Security Risk Management Toolkit: Security Plan

READY to go Mobile Guide

Learn about the essential information to include in a security plan to keep your organization, partners, staff, and communities safe.

Security Plan Structure

Note to Learners

The information in this guide is for educational purposes only; it is not intended to be a substitute for professional or specialist security advice. Any reliance you place on such information is therefore at your own risk and the European Interagency Security Forum (EISF) will have no responsibility or liability under any circumstances.

Tips for Creating an Effective Security Plan

Security plans are not strategic documents. They should be simple, easy to use, and provide information in a format that staff can easily read, understand, and use in their daily work. A security plan is critical to all staff and organizations because it advises staff on how to manage and treat potential security risks and threats. Follow these tips for creating an effective security plan for your organization.

Involve a mix of staff (senior management, administration, program management, field staff, and drivers) as well as different nationalities, ethnicities, and genders in the creation of the security plan. This will provide different perspectives, create a sense of ownership of the plan, and improve compliance.

Focus on detailed security measures for front-end staff in the field as they may be most at risk. Avoid having too much of a management focus.

Consider the exposure to risk for all staff at all levels and in all locations, including national staff delivering programs. Avoid focusing only on a particular group of staff, such as international staff.

Identify if there are specific vulnerabilities of staff with minority profiles that could put them at risk in the working environment. Develop appropriate measures when necessary and raise awareness among staff about these risks.

Follow a general format and provide information that considers key factors about the organization such as the type of engagement, number of staff and size of assets, location of projects, operating context, and other localized factors.

Limit the plan to 20 pages or less to keep the information manageable and easy for staff to read, remember, and use.

Explain clearly to all staff the reasons for different measures for international, national-relocated, and local staff (if it is part of the security plan). Otherwise, the organization may be perceived as only caring for a particular group of staff.

Make the security plan, or at least the relevant parts, available in the language of the users. If translation is not feasible, consider alternative ways to disseminate the information in the security plan.

Explain the security plan to all levels of staff, including those who are less involved in the organization such as cleaners and watchmen. Informing all employees can help prevent staff from sharing or accepting offers of money in exchange for confidential information that could impact the safety and security of staff and your organization.

Elements of a Security Plan

Include these key elements in your organization's security plan.

Overview of the Security Plan

- Explain the purpose of the plan and why it is important for all staff.
- Identify who is responsible for preparing the plan, updating it, and training staff.
- Determine your risk threshold; what level of risk can your organization manage and what level is too high or unacceptable.
- Describe your security strategy; how your organization uses acceptance, deterrence, and protection strategies, and how you evaluate the results.
- Include the date the plan was written, and when and how often it should be reviewed and updated.

Current Context (Your Risk Assessment)

- Describe the overall context including a general description of the country and the region, and current challenges.
- Explain your risk assessment system including how are you identifying threats and your rating system.
- Identify the threats you face in your context and consider internal threats.
- Evaluate these threats and provide their risk rating.

Standard Operating Procedures (SOPs)

Determine Standard Operating Procedures (SOPs) for all the threats and risks identified in your security risk assessment. Provide simple, clear instructions for how staff should prevent risk (reduce probability) and how to react if an incident occurs (reduce impact). Use checklists, procedures, or actions to address the following areas:

- Cash in transit
- Communications strategy and social media plan
- Incident reporting and internal threats (harassment, bullying)
- Field travel and vehicle safety
- Fire (in the office or compound)
- Office and facility access control
- Robbery and theft
- Vehicle accident
- Other SOPs

Other Key Sections

Provide other key information that is relevant for your organization, staff, and programs, such as:

- Health and safety policies to protect staff from physical and mental threats such as illness (malaria, HIV), injury, accidents, stress, and post-traumatic stress disorder (PTSD)
- Human resources policies related to recruitment, background checks, contracts, and confidentiality
- Diversity and anti-discrimination policies, including information about how your organization accommodates for specific vulnerabilities of staff and mitigation measures against internal threats (reporting systems, whistleblowing)
- Administrative and financial security policies for preventing theft, fraud, corruption, as well as cash handling and procurement
- Other key sections

Crisis Management Section

- Describe who is part of your Crisis Management Team (CMT) and their reporting lines.
- Explain how the CMT will be activated in an emergency situation.
- Describe contingency plans for any crises that may occur such as kidnappings, natural disasters, evacuations, or armed conflict. Unlike SOPs, contingency plans are an internal management tool that are not for general distribution or public knowledge.

Facility Security

Securing Offices, Compounds, and Other Facilities

When considering a new office, residence, or compound, it is critical to first review your organization's security risk assessment to understand types of threats, the level of each threat, and what level of protection or deterrence you will need to mitigate such threats. This also applies if you are moving into an existing office with a partner organization.

Consider building an acceptance strategy for all organizational properties, offices, residences, warehouses, clinics, and schools in the locations of operations. This can be more difficult in large urban environments and is easier to manage in rural settings; however, it is always advisable to create mutual understanding with your neighbors. If an acceptance strategy is possible, it is important to agree on who is responsible for managing different security measures such as perimeter security, guard services, local acceptance strategy, and other measures.

Securing the Neighborhood

The neighborhood is the area surrounding the office, compound, facility, or residence. People in this area could have an effect on the safety of staff. Your risk assessment should identify key elements to secure the neighborhood surrounding your place of work.

Identify stakeholders in the neighborhood who will implement your acceptance strategy. Developing understanding with your neighbors is essential in all contexts either in rural areas or urban environments.

Determine the type of road access to the office and how staff will safely travel to other sites. A dead-end road can be an advantage for hostile observation, but it will limit travel options and escape routes.

Determine natural hazards such as rivers (flooding), hills (mudslides/avalanches), swamps (malaria/dengue), or forests (fire/wildlife).

Locate neighboring embassies, military/police posts, banks, government offices, other NGOs, or universities.

Calculate the distance to airports, hotels, and key locations in an emergency.

Identify blocking structures and natural features that would interrupt satellite communications in an emergency.

Review the landlord's record and reputation.

Identify reliable sources of and access to clean water.

Determine reliable access to telephone, the internet, and mobile networks.

Securing the Property

The property is the first area that is under the organization's control. Your security risk assessment should identify:

- Your protection strategy and the ways to secure the area using a perimeter wall, fence or hedge.
- If you feel the need to build a 'bunker' to stay safe, then you probably should not be based in that area.

Planning the Perimeter

Consider the following when planning the perimeter of your organization's property:

- How will your presence impact your neighbors, your organization's image, and the message it sends?
- Do you require a generator? If you do, can it be positioned away from other properties and/or is there room for soundproofing?
- Is there sufficient parking within the compound and/or in the area without inconveniencing others?
- Is your presence creating a security risk for your neighbors?
- If you are employing guards, where will they be located?

Building Protection Measures

It is possible to build protection measures that do not negatively change the appearance of the compound. For example, using barbed wire below the top of the wall or using flower beds or pots to disguise concrete barriers. Consider the following potential issues on your property:

- How do staff, visitors, suppliers, or community members access your property?
- How will vehicle/personnel gates, identity checks, safe parking areas, ID cards, waiting areas, and crowd control (if applicable) be managed?
- How easy is it for people to get into the site?
- Are there shared boundaries with neighbors or open spaces?
- Are there overhanging trees and how close are the buildings to the boundary walls?
- What are potential fire hazards (storage of fuel and combustibles, electrical power lines, designated smoking areas)?
- How is trash collected and dealt with in a safe and environmentally sound way?
- How will you manage emergency exits?
  - ✓ If your compound has a wall and main gate facing the street, how will staff evacuate unobserved if there is a danger in front of the facility?
  - ✓ How will mobility-impaired staff exit safely?
  - ✓ Where will staff go once they are off the property?
  - ✓ Is there a neighboring compound, UN facility, other NGO, or residences staff could access?

Securing the Building

Security for your organization's buildings, whether they are offices, compounds, warehouses, or residences, is key as these hold your most valued items including people, equipment, assets, cash, records, and aid materials/supplies. The design of the building should also be appropriate for natural hazards (earthquake resistant, insulated against heat/cold). It is also important for staff to feel safe in their office and accommodation. Your risk assessment should identify these key elements to secure the organization's buildings.

Secure doors and windows to prevent unauthorized access, but do not trap staff in the event of a fire or evacuation.

Secure roof areas (often a preferred entry point for robberies after hours).

Set up a reception area that controls access to other vulnerable areas.

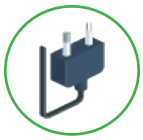
Establish and enforce access control procedures so that visitors cannot roam around the building unsupervised.

Schedule regular electrical inspections to reduce fire risk and establish strict policies to prevent overloading of electrical outlets.

Ensure safe storage of documents including fireproof safes secured to the wall or floor.

Identify and label emergency evacuation routes. Train staff on evacuation procedures and practice emergency evacuation measures. Ensure that the training includes how to assist the evacuation of staff with mobility impairments (using evacuation chairs).

If needed, set up a safe room that will fit all staff in the building and is equipped with emergency supplies (first aid kit, flashlights, blankets, food, fire extinguisher, communication devices that are charged/powered). Check that the emergency communication equipment works in the safe room. Satellite phones normally require line of sight, so external aerials may be needed.

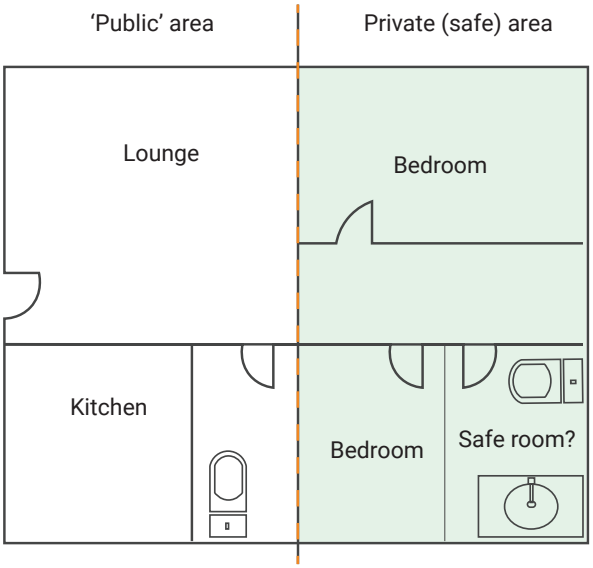


Set up uninterrupted Power Supply (UPS) units to protect computers and other electrical devices when the power supply is not reliable or subject to spikes and power cuts.

Install and test alarms for fire or intrusion. Inform staff of action steps to take when hearing these alarms and practice emergency evacuation measures. Ensure the alarm system can be recognized by staff with hearing or visual impairments.

Securing Staff Residences

Securing staff residences can be approached in a similar way to other properties, but with some additional precautions to ensure safety. While the entire residence needs to have adequate security, valuables (TVs, computers, appliances) are usually held in the 'public' areas of the house where guests or friends may be entertained, and these items are likely to be the principal lure for thieves. Private areas of the residence that include sleeping areas should be more secured than 'public' areas.



Install a solid, lockable door between the public and private areas of the residence.

Improve window and roof security in private areas. Windows should be lockable from the inside, but not create an obstacle in the event of a fire for evacuation.

Stock the safe room with first aid kits, blankets, flashlight, fire extinguisher, and a communications device that is charged and tested regularly.

Install window screens to keep out mosquitos (to prevent disease).

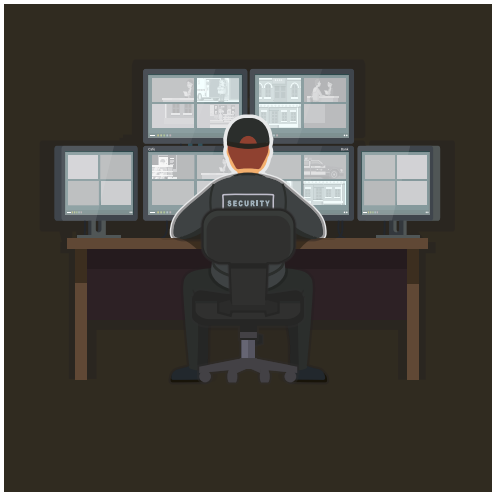
Maintain a firm control of keys and any duplicates.

Install exterior lights, especially around entrances.

Consider local culture. In a conservative environment, you may need to have separate male and female quarters. You may also need to consider the separation between national staff such as guards and drivers, and international staff. This separation may be needed to allow international staff to not worry about giving offense or the wrong impression by drinking alcohol, dancing, or wearing specific clothing that is not accepted in the local culture.

Watchmen and Security Guards

Many organizations decide to work with local watchmen and/or security guards as a first step to developing their security systems for facilities. Organizations often use the term 'watchmen' rather than 'guards' to infer that staff is not expected to risk their own safety to protect the compound and assets. Guards are often the first point of contact between the host community and an organization. The behavior, manners, and professionalism of watchmen and guards will often reflect back on their employer. Follow these guidelines when working with guards or watchmen.



- ✓ *Inform guards of your organization's mandate and Code of Conduct.*
- ✓ *Give guards clear instructions on their duties and how they will be supervised.*
- ✓ *Provide guards with a list of actions on how to manage visitors, suspicious activity, robbery/theft, fire, injuries, or other incidents that likely to occur in the environment and are also identified in your security risk assessment.*
- ✓ *Ensure that staff members treat guards with respect and understand their duties to ensure compliance.*
- ✓ *Give guards an emergency contact list and determine a means to communicate if an incident should occur.*
- ✓ *Guards working for NGOs are usually unarmed. However, in high-risk environments, some organizations may have an armed response in case of emergency, either activated by panic buttons or existing guards. If this is the case for your organization, get information about who provides the armed service (private company, police, military), its purpose (protecting the organization's staff and assets or apprehending the attackers), their level of training, and your organization's liability if someone (staff, guard, bystander) is shot during an armed response.*

Commercial Guard Services

Commercial guard services are provided by a contracted guard services company. The guard company may rotate its staff which can make it difficult to create a level of trust between the guard and organizational staff. It is important, particularly for residential buildings, that staff members know and trust the guard onsite, otherwise, the guard can create feelings of insecurity rather than alleviating them. Here are some advantages and disadvantages to working with commercial guard services.

Advantages

- The guard service company can offer additional services such as a rapid response team (be clear on what this involves), alarms, radio networks, vehicle patrols, and night supervisors.
- The guard service company is in charge of managing recruiting, training, payroll, human resources, administration, and scheduling.

Disadvantages

- The organization has little or no control over the guard's instructions and duty standards.
- Guard service companies are mostly concerned with making a profit over the organization's security needs.
- Guards can often be underpaid and unmotivated.

Contracted Guards

Contracted guards are employed directly by the organization. Here are some advantages and disadvantages to working with contracted guards.

Advantages

- Guards are often better paid since the money of the aid organization is not for commercial profit.
- As members of staff, guards have increased loyalty and knowledge of the organization's standards, policies, and code of conduct.

Disadvantages

- The organization is fully responsible for recruiting, training, providing uniforms, equipment, administration, and supervision of contracted guards.
- There is no additional support available to help manage a contracted guard.

Community Volunteers

Community volunteers are usually guards provided by the host community in program areas. They are often the only option in remote areas. The organization usually covers the cost of salaries, training, and minimal equipment. Here are some advantages and disadvantages of working with community volunteers.

Advantages

Employing local guards supports an “acceptance strategy” approach by incorporating the community into security risk management.

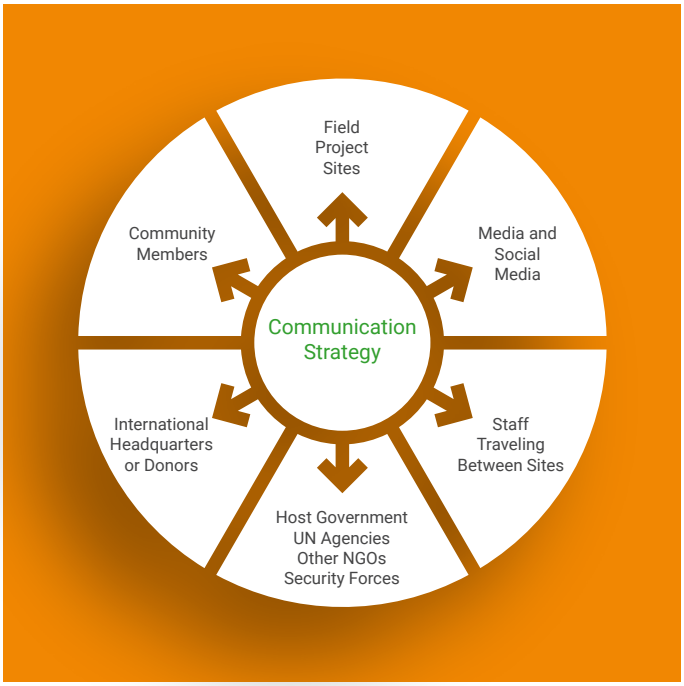
Disadvantages

- No set standards for duties.
- Lack of accountability.
- Open to abuse of power and misconduct.

Communications and Information Security

Planning Your Communication Strategy

In setting up any new deployment or program, it is important to identify what types of communications will be available (landline, mobile networks, satphones, internet, surface mail, courier) and how reliable they are likely to be in your operating environment. In the modern world, communication is considered a key 'survival' need just as much as food, water, and shelter. As part of your communication strategy planning, consider what you will need to effectively communicate with different staff, partners, and key stakeholders.



Community Members

- Engagement
- Building acceptance
- Planning
- Consultation

Field Project Sites

- Program management
- Safety reporting
- Progress reports
- Coordination
- Monitoring and evaluation
- Staff health and welfare

Media and Social Media

- Publishing stories
- Fundraising information
- Managing expectations
- Controling messaging
- Reputation risk

Staff Traveling Between Sites

- Reporting delays and vehicle issues
- Safety and security during travel
- Breakdowns and accidents
- Travel delays
- Road safety issues

Host Government UN Agencies

- Coordination
- Emergency messaging
- Reporting incidents

Other NGOs Security Forces

- Negotiating access
- Requesting support

International Headquarters or Donors

- Reporting
- Crisis management
- Donor requirements
- Funding proposals
- Program evaluations

Tips for an Effective Communication Strategy

Follow these tips to set up an effective communication strategy for your organization, partners, and staff.

Budget early for reliable communication systems. Have a backup and alternate systems for replacing damaged, lost, or stolen equipment.

Be aware of new technologies that can cost-effectively improve your communications. This may include satellite 'back-packs' for smartphones or satellite messaging systems rather than traditional voice phones. Buy the best you can afford.

Consider the image your communication equipment conveys. If having a low profile is part of your security strategy, adding high frequency (HF) radios and aerials to vehicles to make you stand out as much as an organizational logo.

Never assume the internet and mobile networks will be reliable. During security emergencies, conflict, civil unrest, or after natural disasters, governments often take control of (or shut down) networks at the time when you will need them most. For this reason, do not only rely on one single system whether it is a landline, mobile networks, satellite phones, the internet, or other systems.

Be creative. In emergencies, organizations need to have alternate ways to communicate with remote staff and communities if phones or the internet go down. Some creative ways include using taxi drivers and even camel riders to deliver messages to others.

Identify communication systems that require a license. Radio or satellite systems may require a license to operate. The United Nations may be able to give support in obtaining such licenses. Your organization should budget for airtime and/or licensing where necessary.

Tips for Communications Security and Procedures

Follow these tips on how to establish and maintain an extensive communications network to ensure the safety, security, and success of operations.

Train staff on how to use radio networks or satellite phones (if available) as part of their induction. Brief them on where the equipment can be used in their working environment (in and outside) and address any challenges (black spots).

Ensure staff can communicate with family and friends during deployments, especially in emergencies.

Use social apps for sharing information in real-time directly between staff (WhatsApp, Telegram). Set clear guidelines on what information can or cannot be shared in these apps, and the procedures to follow for acting upon the information received.

Inform staff of all communication procedures and guidelines. Make written procedures and essential emergency contact information, including phone numbers, frequencies, and call signs, easily available in the office, for each vehicle, and on a card, for each staff member to carry.

Test communication systems and equipment regularly and have backup power supplies for radio and mobile/satellite phone charging.

Instruct staff on how they should not transmit sensitive information, such as the transfer of cash or travel plans, in plain language over the radio or phone networks.

Obtain approval from the host nation's government and licensing prior to using communication equipment, including radios, cellular phones, and satellite phones.

Obtain multiple VHF and HF frequencies for radios for each office when possible. Coordinate with other organizations such as the United Nations to use their radio networks.

Perform routine checks of SMS, satellite phone calls, or radio with remote offices and travelers in the area (as appropriate).

Implement a policy for when a staff member or team fails to check in and cannot be contacted. Make sure all staff are familiar with this policy and enforce it.

Establish duress code words or phrases for common emergency conditions, such as kidnapping or intrusion, and inform staff of these codes.

Monitor radios and emergency phones 24 hours a day (as appropriate).

Tips for Information Security

International aid and development organizations are not always regarded as neutral, independent entities. They intervene, hold accountable, advocate, and often subsume activities normally associated with governments such as health care, water, sanitation, and emergency relief. In many circumstances, they undertake these activities while funded by 'Western' governments with their own political agendas. This can make humanitarian organization's work seem suspicious in some people's eyes.

Follow these tips to help reduce your organization's vulnerability to information security risks.

Be cautious of anything you or your colleagues write in an email that could be read by criminals or government agents. Governments can monitor other organizations' phone calls, internet activity, and social media, and may have the ability to hack computer hard drives.

Be aware that criminal organizations may perceive your organization as a 'wealthy target' based on its use of vehicles, laptops, satellite phones, as well as publicly announced donor funding levels.

Restrict staff from saving personal and sensitive information on your organization's shared drive. Their data could include inappropriate photos, personal information, and context analysis that may be misunderstood or deemed insulting by other staff.

Determine the type of business and personal information that is safe and unsafe to kept on mobile devices such as smartphones as this might easily be lost or stolen.

Assess the impact information may have if it falls into the wrong hands, such as harassment of staff, dissemination of inappropriate photos, or access to emails or office VPN/server.

Back up all files regularly and keep backup copies of all key documents and records (government agreements, legal documents, bank records, HR records) off-site in case of fire, flooding, theft, or other events that could destroy the originals.

Use shredders for any files that are not kept in safe storage.

Do not leave paper documents in trash bins or on desks. This could allow information leaks if they are left for cleaners and other staff or visitors to see, copy, or remove.

Maintain good security firewall systems on any server.

Minimize staff access to networks with non-organization computers, tablets, or phones to prevent the spread of viruses.

Set up verification processes for information received through WhatsApp and other social apps that make it easier to share information directly between staff. There should also be clear guidance on what should and should not be shared.

Remember that messaging software like Skype is not secure against hacking.

Establish a social media policy that makes it clear to staff what they can and cannot post on social media sites.

Avoid communications that could make you appear to be gathering ‘intelligence’ or passing any military or security information to foreign governments, donors, or your NGO’s headquarters.

Avoid encrypting information whenever possible as this may send the wrong message to staff and partners, particularly if your NGO claims to be open and accountable. You may be questioned about the need to encrypt documentation.

Avoid desktop computers when possible. Although laptops are easier to steal, they are more mobile if the office or project needs to be relocated.