7.2 Site security

Site security can deter or stop intrusion, delay attack and mitigate the effects of an incident in the immediate vicinity of a site.[97] This chapter focuses primarily on offices and residences for staff living away from home. It is also necessary, however, to consider site security for locations where staff spend a significant amount of time, such as project sites, refugee camps, school buildings, medical facilities and distribution points. Site security measures may sometimes also be needed around the private homes of staff.

7.2.1 Site selection

Site protection starts with identifying and selecting a suitable location, bearing in mind that the perfect choice seldom exists. In addition to space, price and other criteria, the physical strengths and weaknesses of a site can be assessed from a security point of view – what is acceptable, what must be improved and how much this would cost. This allows an organisation to assess suitability and to detail and negotiate any permissions to make alterations before signing a lease.

Security approaches

In any physical security review, whether selecting a site or adding new physical security measures, it is important to consider the local community's perceptions and attitudes towards these measures. For instance, constructing a 2.5-metre wall may be advisable from a protection perspective but may raises suspicions or be disruptive to the local space. This 'acceptance lens' can be applied to all examples of good practice shared in this chapter.

Individual profile considerations

When selecting offices and accommodation, it is important to consider the personal profiles and needs of staff and likely visitors. This can help create a secure, inclusive and supportive work environment.

In certain contexts, it may be culturally inappropriate or potentially unsafe for female staff to live alone. In such cases, shared living arrangements that align with social norms and meet the needs of female colleagues may be appropriate. Providing separate quarters for male and female staff might be advisable, depending on the cultural and social context. Accessibility requirements for

97 The risks change dramatically in situations of insurgency and war, where additional measures are required. These are considered in more detail in Chapter 7.10.

disabled staff are also an important consideration. Providing options for private or shared accommodation that respects gender identity and sexual orientation can help mitigate risks and ensure a welcoming environment.

Consulting with diverse groups of staff when choosing sites can help ensure their needs are adequately met.

▶ *See Chapter 1.2 for more on inclusive security considerations.*

Physical criteria

Organisations can consider various physical criteria when selecting a site. This may include the following:

- **Structural resilience.** It is advisable for organisations to ensure that buildings are sufficiently robust and resilient to withstand the impacts of extreme weather and other environmental risks, including floods and landslides. This can involve checking the structural integrity of the building, the quality of materials and the effectiveness of drainage systems in the area.
- **Location.** Organisations may want to avoid areas that offer opportunities for concealed approaches and escapes – for instance those with dense vegetation or narrow and poorly lit alleyways. Areas with many unoccupied, damaged or derelict buildings may also present risks. In situations of active armed conflict, site selection criteria will often include considerations of distance from potential military targets and access to shelter facilities. While security concerns may drive the selection of affluent neighbourhoods, diplomatic enclaves or gated communities, these choices could convey an elitist image, potentially affecting how the organisation is perceived.
- **Security perimeter.** A double perimeter, where a building or apartment is situated within a compound or a larger gated area, is generally preferable. An effectively managed perimeter can act as a deterrent to unauthorised access and provide early warning in case of intrusion.
- **Emergency evacuation.** How easily can staff and visitors evacuate the building or immediate area in the event of an emergency, such as a fire? Consider exit routes, whether the building's design facilitates the safe and swift evacuation of all occupants, and whether the local fire brigade can access the site efficiently.
- **Floor level.** It is often advisable to rent office space or an apartment above the ground floor to reduce vulnerability to intruders. However, higher floors may be unreachable by emergency equipment and difficult to escape from.

If the roof is accessible, perhaps from a neighbouring building, occupying the apartment directly beneath could increase risks.

- **Accessibility.** Ensure that entrances, exits and common areas are accessible to those with mobility challenges, and that emergency procedures account for their needs. Considering whether the building is equipped with features such as ramps, elevators and accessible restrooms is advisable.
- **Secure parking.** It may be prudent to confirm that the site provides secure parking facilities: the parking area is well lit, monitored by security cameras and protected by controlled access points, such as gates or barriers. Secure parking is an important aspect of the overall security of the premises, particularly during non-peak hours. Parking spaces can also present risks in active conflict settings, and these are discussed in more detail below.

▶ *See Chapter 7.10 for additional site considerations in active combat areas.*

Building ownership, occupancy and tenancy

- **Ownership of the building.** Organisations should ascertain the ownership of the building, for example whether it is held by an individual, a bank, a shop or a religious organisation. Understanding the owner's identity and their potential role within the community may provide insights into how their affiliations could impact the organisation's image and operations.
- **Occupancy and tenancy.** When evaluating a building, it is advisable to consider who else occupies or rents space within the premises. The presence of other tenants might offer added awareness and a degree of collective protection. However, other tenants could introduce risks, particularly if they are or might become targets themselves. A single-tenant site may be more fully under the organisation's control.
- **Other organisations.** Security advantages and efficiencies can sometimes be gained if several aid organisations occupy sites in the same place or close together. UN agencies, for example, often group their offices in a single area to enhance security and reduce costs. Some NGOs have also adopted this approach. However, grouped sites may evolve into gated communities, potentially isolating organisations from the broader community, or create the impression of close association between organisations, which may impact local perceptions and acceptance. The concentration of possible targets within a single area means that an attack may have a much larger impact if successful.

The neighbourhood

It is advisable to examine the surrounding area, ideally within a radius of at least 1.5km, to gain a comprehensive understanding of the neighbourhood. Key considerations include the following:

- **The stability and social cohesion of the resident population.** High social cohesion might suggest a reliable, informal neighbourhood watch scheme, with residents who are vigilant and concerned about security. Low social cohesion could indicate a lack of interest in neighbours' security, potentially allowing strangers easy access to the site.
- **The nature of the neighbourhood.** Are most people local residents, or do large numbers of workers or travellers frequently pass through? The less local the population, the easier it may be for outsiders to enter the area without attracting attention.
- **Availability of local authority and rescue services.** Determine the locations of the nearest fire station and police posts and the residences of influential local leaders. Identify the areas police patrols cover most frequently.
- **Access control measures.** Consider the type of access control used by local residents, including how they enter and exit premises and whether there are physical or virtual/computer systems in place. Are guards stationed outside homes? Are homes in the area heavily fortified?
- **Crime levels.** Criminality may be an important factor, keeping in mind that crime levels can be high in both affluent and less affluent areas. Regardless of the area's wealth, organisations and their staff should avoid the appearance of wealth. Whether or not to select a location near a police station depends on the context and the relationship between the police and the local community.

In general, cultivating good relations with neighbours, without being intrusive, can be an important site security measure. Establishing even a basic relationship may increase the likelihood of neighbours acting if they observe something suspicious.

7.2.2 Site reinforcement

With regard to the physical security of work and residential sites, a useful rubric is 'Deter, detect, delay and respond'.[98] This can include: adding elements to make a building harder to enter, such as walls, bars and access controls; removing

98 GISF (2024) *3. Site security.* NGO Security Toolbox (https://gisf.ngo/toolbox-pwa/resource/3-site-security/).

elements that make it hard to see potential intruders and adding cameras, alarms and watchmen; having a saferoom that can delay intruders' access to staff; and putting procedures in place to quickly respond when intrusions are detected. The following sections cover these measures in detail.

The outer perimeter

The following are factors when considering the security of the outer perimeter of a site.

- **Surroundings.** If the vegetation surrounding the building provides potential access or hiding places, organisations can consider trimming, cutting or replacing it with thorn bushes. Rubbish or rubble near the perimeter could potentially assist an assailant in monitoring or gaining access to the building, or hinder the response of security personnel. Prompt removal of any debris that could conceal explosive devices is also advisable.
- **Walls and gates.** Constructing walls around the site may enhance security. Good practice generally suggests that these should be at least 2.5 metres high and fortified with additional measures such as barbed wire or broken glass along the top. Nearby trees or other objects that could make scaling the walls possible may also need to be addressed. Gates, as potential vulnerable points, should be properly secured, with peepholes for visual verification of visitors. In some contexts having a secondary, but secure, exit point might be prudent.
- **Lighting and visibility.** Improved lighting can serve as a deterrent to potential threats, but care should be taken to strike a balance between enhancing visibility and drawing attention. Lighting should also not negatively affect neighbours. Sensor lights that activate upon detecting movement may be a good option, provided they have a consistent power supply. In areas prone to power outages, alternative energy sources like generators or solar lighting might be considered. The decision to display the organisation's logo on the outer perimeter will depend on whether the organisation has determined that visibility in the given context enhances or detracts from its security. In environments where the organisation is well regarded, displaying the logo can be appropriate, accompanied by translations in the local language.
- **Unoccupied sites.** For sites that are unoccupied for periods of time, organisations may implement measures to create the illusion of activity, such as periodically turning lights on and off and adjusting shutters to deter potential intruders.
- **Consistency with local security practices.** Adopting similar levels of site protection as other buildings in the vicinity, even if perceived risk levels do not seem to warrant it, could be advisable.

- **Parking and vehicle access control.** Parking arrangements should be designed to prevent unauthorised vehicle access to the site, and reduce the risks of attacks on vehicles. Where risks such as vandalism, car theft, mob violence or bombing are present, vehicles are best parked in secure locations, such as within a compound. It is also advisable to ensure sufficient parking space when selecting a site, and that vehicles are locked when not in use. Operating procedures for vehicle key control, parking arrangements and emergency use should be established. Parking and fuel arrangements should facilitate easy departure from the site. This can mean ensuring that vehicles are fully fuelled at the end of each day and parked to allow quick loading and exit.

Crime prevention through environmental design

Crime prevention through environmental design (CPTED) focuses on improving site security by manipulating the physical environment to guide behaviours and reduce the opportunity for crime. This is often overlooked during the design or renovation of facilities, or when security solutions are developed over time. CPTED strategies include the following:

- **Natural surveillance.** Increasing exterior and interior visibility to expose would-be perpetrators and enhance the sense of safety for legitimate users. It involves carefully managing landscaping, lighting and placement of windows and entrances for clear sightlines and to reduce opportunities for concealment.
- **Natural access control.** Utilising physical elements like structures, barriers, landscaping, lighting and signage to direct access to specific, controllable points.
- **Territorial reinforcement.** Defining public, semi-public and private spaces through physical elements like buildings, fences and landscaping. This encourages occupants to challenge intruders and makes them more easily identifiable.
- **Maintenance.** Avoiding visible signs of disorder like broken windows, graffiti and discarded equipment, which can create an impression of abandonment and neglect that invites criminal activity.

- **Bollards and anti-ram barriers.** Strategically placed, bollards may restrict vehicle access but still allow pedestrian flow. Bollards can be fixed, removable or retractable. Anti-ram barriers can provide enhanced protection against vehicle-borne threats and are usually designed to withstand high-speed impacts. Options include reinforced concrete barriers, steel bollards and cable systems. Bollards can be integrated into the overall perimeter security system, complementing walls and gates.
- **Integration of perimeter security measures.** By using a combination of physical barriers alongside other security measures, organisations can establish a layered defence. Aligning these perimeter security measures with the organisation's broader security objectives, including fostering acceptance and goodwill among the local population, is crucial to ensuring a cohesive and comprehensive approach to safeguarding personnel and assets.

The inner perimeter

It is advisable for organisations to assess each site from the perspective of an intruder, identifying any potential weak spots, particularly around doors and windows, but also garage doors and cellars.

- **Entrance doors.** Organisations may want to ensure that entrance doors are strong, including the frames and hinges. If any glass is present in the door, consider replacing it. Installing an optical viewer (peephole) along with a primary and auxiliary lock on outer doors can enhance security. For additional internal security, organisations can consider installing a safety chain and a sliding deadbolt or strong bar across the door. Heavy-duty padlocks, placed at the top and bottom of the door with welded padlock rings, can provide further protection. Finally, it is advisable to position panic buttons or telephones away from entrance doors to prevent an intruder from blocking access to them.
- **Windows.** Organisations may want to secure windows, particularly on the ground floor, with bars, grills or shutters provided they are easy to open from the inside in case of an emergency. If upper-floor windows are accessible from the outside, it may be useful to secure them with bars or grills. It is important to ensure that these cannot be easily unscrewed or removed from the outside.
- **Night-time routine.** It may be advisable to close curtains at night to prevent intruders from observing who and how many people are inside the building. Staff may wish to leave a light on when departing the premises to create the impression that someone is still inside. All locks and bolts should be checked to ensure they are in good working order and should be routinely locked as night falls or before going to bed.

- **Alternative exit in emergencies.** In case of fire, intrusion or rioting, it is advisable to have an alternative exit from the building. This escape route, including any window protections, should be easily accessible from the inside, taking into account the personal profiles of all staff (such as mobility needs). If bars are already fitted to windows, organisations may want to modify them to allow easy exit from the inside. This could involve hinging the bars on one side and securing them with a padlock, ensuring that occupants can quickly access the key in case of emergency.
- **Burglar alarms and closed-circuit television (CCTV).** While burglar alarms and CCTV cameras may be uncommon in many aid contexts, organisations could still consider using these for additional security. Both typically depend on an electricity supply, though some burglar alarms operate on batteries. CCTV cameras may offer limited deterrence unless intruders are aware of their presence and function, and there is a reasonable chance of being caught. High-decibel security devices, which operate remotely and directionally, create an unbearable sound that can stop intruders or even rioting crowds from advancing further into the premises. They are usually equipped with sabotage protection and operate on batteries.

Basic fire safety considerations

To address the risk of fire, consider the following:

- Fit smoke and carbon monoxide alarms and place fire extinguishers in the kitchen and on every floor – electrical and oil fires require a CO_2 or powder-filled extinguisher; for other types of fire a foam or water-filled extinguisher should be used.
- Check extinguishers and have them serviced at least once a year.
- Identify fire escape routes and ensure that, when locked from the inside, they can be opened instantly.
- Organise regular fire drills, especially if staff turnover is high.
- Make sure that gas room heaters are properly vented and check that they have thermocouples (devices that prevent the gas supply from turning on without a pilot light or other source of ignition) – heaters without thermocouples should not be left unattended and should not be used at night.

- Formally designate trained individuals to ensure that disabled staff are assisted in case of an emergency (sometimes described as a 'buddy system'); these individuals should be staff who spend most of their time on site.
- Place evacuation maps so that they are prominent but not visible to passers-by and perhaps code the identification of rooms so that it helps staff and visitors without also serving as a potential guide to intruders.

Safe rooms

A safe room can serve as a critical refuge for occupants during emergencies, providing protection from intruders until help arrives. Most safe rooms are not designed to withstand bomb or shell impacts.

- **Location and accessibility.** A safe room should be easily accessible and ideally situated in the core of the building for quick entry. Alternatively, upper floors can be converted into safe areas by securing staircases with locking grills during vulnerable times, such as at night.
- **Security features.** The safe room should ideally be equipped with reinforced doors and secure windows to deter intruders. A telephone or emergency radio should be available to summon assistance. Organisations may want to consider installing uninterruptible communication systems to maintain connectivity during power outages. A list of key contact numbers, including emergency services and internal response teams, can be prominently displayed within the safe room.
- **Emergency supplies.** The safe room should be stocked with essential supplies to sustain occupants during an emergency. This can include first-aid kits, a small quantity of water, non-perishable food items and sanitary provisions. Chairs, mattresses and bedding can be added in case staff have to take refuge for longer periods or overnight. Perishable items and medicines should be regularly checked and replaced.
- **Training and drills.** Regular training sessions and drills (including simulated scenarios) familiarise building occupants with the safe room's location, layout and procedures, including how to access it quickly and what to do while sheltering in the safe room during an emergency.

- **Communication protocols.** It is advisable to establish clear communication protocols within the safe room, outlining procedures for contacting emergency services and coordinating with external responders. Designating individuals responsible for initiating communication with authorities and providing updates on the situation is beneficial. A communication hierarchy can help to streamline information dissemination and decision-making.

▶ *To learn more about communications security, see Chapter 6.1.*

7.2.3 Site security risk management

Individual awareness

Site security is everybody's responsibility. Everyone – including receptionists, telephone operators, cleaners and gardeners – should be attentive and report anything unusual or suspicious, as well as breaches in security procedures (for example, doors or windows left open or keys left lying around). For residential properties, this includes all residents (including family members). These individuals should receive guidance on not letting unknown people into the property, giving information to unknown callers, giving details about the office layout or allowing their keys to be duplicated. Receptionists can play a key role in monitoring visitors and telephone calls, as well as letters and parcels being delivered, and can be trained to report anything and anybody that appears suspicious.

Guards

Aid organisations sometimes use guards for their residences, warehouses and offices. Guards may either be hired directly or contracted from a local provider. They can be ineffective if they are untrained, poorly instructed, poorly paid, poorly equipped or poorly managed. This is unfortunately not uncommon in many of the contexts in which aid work takes place. It is also not uncommon to find a bed in the guardhouse of aid organisation compounds, increasing the likelihood that the guard will fall asleep on duty. During the day, guards might be busy doing other things and may be distracted. When hiring guards, it is important to provide clear terms of reference and make this part of the contract.

In recruiting and managing guards, consider the following:

- Obtaining reliable references and, if possible, recruiting staff from the immediate neighbourhood. This can ensure that they are familiar with the area and its regular occupants and may increase their motivation to identify potential wrongdoers.

- Checking the language abilities of potential recruits. The primary occupants of a building need to be able to communicate with the guard.
- Hiring and deploying enough guards to detect intrusions and to support each other while working together.
- Ensuring that guards receive a full introduction to the organisation.
- If the guard is to carry a weapon (lethal or otherwise), the circumstances under which it may be used should be governed by the contract signed with the individual or the guard provider and reflect the organisation's security policy. It is recommended that such policies be reviewed by the organisation's legal adviser. Organisations can include contractual stipulations against the use of harmful substances (e.g. alcohol) while on duty and against additional jobs that may affect the guard's performance.
- Providing essential equipment, instruction and training. Equipment may include rain clothes, torches, a whistle or other alarm and a handheld radio or separate telephone in the guardhouse.
- Providing a logbook with instructions on keeping the log and reporting suspicious activity, as well as a list of key contact numbers.
- Providing clear instructions and training on how to deal with visitors and what to do if guards come across an intruder.
- Providing clear instructions about monitoring the surroundings, patrolling the compound and rules regarding gates, doors, windows and keys.
- Guards normally only have access to the outer (not the inner) perimeter, especially at residential premises. At the office building, they should usually have access to corridors, staircases and the roof, but not necessarily to the offices themselves.
- In areas where trespass or robbery is a high risk, consider routine inspection schedules alternated with rounds at less predictable times. Spreading guards out, with at least one in a position where they cannot be easily observed and overpowered – for example on a roof terrace – can be beneficial.
- Trained specifically for guarding purposes, dogs can be an excellent early warning of intruders and often a deterrent. However, a dog is potentially dangerous to people it does not know, and control measures may be necessary to protect legitimate visitors and staff.

Managing access

Access control starts with establishing key management control measures. Organisations may also use magnetic access cards, cipher locks (electronic push-button systems that allow entry only to people who know the code), magnetic readers, smart cards or biometric devices. Larger offices, typically in bigger cities, may control access by installing doors or turnstiles that operate with magnetic cards. Management controls should ideally be put in place for all of these. Systems can be expensive and may fail if the power supply is interrupted or if the mechanism malfunctions.

Site keys

Organisations can maintain a comprehensive log of keys and who holds them, and ensure that the number of keys in circulation is strictly controlled. If there is any doubt concerning key security, changing the locks is advisable. Keys can be labelled in code so they cannot be easily identified. Spare keys should be securely stored in a locked key box with a glass front that can be broken in case of emergency.

All personnel with access to keys, including household staff, should be informed of any key management protocols – for example, carrying keys on their person rather than leaving them on desks, in cars or in unattended coats and bags. Keys generally should not be duplicated unless explicitly instructed by the organisation's management, and any loss of keys should be reported immediately.

Being overly strict with key control can introduce its own hazards. For example, staff may be unable to escape from a burning building if they do not have access to the key for the emergency exit door. Similarly, a response to an emergency call from a colleague may be delayed if vehicle keys are locked away.

With regard to visitors, access control generally serves two functions: to establish the purpose and legitimacy of a visitor and to ensure that visitors do not constitute a threat. In some circumstances, access may have to be very

strictly controlled; visitors may be actively discouraged or directed to a separate building away from the organisation's main facility. In any case, it is helpful to have a designated visitor waiting space. This should be easily visible to security personnel and the receptionist. It should be connected to a toilet facility, but no uncontrolled access to the building should be possible for a visitor still waiting for clearance.

There are degrees of security control. For example, having visitors sign in and out is hardly a security measure in itself, as anyone can still get in. Stricter standard procedures might include ensuring that:

- all staff wear visible photo ID when on the premises;
- all visitors show identification;
- all visitors are given an ID or a pass, collected when they leave;
- no visitors are allowed in unless there is explicit authorisation from the person they want to see or who agrees to see them; and
- no visitors are allowed in unless accompanied by a staff member.

Stricter procedures include checks of visitors' bags and manual or electronic body searches (female guards and special training are usually needed for this).

In high-risk environments, anyone unknown, unauthorised or unable to provide convincing identification should not be let in. Initial cursory checks to establish whether a visitor could present a threat should take place at the outer perimeter, before they are admitted into the inner perimeter of a building. Only when a visitor does not seem to present a threat should they be let in. Establishing the purpose of the visit, contacting the host department, registering the visit and issuing a visitor's pass can then be done as a distinct second step within the premises, thereby minimising the number of people waiting at the main entrance. If in doubt, guards should be instructed to contact a supervisor.

In the event that a suspicious or unauthorised individual is encountered, security personnel or focal points should be alerted immediately. Protocols could be in place for notifying personnel promptly and discreetly, for instance through radios or panic buttons. Security personnel may consider introducing code words for summoning help discreetly. If the situation escalates or poses a significant threat, a lockdown may be necessary to secure the premises and protect staff. It is recommended that lockdown procedures are clearly outlined to staff, detailing actions to be taken, such as securing doors and barricading entry points.

Access policy: questions to consider

- **Should visitors' vehicles be allowed into the compound (if applicable)?** It may be worth considering where visitors should park. For instance, in the event of a bomb threat it is advisable to ensure that no non-organisational vehicles are present within the compound. Organisations may also want to consider prohibiting visitor parking around the building. Guards may be instructed to search vehicles, but this is a skilled task and requires proper training.
- **What is the organisation's policy on visitors bringing bodyguards or weapons onto the premises?** Organisations may choose to have a policy regarding the presence of weapons on organisational premises, taking into account the context and the type of visitor (e.g. police or government officials), and whether visitors arriving with their own bodyguards should be permitted to bring them into the premises. The potential liability of the organisation in the event of an attack on a visitor whose bodyguards were not permitted entry may need to be considered. Holding meetings in an annex of the building or on a veranda, where bodyguards could remain nearby, may provide a practical compromise. Guards should be trained on how to handle these kinds of circumstances.
- **How should access for service personnel and deliveries be managed?** Service access warrants careful consideration, including access for maintenance, repair, utilities personnel and deliveries. Decide whether service personnel should be allowed onto the premises in the absence of relevant staff, and whether arrivals can be planned and scheduled in advance. Requiring identification from service personnel could enhance security and, in the case of street vendors, staff may want to purchase goods outside the gate to limit access.

▶ *See Chapter 4.2 for more discussion on armed protection.*

Beyond traditional access control measures like visitor sign-in, there is a growing trend towards biometric authentication methods, such as fingerprint or iris scanning. Incorporating biometric authentication into access control procedures

can bolster their security posture while maintaining efficiency and convenience for legitimate visitors and staff members. Some organisations have opted for two-factor authentication (e.g. biometrics and a card), or created different authorisation levels for different facilities or departments. Organisations need to consider the risks of power failures, as well as the sensitivity of biometric data collection and potential risks of data breaches. Improper storage or encryption of biometric data could lead to identity theft or other privacy violations if the data is breached. These risks can be managed through proper data storage, encryption and system security measures.

Threatening phone calls and letters

Problematic phone calls can range from crank calls to sexual harassment and bomb threats. Where this is a risk, staff should be trained in how to respond. Using caller identification technology or call tracing can aid in identifying the origin of problematic calls and assist in investigations. Sexual harassment calls made to women can sometimes be stopped by having a male co-worker or co-resident answer the phone. If the caller persists, it may be best to change the telephone number. As a general rule, staff should not share their personal phone numbers and only give their work number on their email signatures and business cards.

In the case of threatening calls, recipients should try to remain calm and polite; refrain from sharing personal or sensitive information; give as little information as possible to the caller; listen attentively to gather as much information as possible to help with the caller's identification; write down all relevant details, including the name and phone number, if known; and report the threat immediately. If the call is a bomb threat, the key question will be when and where the bomb will explode. Unless confident that the threat is not real, the building should be immediately evacuated. If the office receives a threatening letter, it should be treated seriously and shared quickly with senior managers, the authorities and other organisations in the area, as appropriate.

Suspicious letters or parcels

While not a common threat to aid organisations, it is possible that a letter or parcel may be delivered that is deliberately contaminated with a poisonous chemical or biological substance, or that contains explosives. Possible indicators are traces of powder on the envelope, a strange odour and, in the case of a bomb, a ticking sound or visible wires. The parcel may be unusually heavy for its size, the address may be misspelt or the letter or parcel may be addressed to someone who no longer works for the organisation. It may lack postage or may have excessive postage, indicating that it was not assessed for postage at a post office.

Any such letters or parcels should be left where they are, the room vacated and security personnel alerted. Anyone who handled the object should be instructed to wash immediately with soap, especially their hands. The letter or parcel may have to be destroyed or opened by specially trained security personnel with proper equipment (contamination with a poisonous substance requires fully protective gloves as a minimum, and possibly fully protective face masks, as some substances may enter the body through inhalation).

7.2.4 Distribution sites

A number of measures can help increase security for staff and target populations at distribution sites.

- **Understanding the target population.** Gaining a good understanding of the target population is helpful, including how the population, as well as others in the vicinity, may perceive the distribution, whether there are potential tensions between groups and the likelihood of political interference. Staff could look out for any signs of desperation for the items being distributed, and identify elements that could have an interest in manipulating the distribution process.
- **Perimeter and site management.** Establishing a well-defined perimeter can be beneficial. Fencing or walls may be appropriate, or barricades with additional monitoring.
- **Location of the distribution site.** It may be advisable to choose a location where ambient traffic, both vehicular and pedestrian, is not obstructed, and ensuring the site does not attract unwanted bystanders or disturbances.
- **Managing entry and exit points.** Designate one entry point and one exit point. Effective management of crowds at the entry point can allow for swift separation of legitimate aid recipients from those who may not be eligible. Ensure sufficient staff are in place to manage unruly individuals. Exit points should be managed carefully, ensuring that recipients can leave the site in a safe and orderly manner.
- **Crowd control and movement.** Keeping people moving is important. Staff or authorities can monitor the area to prevent crowds, including family members assisting recipients, from gathering and impeding the departure of others. The safety and protection of those leaving the site, particularly women and young children, should be considered. Carrying large bundles, for example, may make aid recipients more vulnerable to potential targeting, and staff could consider ways to make distributed items less conspicuous.

▶ *For more details on distribution risks see Chapter 7.6 on civil unrest.*

Further information

Guidance

Davis, J. et al. (2020) 'Module 8, Security of facilities' in *Security to go: a risk management toolkit for humanitarian aid agencies*, 4th edition. GISF (https://gisf.ngo/resource/security-to-go/).

GISF (2024) *3. Site security*. NGO Security Toolbox (https://gisf.ngo/toolbox-pwa/resource/3-site-security/).

International CPTED Association (n.d.) The International Crime Prevention Through Environmental Design Association (www.cpted.net/).

Safer Edge (2014) *Office closure*. EISF (https://gisf.ngo/resource/office-closure/).

Source8 (2015) *Office opening: a guide for non-governmental organisations*. EISF (https://gisf.ngo/resource/office-opening/).