- **Miners' Canaries**: Miners used small birds to detect low oxygen levels; the birds would succumb to lack of air first, warning the miners of danger.

Modern Alarm Systems

With advancements in technology, alarm systems have become more complex and accurate. Some modern systems can even perform self-analysis to minimize false alarms.

Types of Conditions Alarm Systems Can Warn About

1. **Intrusion**: Unauthorized entry.
2. **Fire**: Detection of flames or heat.
3. **Smoke**: Presence of smoke particles.
4. **Toxic Chemicals**: Release of hazardous substances.
5. **Environmental Changes**: Variations in temperature or humidity.
6. **Equipment Malfunction**: Failures in machinery or systems.

Responsibilities of a Security Guard

A Security Guard should have the following basic skills related to alarm systems:

1. **Arming the System**: Activating the alarm system to monitor conditions.
2. **Disarming the System**: Deactivating the alarm system, usually when it is no longer needed or to allow authorized entry.
3. **Resetting the System**: Returning the alarm system to its normal operating state after it has been triggered.
4. **Testing the System**: Ensuring the alarm system is functioning correctly.
5. **Recognizing Problems**: Identifying obvious issues with the system to ensure it operates effectively.

By understanding these key aspects of alarm systems, Security Guards can effectively respond to various emergencies and ensure the safety and security of the premises they are responsible for.

Types of Alarm Systems

Alarm systems can be classified into two main types: mechanical and electrical, or a combination of both.

Mechanical Alarms:

- These alarms rely on physical mechanisms to alert individuals. An example is wind chimes placed near the door of a store, which notify the clerk of any entrance or exit by potential customers.

Electrical Alarms:

- These systems use sensors and electronic devices installed in homes, buildings, and compounds to activate an alarm in response to specific triggers.

Main Purposes of an Alarm System

Alarm systems serve to warn people of various problems, including:

1. **Intrusion**: Detecting illegal entry into a property.
2. **Fire**: Identifying the presence of flames or excessive heat.
3. **Smoke**: Sensing smoke particles in the air.
4. **Toxic Chemical Release**: Alerting to the release of hazardous substances.
5. **Temperature Changes**: Monitoring significant changes in temperature.
6. **Humidity Changes**: Detecting variations in humidity levels.
7. **Equipment Breakdown**: Notifying of machinery or system failures.
8. **Water Leaks or Other Types of Leaks**: Detecting leaks that could cause damage or present hazards.

By providing immediate notifications of these conditions, alarm systems help ensure prompt responses to emergencies, thereby enhancing safety and security.

Components of Alarm Equipment

How Do Alarm Systems Operate?

Alarm systems, despite their varying complexity, consist of three main components: the sensor, the transmitter, and the control panel or annunciator. You can visualize an alarm system functioning similarly to the human body:

1. **Sensor**:
    - **Analogy**: Senses (sight, hearing, touch)
    - **Function**: Detects changes in the environment, such as motion, smoke, temperature, or unauthorized entry.
2. **Transmitter**:
    - **Analogy**: Nerves
    - **Function**: Carries the detected information from the sensor to the control panel or annunciator.
3. **Control Panel/Annunciator**:
    - **Analogy**: Brain
    - **Function**: Processes the information received from the transmitter and decides the appropriate response, such as sounding an alarm, notifying security personnel, or triggering an automated response.

By understanding these components and their functions, Security Guards can effectively monitor and respond to the alarm systems they work with, ensuring timely and appropriate actions are taken in response to detected issues.

Components of Alarm Equipment

1. Sensor

Sensors are the hardware components that detect information from a protected area. They act as the "eyes and ears" of an alarm system, indicating the presence of specific conditions such as movement, light interruption, smoke, toxic chemicals, temperature, pressure, or humidity changes.

Types of Sensors

1. **Magnetic Contacts**:
    - **Function**: Detect the opening of doors, windows, drawers, and cabinets.
    - **Mechanism**: A magnet on the moving part and another on the frame. Movement opens a spring contact, signaling the control panel.
    - **Security Concern**: Easily defeated by substituting a secondary magnetic field.
2. **Shock Sensors**:
    - **Function**: Detect vibrations from pressure or forced entry.
    - **Mechanism**: Activated by the shock of a blow, signaling the control panel.
    - **Application**: Installed in windows, doors, gates, walls, safes, vaults.
    - **Security Concern**: Can be triggered by strong winds.
3. **Motion Detectors**:
    - **Function**: Capture the movement of intruders.
    - **Mechanism**: Various types including photoelectric cells, ultrasonic detectors, microwave sensors, infrared sensors.
    - **Application**: Installed in high-traffic areas.
4. **Photoelectric Cells**:
    - **Function**: Detect light interruption.
    - **Mechanism**: A beam of light (laser, infrared, or ultraviolet) is sent across a path. Interruption triggers an alarm.
    - **Security Concern**: Can be bypassed by stepping over or under the beam.
5. **Ultrasonic Detectors**:
    - **Function**: Detect movement via sound waves.
    - **Mechanism**: Sound pulses bounce off objects; changes in bounce time/pattern trigger the alarm.
    - **Security Concern**: Can be triggered by small animals or air movement.
6. **Microwave Motion Sensors**:
    - **Function**: Detect movement using radio waves.
    - **Mechanism**: Radio waves pass through solid walls and detect motion.
    - **Security Concern**: Can detect motion in other rooms.

7. **Audio Alarms**:
    - **Function**: Monitor noises.
    - **Mechanism**: Microphones detect sounds such as breaking glass.
    - **Security Concern**: Can be triggered by air conditioning or heating equipment.
8. **Infrared Sensors**:
    - **Function**: Measure infrared energy to detect intruders.
    - **Mechanism**: Detects body heat from warm-blooded animals.
    - **Security Concern**: Can be triggered by changes in heating/cooling systems.
9. **Pressure Sensors**:
    - **Function**: Trigger alarms when pressure is applied.
    - **Mechanism**: Installed under mats, near vaults, and safes.
    - **Security Concern**: Triggered by walking pressure.
10. **Gauges**:
    - **Function**: Measure pressure or fluid levels.
    - **Mechanism**: Attached to boilers and heating devices to signal control panels.
11. **Temperature Sensors**:
    - **Function**: Monitor environmental temperature changes.
    - **Mechanism**: Detects radical temperature changes (e.g., rise to 1000 degrees or fall below freezing).
    - **Application**: Fire detection, monitoring critical temperature thresholds.

Sensor Types and Security Concerns

Sensor Type	How It Works	Security Concerns
Shock	Activated by vibration from pressure or forced entry; installed in windows, doors, gates, walls	Strong winds could trigger it
Motion	Activated by movement; installed in high-traffic areas	-
Laser Beam	Beam of light sent to receiver; intruder breaks the beam	Intruders can step over/under the beam
Ultrasonic	Sound waves sent to receiver; movement alters wave pattern	Small animals or air movement could trigger it
Microwave	Radio waves sent to receiver; movement breaks radio signal	Waves can penetrate walls, detecting motion elsewhere
Audio	Microphone picks up loud sounds (e.g., breaking glass)	Air conditioning/heating noise could trigger it
Magnetic/Foil Circuit	Activated by opening doors/windows	Secondary magnets can neutralize it
Infrared Energy	Detects heat increases from human/animal bodies and fire	Rapid heating/cooling changes could trigger it
Pressure	Activated by walking pressure; installed under mats	-

Sensor Type	How It Works	Security Concerns
Wire	Activated by tension changes; stretched along perimeter barriers	-
Proximity Alarm	Electromagnetic field around the object; activated by entering the field	Animals/tall grass can trigger perimeter alarms

By understanding these sensors and their potential vulnerabilities, Security Guards can better manage and respond to alarm systems, ensuring the protection of the premises.

2. Transmitter

A transmitter is any device that sends alarm messages from the sensor to the control panel. These messages can be transmitted through various means, including hard wiring, telephone wires, fiber optic lines, and radio signals.

Function of Transmitters

Transmitters play a crucial role in the operation of alarm systems by relaying information from sensors to the control panel. Here's how they work:

- **Signal Transmission**: When a sensor detects an event, such as a broken window, it generates a signal. The transmitter sends this signal to the control panel.
- **Communication Pathways**: Transmitters use different types of communication pathways to send signals:
    - **Hard Wiring**: Traditional wires that physically connect sensors to the control panel.
    - **Telephone Wires**: Utilize existing telephone infrastructure to transmit signals.
    - **Fiber Optic Lines**: Use light signals through optical fibers for high-speed, high-security transmission.
    - **Radio Signals**: Wireless transmission using radio frequencies, suitable for situations where wiring is impractical.

Example Scenario

Consider a scenario where a window is protected by a light wire or metal foil:

- The window is smashed, breaking the wire or foil and interrupting the electric circuit.
- The sensor detects the interruption and generates an alarm signal.
- The transmitter sends this signal from the sensor to the control panel via the chosen communication pathway (e.g., hard wiring or radio signal).
- The control panel receives the signal and triggers an appropriate response, such as sounding an alarm or notifying security personnel.

By effectively transmitting signals from sensors to the control panel, transmitters ensure that alarm systems can promptly respond to security breaches and other monitored conditions.

3. Control Panel or Annunciator

The control panel, often referred to as the "brains" of an electronic security system, is the central unit that receives messages and translates this information into specific responses. It typically consists of similar types of hardware across different models.

Function and Operation

A control panel processes messages, warnings, and alerts from various sensing devices and responds accordingly. When it detects certain conditions—such as a rise in temperature, the presence of smoke particles beyond a set threshold, movement, or unusual sound levels—it triggers a pre-programmed response. This response might involve contacting emergency services such as police, ambulance, or fire departments.

Key Components and Their Functions

Component	Function
Data Processing Equipment	Receives and interprets information from sensors.
Alarm Transmission Equipment	Activates alarms like sirens, horns, and sends signals via telephone or radio.
On/Off and Reset Controls	Allows the operator to manage the alarm system using panel boards with keys, pads, or buttons.
LCD Panel	Displays the alarm status and system operation details, indicating trouble spots if any.
Backup Power Supplies	Ensures the system remains operational during power outages, whether accidental or planned.

Detailed Breakdown

While manufacturers might offer different systems with unique features, control panels generally include data processing equipment, alarm transmission equipment, on/off and reset controls, system status indicators, and backup power supplies.

- **Data Processing Equipment:** This hardware receives data from the sensing devices and processes it according to pre-set instructions, determining the appropriate response.
- **Alarm Transmission Equipment:** This component raises an alarm, which could be a simple sound like a horn or siren, or a signal sent through telephone lines or radio waves to a monitoring station, either on-site or remotely located.
- **On/Off and Reset Controls:** Typically consisting of keys, toggles, or digital keypads, these controls allow the operator to activate, deactivate, or reset the alarm system.

- **System Status Indicators:** These indicators, often using colored lights, display the system's operational status. Common colors include red (system off but functional), yellow (system trouble), and green (system armed and operating correctly).
- **Backup Power Supplies:** Most alarm systems feature backup power sources to ensure continuous operation during power outages, whether these are accidental, planned, or due to sabotage.

In summary, the control panel is a vital component of an electronic security system, ensuring that all sensing data is correctly processed and appropriate responses are initiated to maintain safety and security.

General Operating Procedures

Electronic alarm systems are designed to be active except during times when the public is allowed unrestricted access to the premises, at which point the alarm may be overridden or deactivated. When specific conditions are met—such as motion detected by a sensor, significant temperature changes, or the detection of smoke or chemicals beyond a predetermined level—the system activates the alarm.

Common Causes of Alarm Activation

There are four primary reasons for alarm activation:

1. **Specified Event Occurrence:** An event like an intruder entering the premises triggers the alarm. (Approx. 0.01%)
2. **System Malfunction:** A technical issue within the alarm system causes it to activate erroneously. (Approx. 19.69%)
3. **Human Error:** Incorrect actions by individuals lead to false alarms. (Approx. 45.80%)
4. **Undetermined Causes:** The cause of the alarm cannot be identified. (Approx. 34.50%)

Industry statistics indicate that the number of false alarms due to errors is significantly higher than the number of genuine alarms. Despite this, security personnel responding to an alarm must always treat it as a legitimate event to ensure safety and security.

Types of False Alarms

1. **Malfunction:** This refers to any fixable issue within the alarm system that causes incorrect operation, either triggering a false positive (alarm sounds without a real threat) or a false negative (alarm fails to sound when needed). Regular maintenance is essential to prevent malfunctions. Factors like deteriorating wiring, structural damage, or physical impacts on electronic devices need periodic inspection to ensure the system remains fully functional.

2. **Human Error:** False alarms often result from human mistakes, such as improper activation or deactivation of the alarm or incorrect installation of equipment. Proper training and careful handling can reduce these errors.
3. **Undetermined Causes:** Sometimes, the source of a false alarm cannot be pinpointed to either the system or human error. These cases require thorough investigation to prevent recurrence.

Ensuring the effective operation of security systems involves regular maintenance and proper handling by all individuals involved. This vigilance helps maintain the reliability and accuracy of the alarm systems, thereby enhancing overall security.

Monitoring of Alarms

Alarm systems are crucial for property security, but having an alarm does not necessarily mean it is monitored. Alarm systems are generally categorized into two main types:

Local Alarms (Unmonitored Alarms)

Local alarms, also known as unmonitored alarms, activate localized alert devices such as bells, horns, sirens, or strobe lights when triggered. These alarms do not notify external agencies like the police, fire department, or monitoring services. Although cost-effective, local alarms might not be effective unless people are present in or near the protected building. However, the presence of a security guard on-site combined with a local alarm can significantly reduce the chances of an undetected alarm.

Monitored Alarm Systems

Monitored alarm systems are divided into two subcategories: locally monitored and centrally monitored.

Locally Monitored Alarm Systems

A locally monitored alarm system enhances a basic local alarm by adding a dialer or communicator. The control panel connects to a telephone line, which can be either dedicated or shared. When the alarm is activated, the control panel automatically dials a series of pre-programmed numbers, transmitting information about the event.

Centrally Monitored Alarm Systems

Centrally monitored alarm systems connect the control panel directly to a central monitoring agency through a dedicated transmission line. These agencies operate 24/7, 365 days a year. When an alarm signal is received, trained personnel follow a pre-determined protocol using a list of contact numbers. For instance, if an intruder alarm is triggered (e.g., a window sensor detects a break-in attempt), the central agency might first call the store, then the store owner.

If neither responds, the police or other emergency services are contacted. The alarm signal typically indicates the type of alarm (e.g., fire, window breakage), guiding the central agency on which emergency personnel to notify. These systems can also detect a cut or broken phone line and treat it as an alarm.

In summary, while local alarms are less expensive and suitable for smaller or less critical locations, monitored alarm systems, particularly centrally monitored ones, provide a higher level of security through continuous surveillance and immediate response to alarms.

Security Responsibilities During an Alarm

Security guards need to be familiar with the alarm systems in the areas they are protecting. If unsure, they should consult with their supervisor or the site owner to understand the system's equipment and ensure compliance with the client's instructions regarding alarm operations.

Pre-Determined Responsibilities

The specific duties of a security guard during an alarm should be clearly outlined in advance by the client (the hiring agency) and the security firm. These responsibilities may include:

- Notifying the client or relevant emergency personnel (police, fire department, etc.)
- Identifying the cause of the alarm
- Taking appropriate action based on the situation

Primary Responsibilities

Regardless of the alarm's nature, the primary responsibilities of a security guard remain consistent: protecting people and property. The response to an alarm can vary based on instructions from the security company or the client. Common scenarios include:

- **Immediate Evacuation:** In some cases, the guard may be instructed to evacuate the premises immediately once an alarm is activated.
- **Securing the Building:** In other situations, the guard might be required to seal the building. For example, after a bank robbery, security guards are often tasked with securing the crime scene until the police arrive. This may involve encouraging customers to stay on the premises for police interviews.

By clearly understanding and following these pre-determined responsibilities, security guards can effectively manage alarm situations, ensuring the safety of people and the protection of property.