

I mproving security at work and at home

Purpose:

Assessing security at work or at home.

Planning, improving and checking security in offices and homes.

Security at work and at home

Security at the organisation's headquarters or offices and in staff members' homes is of fundamental importance to human rights defenders' work. We will therefore go into some depth about how the security of an office or home can be analysed and improved. *(For the sake of simplicity we will only refer to "offices" from now on, although the information below also applies to home security.)*

General aspects of office security

Our aim in improving security can be summarised in three words: **Prevent unauthorised access**. This is true whether your office is in an urban or rural area. In rare cases it may also be necessary to protect an office against a possible attack (against bombing, for example).

This brings us to the first general consideration - the vulnerabilities of an office. They increase risk, depending on the threat you face. For example, if you are at risk of someone stealing equipment or information, you must remove your vulnerabilities accordingly. A night alarm (electric, if you have access to electricity, or a night watchman, or otherwise a dog) is of little use if nobody is going to come and check what has happened. On the other hand, if there is a violent break-in in daylight, reinforced door railings or alarms won't be very useful. In short, take measures according to the threats you face and the context you are working in.

The vulnerabilities of an office must be assessed in the light of the threats you may face.

However, it is important to find a balance between putting appropriate security measures in place and giving outsiders the impression that something is being “hidden” or “guarded”, because this can in itself put you at risk. In office security you often have to choose between keeping a low profile or taking more obvious measures if need be. On the other hand, a potential aggressor will be aware that your office contains valuables or contentious information and that you ‘need’ to protect it.

**The security of an office
is no greater than its weakest point.**

If somebody wants to gain entry without your knowledge, they won’t choose the most difficult entry point. Remember that the easiest way of gaining access to an office and observing what goes on inside is, sometimes, as simple as knocking on the door and getting inside.

The office location

Whether the office is in an urban or rural area, the factors to consider when setting up an office are: the neighbourhood; whether the building is associated with any particular people or activities from the past; accessibility of public and private transport; risk of accidents; how suitable the building is for putting the necessary security measures in place, etc. (*Also see Location evaluation risk below.*)

It is useful to review which security measures are being taken by others in the neighbourhood. If there are many, this may be a sign of an unsafe area, for example, in respect of common crime. It is also important to talk to people in the area about the local security situation. In any case, make sure security measures can be taken without attracting undue attention. It is also useful to get to know local people as they can pass on information regarding anything suspicious going on in the neighbourhood.

It is also important to check out who the owner is. What reputation do they have? Could they be susceptible to pressure from the authorities? Will they be comfortable with you putting security measures in place?

The choice of office must take account of who needs to come to the office. An office where victims come to seek legal advice will have different requirements to an office which is primarily a place for staff to work. It is important to take account of how easy it is to get to by public transport, will it result in unsafe journeys between the area where staff live, those where most work activities take place, etc. The surrounding areas must be evaluated, especially in order to avoid having to travel through unsafe areas.

In some cases, the office may simply be the defender’s house (see rural area below). Yet, the above consideration must be given.

Once the location has been selected, it is important to undertake periodic evaluations of aspects of the location which can vary, for example if an ‘undesirable element’ moves into the neighbourhood.

CHECKLIST FOR CHOOSING A GOOD OFFICE LOCATION IN SERVED AREAS	
NEIGHBOURHOOD:	Crime statistics; closeness to potential targets of armed attacks, such as military or government installations; secure locations for taking refuge; other national or international organisations with whom you have a relationship.
RELATIONSHIPS:	Type of people in the neighbourhood; owner, former tenants; former uses of the building.
ACCESSIBILITY:	One or several good access routes (the more, the better. But remember that the undesired element will also have a greater choice); accessibility by public and private transport.
BASIC SERVICES:	Water and electricity, phone.
STREET LIGHTING	In the surrounding area.
SUSCEPTIBILITY TO ACCIDENTS OR NATURAL RISKS:	Fires, serious flooding, landslides, dumping of dangerous materials, factories with hazardous industrial processes, etc.
PHYSICAL STRUCTURE:	Solidity of structures, facility for installing security equipment, doors and windows, perimeter and protection barriers, access points (see below).
FOR VEHICLES:	A garage or at least a courtyard or enclosed space, with a parking barrier.

In case the office is located in a secluded, remote and badly served area, the result of the check list might indicate that several of the items do not exist in the area. Capacities will need to be developed to compensate for specific vulnerabilities. For example, if there are no other organisations around, you might consider resorting to the local community. Or, in case of no running water or extinguisher: make sure you have a big enough water recipient always full.

Third-party access to the office: physical barriers and visitor procedures

You now know that the primary purpose of office security is denying unauthorised people access. One or several people could enter to steal, acquire information, plant something which can later be used against you, such as drugs or weapons, threaten you, etc. Every case is different, but the aim remains the same: Avoid it.

Access to a building is controlled through **physical barriers** (fences, doors, gates), through **technical measures** (such as alarms with lighting) and **visitor admission procedures**. Every barrier and procedure is a **filter** through which anyone who wishes to gain access to the office must pass. Ideally, these filters should be combined to form several layers of protection, capable of preventing different types of unauthorised entry.

Physical barriers.

Barriers serve to **physically** block the entry of unauthorised visitors. How useful physical barriers are depends on their **solidity** and ability to cover **all vulnerable gaps** in the walls.

Your office can have physical barriers in three areas:

- 1 ♦ The **external** perimeter: Fences, walls or similar, beyond a garden or courtyard. In the absence of external physical perimeter, you may define the extension of external perimeter that you will keep under control.
- 2 ♦ The perimeter of the **building or premises**.
- 3 ♦ The internal perimeter: Barriers which can be created within an office to protect one or several rooms. This is particularly useful in offices with many visitors passing through, as it allows for a separate public area and a more private one which can be protected with additional barriers.

The external perimeter

The office should be surrounded by a clear external perimeter, possibly with high or low fences, preferably solid and high to make access more difficult. Railings or see-through wire mesh will make the organisation's work more visible, and it is therefore better to have brick walls or similar.

In the absence of clear external fenced perimeter, you can decide how much external extension you can visually control so as to be able to see undesirable elements getting closer to your office. You might consider using convex mirrors.

The perimeter of the building or premises

This includes walls, doors, windows and ceiling or roof. If the walls are solid, all the openings and the roof will also be solid. Doors and windows must have adequate locks and be reinforced with grills, preferably with both horizontal and vertical bars well embedded into the wall. The roof should offer good protection - not just a simple sheet of zinc or a layer of tiles. If the roof cannot be reinforced, block all possible access to the roof from the ground or neighbouring buildings.

If your office window faces the street or a public space, place your desk in such a way that you can see but not be seen. If it faces vegetation, make sure that no one can hide behind it unseen.

Some offices might have more doors and therefore one may serve as “emergency exit”. Remember that an emergency exit may also become an entry point for undesired elements

In a location with a risk of armed attack, it is important to establish secure areas within the office (see in this Manual the chapter on security in areas of armed conflict).

The internal perimeter

The same applies here as to the building or premises. It is very useful to have an area with additional security inside the office, and this is usually very easy to arrange. Even a safety deposit box can be considered an internal security perimeter.

Your office might be made of one room only in which case, you might consider the possibility to use mobile screens/partitions to keep private space away from the visitor sight.

A note on keys

- ▣ No keys should be visible or accessible to visitors. Keep all keys in a cupboard or drawer with a simple combination lock for which only a few group members know the code.. Make sure that the code is changed from time to time for greater security.
- ▣ If keys are individually labelled, do not mark them with a description of the corresponding room, cupboard or drawer, as this will make a robbery much easier. Use number, letter or colour coding instead.

Technical measures: Lighting and alarms

(in case your office has got access to electricity service or is equipped with an electricity generator).

Technical measures strengthen physical barriers or visitor admission procedures (such as spy holes, intercoms and video cameras. See below). This is because **technical measures are only useful when they are activated to deter intruders**. In order to work, a technical measure must provoke a particular reaction, for example, attracting attention from neighbours, the police or a private security firm. If this does not happen, and the intruder knows that it won't, such measures are of little use and will be reduced to preventing petty theft or recording the people who enter.

- ▣ **Lighting** around the building (of courtyards, gardens, pavement) and on landings is essential.
- ▣ **Alarms** have several purposes, including detecting intruders and deterring potential intruders from entering or from continuing to attempt access.

An alarm can activate a warning sound inside the office; a security light; a general, loud tone, bell or noise; or a signal in an external security centre. An audio

alarm is useful for attracting attention but can be counter-productive in conflict situations or if you don't expect local residents or others to react to it. A careful choice must be made between an audio and light alarm (a fixed powerful light, and an intermittent red light). The latter can be enough to deter an intruder, because it suggests that something else will happen following initial detection.

Alarms should be installed at access points (courtyards, doors and windows, and vulnerable premises such as rooms containing sensitive information). The most straightforward alarms are **motion** sensors, which activate a light, emit a noise or activate a camera when they detect movement.

□ Alarms should:

- ◆ have a battery, so they can function during power cuts;
- ◆ have a delay before they activate so they can be deactivated by staff who might set them off accidentally;
- ◆ include an option for manual activation in case staff need to turn them on;
- ◆ be easy to install and maintain;
- ◆ be easily distinguishable from a fire alarm.

Video cameras

Video cameras can help improve admission procedures (see below) or record people who enter the office. However, the recording must be made from a point which is beyond the reach of an intruder. Otherwise intruders can break open the camera and destroy the tape.

You may need to consider whether cameras will intimidate people you want to come and visit you such as victims or witnesses, or whether they will be seen as a valuable commodity which will attract thieves. It is good practice to post a warning notice if you are using a camera (the right to privacy is also a human right).

Lighting and alarms in case your office does not have access to electricity service or is not equipped with an electricity generator.

Simply avoid staying at your office once it is dark.

The electric alarm can be substituted with other alarm system: a night watch man, neighbours, family, community, dogs: Get their support and see how they can become your alarm system.

Private security companies

This area requires great care. In many countries, private security firms are staffed by ex-security force members. There are documented cases of such people being involved in surveillance of, and attacks on, human rights defenders. It therefore makes sense not to trust security companies if you have reason to fear

surveillance or attacks by security forces. If a security company has access to your offices, they could plant microphones or allow other people in.

If you feel you need to use a security company you should ensure that you have a clear agreement about what their personnel are allowed to do, and not allowed to do on your behalf, and which parts of the building they can access. Of course, you also must be able to monitor that these agreements are fulfilled.

For example:

If you have hired a security service that sends a guard in case an alarm breaks off, this guard may have access to sensitive parts of your office and might set up listening devices in your meeting room.

It is better if you can agree (and if possible screen) which specific staff will be working for you, but this is rarely possible.

If the security guards carry weapons it is important for the human rights organization to have a clear understanding about what their rules are for using them. But it is even more important to weigh the potential benefits of using weapons against their drawbacks. Hand guns are not a deterrence against attackers with higher fire capacity (as it is usually the case), but if attackers know that there are carriers of shot guns within your premises, they may decide to break in ready to open fire, to protect themselves during the attack. In other words, some armed capacity (small arms) will probably lead attackers to open use of arms with higher fire capacity. At this point it is worth asking yourself: if you need guards with sub-machine guns, do you have the minimum socio-political space in which to carry out your work?

Admission procedure filters

Physical barriers must be accompanied by an **admission procedure** “filter”. Such procedures determine when, how and who gains access to any part of the office. Access to sensitive areas, such as keys, information and money, must be restricted.

The easiest way to gain entry to an office where human rights defenders work is to knock on the door and get inside. Many people do this every day. In order to reconcile the open character of a human rights office with the need to control who wants to visit you and why, you need appropriate admission procedures.

In general, people have a particular reason to want to enter or knock on your door. They often want to ask a question or to deliver something, without necessarily asking permission first. Let’s examine this case by case:

Someone calls and asks for permission to enter for a particular reason.

You should then follow three simple steps:

- 1 ♦ **Ask the person both for their identity and reason of visit.** If s/he wants to see somebody in the office, consult the latter. If that person is not present, ask the visitor to return at another time or to wait somewhere outside the restricted office area. It is important to use spy holes, cameras or

entry phones to avoid having to open or approach a door, especially if you want to refuse someone entry or are facing violent or forced entry. It is therefore good to have a waiting area which is physically separate from the office's internal entrance. If an easily accessible public area is essential, ensure that there are physical barriers blocking access to restricted parts of the office.

Someone could request entry in order to check or repair the water or electricity supply or carry out other maintenance work. S/he could also claim to be a media representative, a state official, etc. Always confirm their identity with the company or organisation they claim to be representing before allowing them entry. Remember that neither a uniform nor an identity card are guarantees of proper and secure identification, especially in a medium or high-risk situation.

2 ♦ Decide whether or not to allow access. Once your visitor's identity and reason for entering has been established, you'll need to decide whether or not to allow them in. Just because someone states a reason for entering isn't a good enough reason to let them in. If you are not sure what their errand is, don't allow access.

3 ♦ Supervise visitors until they leave. Once a visitor has entered the office, make sure that someone is supervising them at all times until they leave. It is useful to have a separate area to meet with visitors, away from the restricted areas.

A record should be kept of every visitor with name, organization, purpose of visit, who they met with, time at which they arrived and left. This can be particularly useful when reviewing what went wrong after a security incident.

Someone arrives or calls asking questions.

Regardless of what a caller or visitor might say, you should under no circumstances tell them the location of a colleague or other people nearby, nor give them any personal information. If s/he is insistent, offer to leave a message, ask them to come or call back later or make an appointment with the person they wish to see.

People can often show up mistakenly, asking if so-and-so lives there or if something is for sale, etc. Some also want to sell things, and beggars can come looking for help. If you deny these people access and information, you will avoid any security risk.

Someone wants to deliver an object or package.

The risk you run with a package or object is that the contents could compromise or hurt you, especially in case of a package or letter bomb. No matter how the innocent it may look, do not touch or handle a package until you have taken these three simple steps:

1 ♦ **Check if the intended recipient is expecting the package.** It is not enough that the recipient knows the sender, because the sender's identity could easily be faked. If the intended recipient is not expecting a package, s/he must check that the supposed sender has actually sent them something. If the package is simply addressed to your office, check who sent it. Wait and discuss the issue before making a final decision.

2 ♦ **Decide whether or not to accept the package or letter.**

If you can't establish who sent the package, or if this will take time, the best option is not to accept it, especially in a medium or high risk environment. You can always ask for it to be delivered later, or collect it at the post office.

3 ♦ **Keep track of the package inside the office.** Make sure you know where in the office the package is, at all times until the recipient accepts it.

In some countries, a package is announced over the phone and it is the defender who has to go and pick it up. It might be a trick to attract the defender and expose them to aggression. As the phone might not be registered, it is impossible to track the caller down. Once the defender has enquired about the origin of the package, they can check the information with the alleged sender and ask them the route of the package. Then, the defender can decide whether it is safe to go and pick it up or not. They can also ask the caller to bring round to the office and follow the above procedures. Most probably, if it is a pretext, the caller will abstain from turning up at the office.

During functions or parties.

In these circumstances, the rule is simple: Do not let anyone whom you don't know first hand enter. Only people who are known to trusted colleagues should enter, and only when that colleague is present and can identify their guest. If a person shows up saying they know someone in the office check the information the person being mentioned and if s/he isn't there, don't let them in.

Defenders might hesitate and find it difficult to enquire about a visitor and send them away. However, they don't need to proceed on their own account. They can simply say that they are not authorised to let the visitor in.

Also, for all visitor admission procedures, remember that if the visitor is genuine, they will appreciate the care the organization takes in security and if the visitor is not genuine, they are aware that they also implement security procedures. So, whatever the case, defenders can simply give themselves the authority to deny entry to the unknown visitor. If it helps, they can use a "no and...": I am not authorized to let unknown visitors in however, if you care to leave your visit card, I will be pleased to inform you of future public events we might organise".

Keeping records of phone calls and visitors.

It may also be useful to keep a record of phone calls, phone numbers and visitors (in some organizations, new visitors are requested to present an identity document and the organization registers the number of the document).

Working extra hours at the office.

There should be procedures for staff working extra hours. Members of an organization intending to work extra hours late at night should report by certain hours with another designated member, take special care when leaving the premises, etc.

CHECKLIST: IDENTIFYING WEAK POINTS IN ADMISSION PROCEDURES

- ♦ **Who** has regular access to **which** areas and **why**? Restrict access unless it is absolutely necessary.
- ♦ Distinguish between different **types** of visitors (messengers, maintenance workers, computer technicians, NGO members for meetings, VIPs, guests for functions, etc.) and **develop appropriate admission procedures for each**. All staff should be familiar with all procedures for all types of visitors, and take responsibility for carrying
- ♦ Once a visitor enters the office, can they access weak points? Develop strategies to prevent this.

CHECKLIST: ACCESS TO KEYS

- ♦ **Who** has access to **which** keys and **when**?
- ♦ Where and how are **keys** and **copies** of those **kept**?
- ♦ Is there a **record of key copies** that are in circulation?
- ♦ Is there a risk that somebody will make an **unauthorised key copy**?
- ♦ What happens **if somebody loses a key**? The corresponding lock must be changed, unless you are absolutely sure that it has been accidentally mislaid and that nobody can identify the owner of the key or your address. Remember that a key can be stolen – for example, in a staged robbery – in order for someone to gain access to the office.

All staff members have a responsibility to take action against anyone who is not properly observing the admission procedures. They should also make a note in the security incidents book of any movements by suspicious people or vehicles. The same applies to any object placed outside the building, in order to rule out the potential risk of a bomb. If you suspect a bomb, don't ignore it, **don't touch it**, and do contact the police.

When moving offices, or if keys have been lost or stolen, it is essential to change all the locks in the entrance area, at the very least.

Checklist: General office security procedures

- Provide fire extinguishers and flashlights (with replaceable batteries). Make sure all staff members know how to use them.
- Provide an electricity generator if there is a strong possibility of power cuts. Power cuts can endanger security (lights, alarms, telephones, etc.), particularly in rural areas.

- Keep a list handy of local emergency numbers for police, fire brigade, ambulance, nearby hospitals for emergencies, etc.
- If there is a risk of conflict nearby, keep a supply of food and water in reserve.
- Establish the location of secure areas outside the office for emergencies (for example, the offices of other organisations).
- Nobody from outside the organisation must be left **alone** in a vulnerable area with access to keys, information or valuables.
- **Keys:** Never leave keys where visitors might have access to them. Never “hide” keys outside the office entrance – this makes them accessible, not hidden.
- **Admission procedures:** Security barriers offer no protection if a potential intruder is allowed to enter the office. The main points to bear in mind are:
 - ◆ All group members are equally responsible for visitor control and admission.
 - ◆ All visitors must be accompanied at all times while in the office.
- If an unauthorised visitor is found in the office:
 - ◆ Never confront someone who seems prepared to use violence to get what they want (for example, if they are armed). In such cases, alert colleagues, find a safe place to hide and try to get help from the police.
 - ◆ Approach the person carefully or seek assistance in the office or from the police.
- In high risk situations, always keep control of vulnerable things, such as the information stored on a hard drive, in order to make them inaccessible or remove them in case of an emergency evacuation.
- Bear in mind that in case of confrontation with a potential intruder, the people working in the office are on the front line. Ensure that they have the necessary training and support at all times to deal with any situation, and without putting themselves at risk.

Regular inspections of office security

Regular supervision or inspection of office security is very important, because security situations and procedures vary over time, for example, because equipment deteriorates or if there is a high staff turnover. It is also important to achieve some sense of staff ownership of the office security rules.

The person responsible for security must carry out at least one review of office security **every six months**. With the help of the list below this can take as little as one or two hours. The person in charge of security must ensure that staff feedback is sought before the final report is written, and then present the security report to the organisation in order for the necessary decisions to be made and for action to be taken. The report should be kept on file until the next security review.

CHECKLIST: OFFICE SECURITY REVIEW

REVIEW OF:
CARRIED OUT BY:
DATE:

1 ♦ EMERGENCY CONTACTS:

- ♦ Is there a handy and up to date list with telephone numbers and addresses of other local NGOs, emergency hospitals, police, fire brigade, ambulance, International NGOs and embassies?

2 ♦ TECHNICAL AND PHYSICAL BARRIERS (EXTERNAL, INTERNAL AND INTERIOR):

- ♦ Check condition and working order of external gates/fences, doors to the building, windows, walls and roof.
- ♦ Check condition and working order of external lighting, alarms, cameras or video entrance phones.
- ♦ Check key procedures, including that keys are **kept securely** and **code-labelled**, assignment of **responsibility** for controlling keys and copies, and that keys and copies are in **good working order**. Make sure **locks** are changed when keys are lost or stolen, and that such incidents are **logged**.

3 ♦ VISITOR ADMISSION PROCEDURES AND "FILTERS":

- ♦ Are admission procedures in operation for all types of visitors? Are all group members and staff familiar with them and do they implement them?.
- ♦ Review all recorded security incidents related to admission procedures or "filters".
- ♦ Ask those staff members who usually carry out admission procedures if the procedures are working properly, and what improvements are needed.

4 ♦ SECURITY IN CASE OF ACCIDENTS:

- ♦ Check the condition of fire extinguishers, gas valves/pipes and water taps, electricity plugs and cables and electricity generators (where applicable).

5 ♦ RESPONSIBILITY AND TRAINING:

- ♦ Has responsibility for office security been assigned? Is it effective?
- ♦ Is there an office security training programme? Does it cover all the areas included in this review? Have all new staff members been trained? Is the training effective?

In rural areas:

Defenders also work in rural areas either in a village or in a secluded and remote area. They might not have much choice as to their office location. Yet they need to protect their space from unwanted visitors and objects.

Village: if it is comparable to a micro urban area most of the above considerations may be taken and completed with the following ones.

Remote and secluded location: make sure that the surrounding community, your family and friends can contribute to your alarm system. Try and have them check regularly on you and your office (whether it is your home). You might consider keeping a dog which can be trained to barking at visitors. Make sure it doesn't attack people and that it cannot easily be approached and poisoned.

Get to the area well and avoid being out at dark.

You might consider establishing communication relays through trusted people to have access to as quick a supportive reaction as possible in case you need it.

Summary

The aim of office/home security measures is to reduce the risk of unwanted access

The security of an office is no greater than its weakest point.

Whether your office/home is located in an urban or rural area, you can use the equation in order to reducing the risk of unwanted access.

Threats might be assimilated to consequences of risks.

List all your threats/consequences of the risk of unwanted access. Then, per threat/consequence, list respective vulnerabilities and capacities and work on them.

