

# **SAFETY– SECURITY GUIDELINES**

## **NIHR GUIDELINES**

### **What this safety guide line means?**

NIHR's most precious resource is our people, whose safety and security is paramount. NIHR is committed to maximising our impact on vulnerable communities, while minimising safety and security risks to our staff, and ensuring that they receive training, support and information to reduce their risk exposure.

### **The Goal**

Provide community in insecure environments with much-needed assistance must be balanced with our responsibility to ensure staff safety and security

### **Policy Objective:**

1. Enhancing staff security and safety approach
2. Enhancing decision making process in critical situations
3. Strengthening ownership and ensuring sustainability of survival plan
4. Improving Coordination and networking to keep communications
5. Minimize threats and increase protection measures

### **Policy scope:**

In recent decades, aid workers have increasingly found themselves operating in complex and rapidly changing socio-political environments. As a result, they face numerous risks in providing vital assistance to communities torn apart by conflict and civil unrest. Providing assistance during armed conflicts has always been dangerous but, until recently, aid

### **Responsibility:**

NIHR's general assembly, board of directors and staff are responsible for the full implementation of the policy

### **What to Safety guideline**

The security management framework opposite demonstrates how the safety and security management process can be divided into individual components:

- Assessment The first stage in the security management framework is to develop a thorough understanding of the operational environment. Aid agencies often operate in politically and socially complex environments that change rapidly. In order to adapt security management accordingly, and anticipate possible risks to staff, field teams must understand and critically analyse the environment around them. If you analyse the operational context in sufficient detail, you'll be

able to draw out the information needed to make a realistic assessment of the risks. A comprehensive risk assessment should determine both the likelihood and the potential impact of the various threats that staff faces.

- **Planning.** You then need to identify different mitigation strategies that can be implemented to reduce these risks. The strategies you adopt will depend on the risk assessment, your organisation's values and mandate, and its programme activities in that particular context. You should then put these strategies into practice through the development of safety and security plans. Safety and security plans must be established for the country and, where relevant, for particular programme areas, and should include standard operating procedures (SOPs) and contingency measures or plans for foreseeable

### **High-risk incidents.**

Ensuring the effective day-to-day management of safety and security issues, and compliance by all staff, is often The most challenging aspect of the process.

Operational safety and security management – concerning the routine actions, measures and procedures that govern how staff work in the office, travel to the field,

### **Internal factors**

1. Agency values and mandate
2. Programme activities
3. Global safety and security policy
4. Other organisational policies and procedures
5. Crisis management plan
6. Staff competencies
7. Security training
8. Resources

### **External factors**

1. Government and local authorities
2. Geography and climate
3. Infrastructure
4. Society and culture
5. Inter-agency collaboration
6. Media
7. Image and perception of NGOs

### **IMPLEMENT**

Operational safety and security management

1. Staff induction and briefings
2. Site safety and security
3. Travel and movements

4. Vehicle safety
5. Communications
6. Information management
7. Incident management

## **REVIEW**

### Security reviews

1. Safety and security plan update
2. Minimum standards audit
3. Safety and security management review
4. Post-incident investigation

Monitoring thorough safety and security management requires ongoing monitoring, analysis and mapping of all security incidents. If you make sure that this is done for each security incident that occurs in a particular context, you'll acquire new information and a better understanding of the overall security situation. As your awareness improves, you must continually review each component of the security management framework to ensure that it remains appropriate to the changing situation.

- **R e v i e w .** Security management is a dynamic process and must be continually reviewed. Safety and security plans should be updated and circulated to staff as a matter of routine to ensure plans remain
- **Relevant and effective.** It is also important to carry out periodic reviews of safety and security management in each country to determine whether it meets your organisation's minimum standards, and to
- **Ensure that the most effective management practice is in place.**
- **In the event of a serious incident involving staff, there should be a detailed investigation into the various decisions and actions taken and, subsequently, a review of the safety and security measures in place** The analysis and recommendations raised in these various
- **Reviews should feed back into the relevant components of the security management framework.**

A number of additional factors will influence the management of safety and security at each stage in the security management framework. These include:

1. **Internal factors.** An organisation's ability to manage safety and security in the field will be shaped by many internal factors, such as the agency's mandate and values, its programme activities, the various policies and procedures in place, the level of training provided to staff, and the material and financial resources available.
2. **External factors.** Agencies do not operate in a vacuum and many external factors will affect their ability to manage insecurity. For example, in highly

politicised environments the sensitive relationships that often exist between aid agencies and authorities (government, police, military or rebel factions, etc.) may restrict the security measures that can be utilised. Equally, the actions, or inaction, of other agencies in the same environment will affect how an agency manages its own security.

## **UNDERSTANDING THE CONTEXT**

1. Causes. Investigate what appears to be the main causes of the conflict or violence, and consider how these may have changed over time.
2. Areas affected. Identify the areas in which the fighting or violence occurs, or has taken place in the past. Consider which areas are strategically more important and why.
3. Relationships with civilian population. Determine whether certain groups have a strong support base in the community, or whether they have a more abusive relationship with the civilian population. Consider how your programme or presence could threaten and/or undermine these relationships.
4. Nature of violence. Examine whether terror tactics are adopted by any particular group and whether violence is orchestrated or spontaneous. Identify who their main targets are and why.
5. Political or military developments. Consider what impact political or military developments at the national, regional or global levels will have on the conflict or level of violence in the area where you are operating.

### **You need to investigate in more detail the following:**

1. Types of crime. Research the different types of crime that occur in your area and who appear to be responsible for these crimes.
2. Where it occurs. Identify any patterns with regard to the location of incidents, to determine whether certain areas are more at risk than others.
3. Who is targeted? Examine whether crime is widespread or whether particular groups, including humanitarian agencies, are being targeted.
4. Nature of criminal activity. Consider whether criminal activity is organised or opportunistic. Determine whether weapons and violence are associated with these crimes

## **ASSESSING THE RISKS**

Everyone faces risk in their daily lives. You will try, often subconsciously, to reduce a risk by adopting a measure to make yourself less vulnerable to it: for example, choosing to use a pedestrian crossing rather than crossing a road at its busiest point. This kind of ad hoc assessment is not adequate in the humanitarian environment, however, given the scale and nature of the risks, many of which you may be able to identify in advance. Identifying the threats developing and maintaining a constant awareness and understanding of threats that exist in your surroundings is the first step in assessing risk.

**Types of threats**

Inherent threats (Non-targeted threats)	Targeted threats
<ol style="list-style-type: none"> <li>1. Work and travel – ill health; work place accidents; vehicle accidents;</li> <li>2. Air crashes; boat accidents, etc.</li> <li>3. Natural hazards – earthquakes;</li> <li>4. Floods; avalanches; wildlife, etc.</li> <li>5. Wrong place, wrong time – demonstrations and rallies; indiscriminate violence; looting; crossfire; military actions, etc.</li> <li>6. • Indiscriminate weapons – mines and unexploded ordnance (UXOs); shelling and aerial bombardment; chemical and biological weapons, etc.</li> </ol>	<ol style="list-style-type: none"> <li>1. Crime – armed robbery or theft; arson; ambush; carjacking; bribery, extortion and fraud, etc.</li> <li>2. Acts of violence – bodily harm;</li> <li>3. Assault; sexual violence, etc.</li> <li>4. Acts of terror – bombs/improvised explosive devices (IEDs); suicide attacks; shootings/assassinations, etc.</li> <li>5. Staff disappearance – detention</li> <li>6. Arrest; abduction; kidnapping, etc.</li> <li>7. Psychological intimidation – harassment; death threats, etc.</li> </ol>

**Considering your vulnerability**

It's important to understand why individual staff members, your agency, or humanitarian agencies in general are more or less likely than others to be affected by the threats in the same environment.

**Determining the risks**

Balancing the operational demands of responding to a particular situation or working in a particular area against the need to reduce exposure to security risks is a constant juggling act. It is neither possible nor effective to put in place extensive security measures to deal with every possible threat. You must analyse the different threats to determine which pose the greatest

Risk. These should then become the focus of your security measures.

Very high risk	Immediate response and extreme measures required. Is the risk acceptable?
High risk	Implement specific safety and security measures and contingency plans
Medium risk	Significant safety and security measures required
Low risk	Requires heightened awareness and additional procedures
Very low risk	Managed by routine security and safety procedures

### **Acceptable risk**

Not all agencies will accept the same level of risk; a particular agency may interpret a security situation differently or, because of its mandate, will

Be more or less willing than others to accept higher levels of risk. Some agencies may decide to remain in a high-risk area because they feel that the benefits to the local population outweigh the risks to which their staffs are exposed.

Others, however, may be unwilling to operate in the same environment.

### **SECURITY PLANNING AND DOCUMENTATION**

Having gained an understanding of the risks associated with your location, the next step is to identify ways to minimise them. Often an agency's approach to minimising risks to staff concentrates on the development of local or 'field-based' safety and security documents. Although these are of course important in themselves, what's crucial is the strategic thinking behind them

### **Security strategies**

The different approaches used to manage security risks fall into three broad strategies: acceptance, protection and deterrence.\* The acceptance-based strategy seeks to reduce or remove threats by developing and maintaining widespread acceptance, among all actors, of your presence and work.

## **Acceptance strategy**

How you and your agency are perceived has a fundamental effect on your security. It's a mistake to assume that everyone will understand the concept of humanitarian aid. Similarly, don't assume that various groups in the community know who your organisation is, what work you are

1. Doing and why. All staff must be fully aware of the programme's objectives and be able to communicate them to the different actors your agency interacts with
2. Relationships: It's important to develop and maintain good relationships with individuals, community leaders, governments and authorities – even local commanders
3. Negotiation: In highly politicised environments it's important to obtain from all the different actors their consent for your organisation to operate freely and unhindered, and have access to the areas of humanitarian need. For example, even if you may have permission from the relevant authorities to operate in certain areas, other groups may view your presence or activities with suspicion
4. Participation. The way in which you identify, design and implement your programmes will either enhance or diminish your acceptance.
5. If the community feel they have a stake in the programme and have been consulted in its design and implementation, this can improve your overall security
6. Dissemination. Consider how you communicate and what you say about your agency's goals and activities in the media, public meetings, at checkpoints or in the local bar, and what impact this might have on your acceptance
7. Image and perception. As well as the explicit messages you communicate, it's equally important to be aware of the implicit messages you may convey through your appearance or behaviour, or what you say and do

## **Protection strategy**

In the past, many agencies' response to insecurity was to concentrate mainly on protection strategies. These focus on your vulnerability, by removing or limiting your exposure to the various threats

Diplomatic deterrence. This involves lobbying or advocating to international actors, such as the UN and governments, to exert pressure on behalf of agencies. For example, an external government may use its influence over, or threaten sanctions against, local powers that either pose a security threat themselves or fail to promote the agencies' security interests.

1. Armed protection. Although unarmed guards are commonly used at agency facilities around the world, the use of armed guards or escorts is a controversial issue and rarely undertaken by humanitarian agencies, except in extreme circumstances. For example, because of the high risk of kidnapping and hostage-taking in Afghanistan, Somalia, Iraq and Chechnya, some agencies use armed guards to protect their staff.

2. Military deterrence. This is the least common form of deterrence strategy and a difficult issue for many agencies because of inconsistencies with their mandates or concerns regarding the increasing militarisation of humanitarian action. Military deterrence entails humanitarian agencies receiving direct protection from military forces in an attempt to ensure greater security and safer access. An example is when humanitarian agencies travel in convoys that are protected by international peacekeeping forces.

### **Safety and security management plans**

All NIHR Country Offices must develop and maintain a Country Safety and Security Management Plan (SSMP) \* containing information and procedures relating to the security of staff and assets in that particular context. In countries with programme activities in areas for which there are different or additional risks to staff, further location-specific Safety and Security Management Plans may also be needed.

The Country Director is responsible for developing and maintaining the SSMP in conjunction with his/her Safety and Security Focal Point (SSFP), and for ensuring that these plans comply with NIHR Safety and Security Policy and Standards:

1. All SSMPs must be updated at least annually or following significant changes in the operating environment or as a result of a major incident.
2. New country programmes must develop and disseminate an SSMP
3. Within one month of the initial start-up of the country programme.

### **Safety and security management plans**

The Country Director is responsible for developing and maintaining the SSMP in conjunction with his/her Safety and Security Focal Point (SSFP), and for ensuring that these plans comply with NIHR Safety and Security Policy and Standards:

1. All SSMPs must be updated at least annually or following significant changes in the operating environment or as a result of a major incident.
2. New country programmes must develop and disseminate an SSMP
3. Within one month of the initial start-up of the country programme.
4. During a NIHR emergency response, or *after country management decision to respond*, the SSMP must be reviewed and updated (or a new SSMP developed for new programming areas) in



<p>Level 1 (Normal)</p>	<ul style="list-style-type: none"> <li>• Secure situation within the country/area.</li> <li>• No outward signs of significant social disruption or Instability.</li> <li>• Crime is within normal limits and a functioning system Of justice is in place.</li> <li>• Free and unrestricted movement of staff at all times.</li> <li>• No observable threat to NIHR staff.</li> <li>• Programme activities continuing as normal.</li> </ul>
<p>Level 2 (Tense)</p>	<ul style="list-style-type: none"> <li>• Significant political, economic and social unrest is present.</li> <li>• High crime, ineffective police and/or justice systems.</li> <li>• Local animosity/hostility towards UN and NGOs, But not directed at NIHR staff.</li> <li>• Some restrictions on movement of staff in certain Locations.</li> <li>• Programme activities carrying on as normal but with a Need for extra care and diligence.</li> </ul>
<p>Level 3 (Insecure)</p>	<ul style="list-style-type: none"> <li>• Substantial deterioration in the security situation.</li> <li>• General lawlessness, incidents of rioting or looting Reported.</li> <li>• Emergency or martial law declared.</li> <li>• Organised anti-government or terrorist groups Threatening government stability.</li> <li>• Assassinations of prominent leaders/politicians.</li> <li>• Terrorist activities or other violence indicates Foreigners are being targeted.</li> <li>• Localised incidents of fighting between specific groups, Or as a result of military activity.</li> <li>• Staff movement and presence in particular areas, or at Particular times, is restricted.</li> <li>• Programme activities restricted.</li> </ul>

<p>Level 4 (Dangerous)</p>	<ul style="list-style-type: none"> <li>• Widespread civil unrest and indiscriminate violence.</li> <li>• Fighting or military actions close to area of operations.</li> </ul> <p>Children staff.</p> <ul style="list-style-type: none"> <li>• Staff relocated from particular areas, and possible Further relocation of staff.</li> <li>• All staff movements restricted.</li> <li>• Programme activities restricted to essential 'life saving' Activities or suspended.</li> </ul>
<p>Level 5 (Untenable)</p>	<ul style="list-style-type: none"> <li>• Fighting or military actions in the immediate vicinity of Save the Children's offices and residences.</li> <li>• Security deteriorated to such an extent that it is considered unsafe, or impossible, to relocate/evacuate From the area/country.</li> <li>• Staff waiting for an opportunity to relocate/evacuate.</li> <li>• No movement of staff at any time unless as part of a Relocation/evacuation.</li> <li>• Programme activities suspended.</li> </ul>

**Individual**

All NIHR staff members are responsible for their own safety and security and should exercise common sense.

All staff is responsible for the safety and security of their fellow staff, along with Save the Children's assets, under their management and care; and should, when possible, reasonably support the safety and security of implementing partners and beneficiaries.

Irrespective of the organisation's assessment of risks in a particular situation, any staff member may decline to take up work in an insecure area, and has the Right to leave the project or refuse to carry out particular duties if they feel their safety is in danger. In some situations NIHR may require staff to withdraw from an area, suspend operations, or temporarily close an office for security reasons. Such decisions are binding on all staff and should be acted upon with immediate effect. All staff has a personal and professional responsibility to report to the Country Director or their line manager all safety

and security incidents And any behaviour or actions by other staff members that either breach Save the Children's policies or compromise team safety and security in any way.

## **Management**

Each manager has a responsibility for the safety and security of the staff they manage.

The Country Director is ultimately responsible for safety and security management in the Country Office.

At a minimum, the Country Director is responsible for:

1. Establishing and maintaining an effective safety And security management system that is compliant with NIHR Safety and Security Policy and Standards.
2. Monitoring security trends and the safety situation in country and the region in order to determine the appropriate security threat level at all times.
3. Ensuring the Country Office has adequate budget provisions for safety and security-related expenses to maintain safety and security standards.

Each Country Office should appoint at least one Safety and Security Focal Point (SSFP) to support the Country Director and SMT in the implementation

### **Of safety and security management.**

- In higher-risk Country Offices a full-time Security Officer should be employed. Regional/Area Directors are responsible for maintaining oversight of safety and security management within their respective countries and ensuring that Country Offices have the resources And capacity to manage safety and security effectively.
- In the event of any serious incident, either directly or indirectly affecting a NIHR staff member or the team as a whole, the Regional/Area Director and Head Office must be informed immediately. Depending on the nature and severity of the
- Incident, coordination and decision-making may be undertaken at a senior level within Head Office, in consultation with the Country Office and the respective NIHR members.

## **Organisational**

- A. The overall organisational responsibility for staff safety and security lies with the respective Save the Children's Chief Executive.
- B. The respective Director of Global Programmes is responsible for monitoring policy implementation and advising Directors and the Board of Trustees on security matters. Permission to adopt practices that exceed the policy can be granted only by the Chief Executive.
- C. The Global Safety and Security Department (GSS) provides guidance to NIHR management on matters related to safety, security and crisis management,

and supports initiatives designed to enhance the safety and security of personnel and operational activities. The GSS is responsible for:

1. Establishing NIHR policies, procedures and standards that will ensure the highest level of security for NIHR staff and assets and the lowest risk of loss and liability to the organisation.
2. Monitoring existing and potential risks to staff and programmes, and proposing measures to mitigate those risks.
3. Developing and disseminating appropriate and effective security resources.
4. Providing consultative services to Country Office Directors including: training, security assessments and staff support.
5. Enhancing and maintaining NIHR crisis management capabilities.

Further support and advice is provided at the regional level by the Senior Specialists for Regional Safety and Security (SSRSS).

1. Be briefed. Before working in any area, ensure you are fully briefed on the security situation and informed about the mandate and principles of your organisation.
2. Do some research? In addition to the information you will be given
3. By your organisation, it is important to do some independent research. Detailed information on the country, its culture, and political and security situation can be easily found on the Internet, in newspaper articles, and in various books and reports.
4. Speak to others. Try to consult as many and varied people as possible. Talking to your colleagues, other agencies, and individuals in the community is the best way to develop a good awareness and understanding of the situation.
5. Stay alert. Keep your eyes and ears open at all times. Be conscious of what is unusual or threatening. If you notice things are not normal (empty markets or quiet streets that are usually busy), then ask people why. Ultimately, trust your 'gut feelings'; if you feel threatened, leave the area immediately and find somewhere more secure.

In building positive relations it is important to consider the following:

1. Interact as often as possible with your neighbours, communities, local staff, etc. Listen to them.
2. Introduce yourself to and build a rapport with the local authorities and community leaders.
3. Involve yourself in community activities apart from your work. Do not let your only interaction with the local community be when you enter and leave your protected compound. However, be aware of how any interaction you do have is perceived by others, as there may be security implications resulting from the relationships you develop.
4. Attempt to learn the local language and practise it as often as possible.
5. Avoid expressing political or religious opinions with people you do not know well.

6. Avoid being drawn into relationships that might carry personal obligations or expectations you cannot meet.
7. To avoid giving offence or provocation, adhere to the following basic principles in your conduct:
8. Communicate and interact with all individuals in a dignified and positive manner, according them respect as individuals and community members.
9. Be respectful towards the religious beliefs, local customs and cultural practices of the communities in which you work. In situations where staff feel they must question customs and practices that are harmful to individuals, this must be done in a sensitive and appropriate manner.
10. Do not participate in any form of abuse, violence or improper conduct that exploits anyone, especially those over whom you have a duty of professional trust or care.
11. Strive to create an atmosphere of openness and mutual respect with your colleagues. Share information and include others in the decision- making process.
12. Make sure you understand the ground rules in your location for personal communication between men and women; for example, acceptable levels of familiarity and how to greet male and female members of the society.
13. Be aware that in some cultures it is unacceptable for female staff to work closely or travel alone with male colleagues. Consult with colleagues to find an acceptable solution; for example, ensure that two or more female staff travel or work together.
14. Be considerate in your social and domestic behaviour. You may be living and working with colleagues from many different cultural backgrounds. It is important that team security is not jeopardised because of unnecessary or avoidable team conflicts.
15. Make sure your dress indicates respect for the local culture and dress codes. Avoid displaying obvious signs of wealth, such as expensive jewellery.
16. Do not possess or use illegal drugs or controlled substances. Be aware of local laws and attitudes; alcohol may be illegal, or at the very least public drunkenness may be frowned upon. Always refrain from excessive use of alcohol as this can compromise personal and team security.
17. Sexual relationships between team members, or with individuals in the community, may be considered offensive to local laws and customs and could place the individuals

### **Code of conduct**

As an employee or representative of Save the Children, you must Promote its values and principles and protect its reputation by:

1. Respecting the basic rights of others by acting fairly, honestly and tactfully, and by treating people with dignity and respect, and respecting the national law

and local culture, traditions, customs and practices that are in line with UN conventions.

2. Working actively to protect children by complying with Save the
3. Children's child protection policy and procedures.
4. Maintaining high standards of personal and professional conduct.
5. Protecting the safety and wellbeing of yourself and others.
6. Protecting the organisation's assets and resources.
7. Reporting any matter that breaks the standards contained in Save the

### **Children's Code of Conduct.**

Maintaining high standards of personal and professional conduct means you must not behave in a way that breaches the code of conduct, undermines your ability to do your job or is likely to bring NIHR into disrepute. For example, you must not:

1. Engage in sexual relations with anyone under the age of 18, or abuse or exploit a child in any way.
2. Do not demand or accept any personal favours of any kind from contractors or others providing services to your organisation. Always maintain a cordial but professional relationship with others related to your work.
3. Do not misuse the financial or material resources of your organisation.
4. Means of transport, equipment, and residential and office accommodation should be chosen and acquired to meet operational needs only. Ostentatious appearances will reflect negatively on you and your agency
5. Exchange money, employment, goods or services for sexual favours.
6. Drink alcohol or use any other substances in a way that adversely affects your ability to do your job or affects the reputation of
7. The organisation.
8. Be in possession of, nor profit from the sale of, illegal goods or substances.
9. Accept bribes or significant gifts (except small tokens of appreciation from governments, beneficiaries, donors, suppliers or others, which have been offered as a result of your employment.
10. Undertake business for the supply of goods or services to NIHR with family, friends or personal contacts or use NIHR assets for personal benefit.
11. Behave in a way that threatens the security of yourself or others.
12. Use the organisation's computer or other equipment to view, download, create or distribute inappropriate material, such as pornography.

## **When travelling**

When travelling to and from your field locations, consider the following basic precautions:

1. Always check the security situation of the location to which you are travelling.
2. Before travelling, leave your planned itinerary and contact details with a responsible person.
3. Keep people informed of any changes to your travel plans and any delays.
4. Be clear about your arrival arrangements and know who is meeting you.
5. Check in advance with your field office what you should do in the event of a problem, or if there is no one there to meet you.
6. Carry a list of emergency contact details including names, addresses, phone numbers, and the names of reputable hotels along your route.
7. Look confident and dress appropriately, with valuables out of sight.
8. Keep an eye on your possessions, particularly during security checks, in the baggage collection area and while clearing customs.
9. If possible, take only licensed taxis or those recommended by your
10. Field office. In some countries taxi drivers are known to commit crimes or be accomplices. Agree fares before you get in, make sure you have the sole use and the driver will not pick up other passengers, and check that your bags are actually on board before you depart.

## **When driving**

1. When driving in an unfamiliar setting, consider the following basic precautions:
2. Always wear seatbelts and do not drive under the influence of alcohol or other intoxicating substances.
3. Whenever possible avoid travelling at night. If this is not possible, avoid unlit and deserted roads.
4. Keep the car windows closed and the doors locked.
5. Do not drive alone, especially at night, and think about driving in groups or convoys – even for short distances.
6. Be particularly alert when your car is stationary; for example, at a road junction or traffic lights.
7. If you think you are being followed, make a few turns down busy streets to check. If you are, do not go into your own driveway or a deserted area, but drive to somewhere you know you can get help, such as the nearest police station.
8. If someone tries to force you off the road, sound your horn to attract attention.
9. At all times maintain an adequate distance between your car and the vehicle in front, to allow you space to manoeuvre and escape if necessary.

10. Never pick up hitchhikers, and think twice about stopping to help what appears to be a stranded motorist, regardless of gender.
11. More detailed vehicle security measures are discussed in Chapter 6: 'Travel safety and security'.

### **On foot**

In insecure or unfamiliar settings where you are required to walk, consider the following precautions:

- a. Be aware of your surroundings – do not put yourself into a vulnerable position.
- b. Seek reliable advice on safe areas. Do not take short cuts through isolated areas.
- c. Avoid walking alone, especially at night.
- d. Maintain a low profile and avoid any disputes or disturbances. Be wary of groups of people loitering on the streets.
- e. Make sure your bags are closed and securely carried to avoid them being snatched. Valuables should be concealed under clothing or in a front pocket.
- f. Cross the street if someone suspicious is walking behind or ahead of you. If you are still being followed, head to a populated area and attract the attention of others.
- g. Carry only the cash that you need. Keep a small amount of cash in your wallet to hand over in the event of being mugged. The remainder should be divided between your pockets and bag
- h. Avoid carrying your passport unless it is required as identification.
- i. If a driver pulls up to ask for directions, do not approach the vehicle.
- j. Be cautious when asked to look at a map. If you are offered a lift, politely refuse.

### **Using public transport**

If you are using public transport, consider the following precautions:

- a. Travel in pairs whenever possible.
- b. Wait in well-lit designated areas during off-peak hours.
- c. Avoid travelling in deserted trains or buses. If possible, sit near the driver or conductor. When travelling by train try to select a lockable compartment.
- d. Be careful when accepting any food or drink as it may be drugged.
- e. After getting off, check to ensure you are not being followed.



### **In your home or temporary residence**

While in your home or temporary residence, consider the following basic precautions:

1. Be sure to keep your doors and windows locked, even when you are at home or leaving the building for only a few minutes.
2. Keep curtains or blinds closed at night.
3. Avoid sleeping with your windows open unless they are protected by bars or grilles. Keep valuables and possessions away from open windows, even if they are protected by bars, as it is common for items to be 'fished' through openings.
4. Be wary of unexpected visitors, especially after dark. Identify all visitors before opening the door.
5. Carry only the keys that you use, and mark them so you can identify them quickly in the dark.
6. If you find that a door or window of your home has been broken open