Swiss TPH Generic Security Manual

Guidelines on security management while travelling

Version 1.0

17 September 2019

Swiss TPH
Swiss Tropical and Public Health Institute
Schweizerisches Tropen- und Public Health-Institut
Institut Tropical et de Santé Publique Suisse
Associated Institute of the University of Basel

Abbreviations

EISF	European Interagency Security Forum
HSSE	Health, Safety, Security and Environment
ICRC	International Committee of the Red Cross
INSO	International NGO Safety Organisation
NGO	Non-Governmental Organisation
SDC	Swiss Agency for Development and Cooperation
Swiss TPH	Swiss Tropical and Public Health Institute
UN	United Nations
WHO	World Health Organization

Table of Contents

1. Concepts and guiding principles of security management

It is part of Swiss TPH's Health, Safety, Security and Environment (HSSE) and duty of care requirements to ensure that it does everything reasonable and practicable to reduce the risks faced by staff, students and customers – emphasizing preventative risk mitigation whilst ensuring the capacity to respond to safety and security situations appropriately when required.

For Swiss TPH, security management is about protecting and preserving the lives and wellbeing of the Institute's personnel (and possibly partners) – and about protecting the organization's assets, as well as its programs and reputation.

Duty of care is primarily defined under Swiss law within Article 328 of the Swiss Code of Obligations. Under this legal framework, duty of care primarily refers to an employers' obligation to take all necessary and feasible measures to safeguard the health, safety and integrity of their employees.

> *"Within the employment relationship, the employer must acknowledge and safeguard the employee's personality rights, have due regard for his health and ensure that proper moral standards are maintained. In particular, he must ensure that employees are not sexually harassed and that any victim of sexual harassment suffers no further adverse consequences.*
>
> *In order to safeguard the personal safety, health and integrity of his employees he must take all measures that are shown by experience to be necessary, that are feasible using the latest technology and that are appropriate to the particular circumstances of the workplace or the household, provided such measures may equitably be expected of him in the light of each specific employment relationship and the nature of the work."*[1]

The present document serves as a guideline which describes security management processes in place within Swiss TPH in order to improve the safety and security of all employees working outside of our headquarters (i.e., those travelling or based abroad). It describes key processes that Swiss TPH has put in place to assess and mitigate safety and security risks, including measures to prevent manage incidents if they occur.

While these guidelines attempt to establish a shared understanding of safety and security management, define key terms and principles and clarify responsibilities and processes – procedures and guidelines have to be accompanied by the need for good judgment, constant monitoring, routine internal discussion and analysis of the situation.

Safety & Security information are defined in the three following key documents:

- **Swiss TPH security policy:** short document approved by the ILK setting out the Institute's overall approach and principles in relation to security. This document is actually included in the Swiss TPH Code of Conduct document.
- **Generic security manual:** the present document, giving generic security procedures to be applied by all Swiss TPH staff, but not including location-specific procedures.
- **Local security plan:** document giving location-specific security information and procedures that do not feature in the security manual.

1.1 Objective

Swiss TPH's overall approach to security is one of prevention, relying on proactive rather than reactive measures. The aim of this approach is to create the safest operational environment that allows Swiss TPH to fulfil its objectives, while maintaining the safety and well-being of its staff. In order to succeed, this approach requires:

- The implementation of comprehensive security procedures
- Provision of funding necessary to meet staff safety & security needs
- A good security plan drawn up in accordance with the prevailing security situation
- High personal and institutional security awareness and active leadership in security management
- Good external relations, networking and information gathering

[1] Source: *Duty of Care under Swiss law: how to improve your safety and security risk management processes*, EISF 2018. https://www.eisf.eu/library/duty-of-care-under-swiss-law-how-to-improve-your-safety-and-security-risk-management-processes/

- Effective Communication internally (reporting) as well as externally (dissemination)
- Constant monitoring of context and processes
- Effective and rapid response mechanisms in case of incidents and crisis

1.2 Guiding principles

- Primacy of life and personal well-being: In all undertakings of Swiss TPH, safety & security of its staff comes first.

- Prevention: prevention is achieved by creating safety & security awareness, identifying the risks, developing a plan to mitigate them and making sure the plan is implemented. If things go wrong, effective response and reporting mechanisms have to be in place. The plan has to be monitored and improved on a regular basis.

- Acceptance: Risks can be reduced or removed by building a safe operating environment through the consent, approval, and cooperation from individuals, communities and local authorities. Acceptance cannot be assumed. It has to be earned and actively maintained through a useful network and effective communication.

- The right to withdraw: Even though Swiss TPH's employees have to accept a certain amount of risk in order to fulfil the Institute's mission, they have the right to withdraw from a trip or mission if he/she thinks the risks are too high.

- Responsibility to share safety and security information: All employees have an obligation to pass on safety and security related information. Swiss TPH encourages openness because it provides learning opportunities and helps to improve our risk management.

- Relationships with partners: Swiss TPH will act to address security issues related to a partner or consortium relationship. Coordination and mutual support can only be beneficial for incident prevention and response.

- Compliance: Failure by any employee to follow Swiss TPH safety and security guidelines or to obey a safety and security-related instruction is a serious disciplinary matter and may lead to disciplinary action.

1.3 Working as a team

Every member of the team should feel a responsibility for security. Compliance, discipline and mutual support are needed. All staff should be involved in contributing to good security procedures. Managers should build up team spirit, and demonstrate that they care for its safety.

Since security is a dynamic field, and since staff come and go, security updates should be included regularly in staff meetings. Managers should consult the team when they reassess the security situation and when considering any changes to procedures. It may be helpful to delegate some specific security-related functions to one or more team members, while retaining overall oversight and responsibility.

1.4 Risk threshold

When there are known and specific threats towards Swiss TPH staff in certain areas and this threat is considered as credible, Swiss TPH will not allow staff to work in or travel to this area. This also applies to circumstances where the level of generalized violence suggests a high probability of an incident harming Swiss TPH staff. Swiss TPH commits itself to minimizing the risk to staff and therefore will always explore possible alternatives to attain the aims of the operations. If this is not possible, it can reduce or suspend operations if needed.

The line management is responsible to assess the safety & security situation and make the balance between the outcome of a project and the risks to take to achieve them. The Directorate has the overall responsibility and has always to be consulted in extraordinary cases.

The level of acceptable risk can further be identified in the country specific security plans.

- Acceptance by the local communities, authorities and other stakeholders is one of the preconditions to operate.
- Do not accept unnecessary risk.
- Accept risk when benefits clearly outweigh risks.
- Make risk management decisions at the right level and in coordination with partners.
- Everything reasonable should be done to reduce risk.

1.5 Inclusion and diversity

Swiss TPH strives for equality in its safety & security approach. Individuals should not be subject to any discriminatory restrictions. However, Swiss TPH recognizes that individuals may face different risks or be more vulnerable to certain threats because of their nationality, ethnicity, religion, gender identity, sexual orientation, or disability. Under certain circumstances, the prevailing security context or specific risks to an individual, because of their profile, may require Swiss TPH to take additional security measures. For this reason, individuals shall be informed of specific risks they may face and be advised how to minimize risks.

2 Definitions

2.1 Safety & Security

Safety and security describe the two different dimensions of threats that Swiss TPH employees can encounter:

1. **Safety** – protection from dangers which are unintentional in nature (i.e. illness, accidents, natural hazards)
2. **Security** – protection from loss or harm as a result of an intentional act of aggression (i.e. attacks, armed robbery, ambush or kidnapping)

2.2 Threat, risk and vulnerability

These three words are often used to define key concepts in risk management. They are defined and relate to each other's as follows:

- **Threat**: a danger to you, Swiss TPH or your property
- **Vulnerability**: your level of exposure to a particular threat
- **Risk**: the likelihood and impact of encountering a threat

$$\text{Risk} = \text{Threat} \times \text{Vulnerability}$$

You may be unable to influence the level of threat around you, but you can probably reduce your level of vulnerability in two main ways:

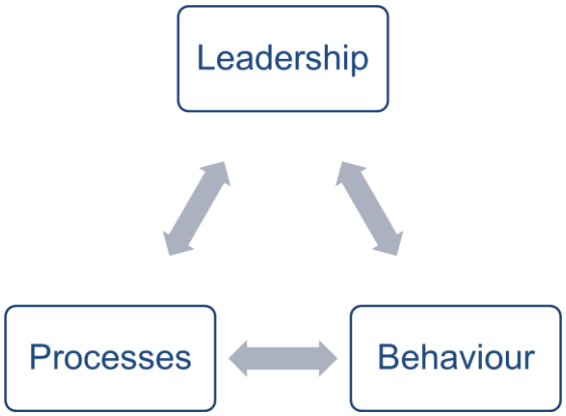
- **Reducing the likelihood of an incident happening** (e.g. by driving slowly, improving locks, or introducing a neighbourhood watch system)
- **Reducing the impact of an incident** (e.g. by wearing seatbelts, or limiting the amount of cash held in the safe)

This is the objective of the risk assessment and analysis: by reducing your vulnerability, you reduce the risk that the threat will become reality and have a serious impact on you. A major part of good security management is reducing vulnerability in every way possible.

2.3 Risk management framework

Policies, processes and tools are never enough to ensure proper safety & security. Time, energy and resources must also be placed on ensuring good safety and security risk management practices are embedded and ingrained in the behaviour of individuals supported by strong leadership.

- **Leadership**: Ownership and responsibility of the implementation of the safety & security management.
- **Behaviour**: Security awareness, compliance with Swiss TPH's processes, rules and regulations and taking into to account local law, customs and realities.
- **Processes**: Tools and procedures have to be in place to support and facilitate the work of Swiss TPH collaborators when operating in risk prone areas and to generate an effective response in case of emergency and crisis



Security management is easier when security is seen as an integral part of an operation – and not as a marginal element. Achieving that, means that the operation has a developed a security culture, where security is automatically considered part of the overall planning and management process and people behave in a manner consistent with established operational standards.

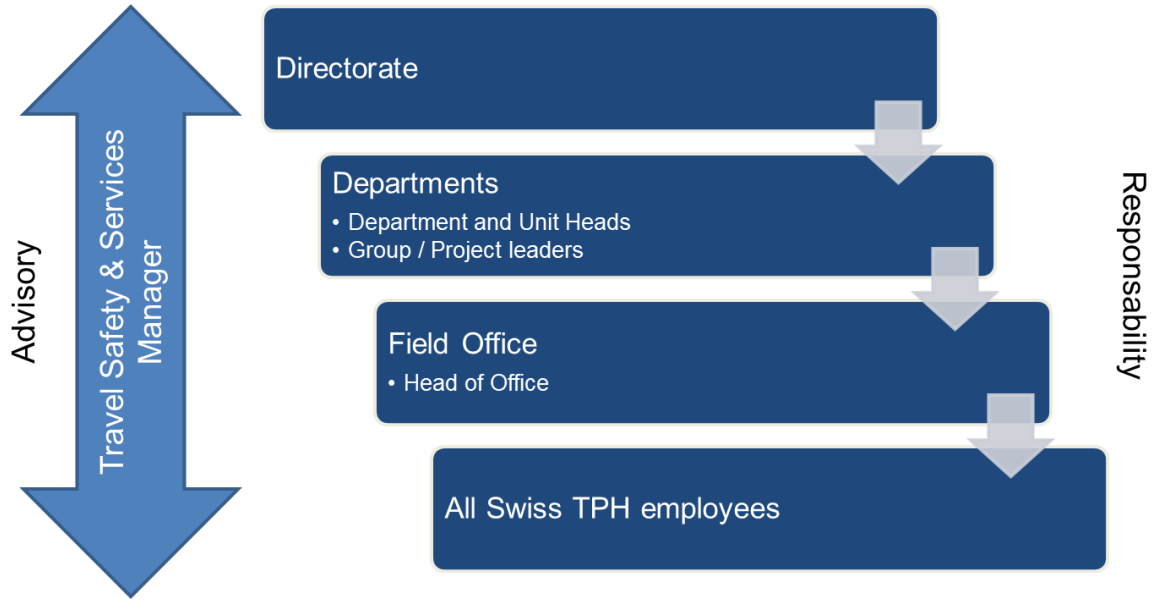
3 Roles and Responsibilities at Swiss TPH

Swiss TPH has adopted an advisory safety & security model. The Travel Safety & Services Manager and Safety & Security focal persons have an advisory and supportive role. The management bears the responsibility of safety & security. Ownership over duty of care, including safety and security risk management, sits within the management line; overall responsibility rested at the Swiss TPH's Directorate.

Safety and security responsibilities are delegated down the management line, with Head of Departments/Unit, Project leaders or country focal persons held responsible for safety and security risk management within their teams. These responsibilities should be reflected in policy and job descriptions.

However, there is a variety of operational setups within Swiss TPH. Not all countries where Swiss TPH is operational has an office or an appointed security focal person. In those cases, the project leader has the responsibility to provide the necessary security management framework for the project to be conducted within a risk threshold acceptable to the Swiss TPH.

Likewise, Swiss TPH works within a consortium of other organisations. It is the duty of the project leader and the local staff to coordinate with the other partners to achieve a safety & security standard, which is satisfactory to Swiss TPH.



Advisory Roles

Levels	Responsibilities
Travel Safety & Services Manager	- Supports and advises the management in implementing, and monitoring compliance of the global security risk management plan. - Oversees safety and security process and responsible for developing and revising general security policy, processes and tools. - Coordinates global crisis management. - Responsible for the treatment of security, risk or threat reports from all staff
Security Focal Point (at regional or country level)	- Supports management in promoting staff security and ensuring staff knowledge of and compliance with security policy and procedures. - Responsible for gathering reliable security information and keeping staff informed and updated on security issues.

Leadership / Implementing roles

Levels	Responsibilities
Directorate	- Strategic direction and high-level oversight on risks for Swiss TPH. - Ultimately responsible for health, safety and security risk management. - Endorses the level of the acceptable risk threshold. - Ensures resourcing of security risk management.
Department and Unit Heads	- Accountable for security risk management within their department and units. - Ensure that safety & security are an integral part of an operation and receives proper resources - Supports the project managers and group/team leaders in implementing the Swiss TPH's security risk management framework and ensuring compliance with the health, safety and security policy.
Group leaders / Project leaders	- Accountable for security risk management within their respective projects. - Ensure the completion of the risk assessment and the local security plan in their respective operations. If needed, coordinates with other project leaders in the same country to finalize these tasks. - Support the Country directors (if in place) in implementing the Swiss TPH's security risk management framework and ensuring compliance with the health, safety and security policy. - Where applicable, appoint a security focal person in the country and define clearly the tasks and responsibilities for the duties (to be included in the job description) - Ensure that safety & security are an integral part of the project and receives proper resources
Local office manager (where present)	- Responsible for security risk management at country level: e.g. monitoring country-level risk, and establishing and maintaining appropriate security plans/arrangements for country-based staff and visitors, responsible for the proper maintenance of the terrestrial vehicles fleet and the proper staff training. - Ensures proper briefings for staff and visitors - Ensures that all security incidents are reported, investigated and learnings implemented. - Sets-up a communication protocol for movements in the field. - Builds up a network of stakeholders to ensure proper acceptance of Swiss TPH activities as well as of supporting partners in case of emergencies.
All Staff	- Responsible for complying with security policy, procedures and directives, and accountable for their own actions.

	- Must understand security context and ensure their behaviour does not increase risk to themselves and/or others. - Responsible for reporting all security incidents, risks or threats using correct channels.

4 Security strategy

Three broad security approaches can shape an organization's security management strategy, namely acceptance, protection and deterrence.

1. An **acceptance approach** attempts to reduce or remove threats by increasing the acceptance (the political and social consent) of an agency's presence and its work in a particular context.
2. A **protection approach** uses protective devices and procedures to reduce one's vulnerability to the threat, but does not affect the threat itself. In security terms, this is called hardening the target. For example: locks, walls, guards
3. A **deterrence approach** aims to deter a threat with a counter-threat. It ranges from legal, economic or political sanctions (not necessarily by aid agencies) to the threat or use of force.

Swiss TPH will exercise a preference for a strategy of acceptance, but in combination with protective measures. The level of protection will depend on the risk level in a country. Deterrence is not suitable to Swiss TPH objectives since it signals a lack of trust that erodes acceptance and is therefore counterproductive.

Different approaches have different resource implications. Acceptance is perhaps the hardest to measure in financial terms, but should not necessarily be considered inexpensive. If actively pursued, acceptance may require considerable staff time and possibly new program initiatives, such as media outreach. Protective devices and materials carry a direct financial cost, while protective procedures (for example imposing curfews or always driving with two cars) can add to the budget by restricting operational capacity.

5 Travel procedures

5.1 Decision to travel

Along with operative and financial aspects, safety & security is a key argument in the decision to travel or not to travel.

It is the responsibility of the traveller and the respective project leader to assess the security situation and to decide if the trip should take place or not. To get up-to-date and accurate information on the security situation of your destination, always consult locally based collaborators or partners.

In case of disagreement on the feasibility of the trip, the line manager (Unit or Department head) takes a decision.

As stated in the guiding principles, the traveller has ultimately a right to withdraw with a valid reason.

5.2 General preconditions

Before any staff can travel for Swiss TPH, he/she should

1. Be in a good health condition and acquire adapted immunization
2. Receive a minimal training in safety & security
3. Obtain enough resources and information to fulfil its operational objectives
4. Fulfil all the administrative duties required

Depending in which context the Swiss TPH staff is operating, the exact procedures can vary.

For Swiss TPH staff with an employment contract from Basel, he/she can consult the Swiss TPH Travel Checklist.

5.3 Briefings and Tandem system

The aim of briefings is to enable staff to understand the local situation sufficiently to live and work safely in it. This includes the cultural and political situation in the country with instructions on what to do and who to contact when something should go wrong. A security briefing should be given to all Swiss TPH staff before they travel to an insecure location.

The extent of the briefing should be proportional to the risk factor of the destination country. For countries with high risk factor, at least two types of briefings have to be conducted for staff based in Basel:

1. A pre-departure briefing
2. A local briefing upon arrival

To cover those needs, Swiss TPH has established a tandem system involving persons who are familiar with the safety & security situation of a particular country. This tandem consists out of

1. A person at Swiss TPH HQ in Basel, the so-called **HQ Focal Point**, who is responsible of the pre-departure briefing. The HQ Focal Point gives a general briefing on the country, institutional framework and useful pre-deployment information.
2. A person at the local office or partner institution, the **Country/Region Focal Point**, who is responsible for a local briefing at arrival of each traveller. The country/Region Focal Point gives a more in-depth presentation of the country's political and social situation as well as its latest developments. The local briefing should cover the risks as well as the measures how to mitigate these risks including how to react in case of an incident and emergency contacts. It should include information about local customs, no-go areas, places where to shop and eat.

Both tandem parties can delegate their duties to another staff if needed. However, they remain the first persons to be contacted by the travellers.

Nationally recruited staff should receive a full security briefing before they start work. In some circumstances, it may be necessary to provide a security briefing to the family members of staff, either directly or through the staff member concerned.

If you are travelling to a place with no Swiss TPH presence, look for assistance of some colleagues at Swiss TPH headquarters who might already been in the region of destination. Likewise, ask partner agencies like SDC, ICRC, UN, Mission21 and possible local contacts for security information.

In addition to the briefing, the traveller has to make his/her own assessment. A starting point can be the travel advice from diplomatic agencies.

1. The Swiss EDA website http://www.eda.admin.ch;
2. French advisory service: https://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs/conseils-par-pays-destination/
3. The UK https://www.gov.uk/foreign-travel-advice which shows more details including a map;
4. Foreign affairs travel advice of your country of nationality official website.

In addition, the traveller should check on google maps where his/her destination points (offices, hotel and airport) are located in order to gain some information about the travelling routes and write down their addresses and landmarks nearby.

A list of country responsible can be found on the intranet (https://intranet.swisstph.ch/de/aoc/health-safety-and-security/swiss-tph-travel-safety-security-concept/). If you are not connected to the intranet please refer to your line manager for the list.

5.4 Contacts and Emergency contacts

Travellers based at Swiss TPH headquarters have carry their emergency card at all times.

Each Swiss TPH office or project in the field should create their own emergency card and make it available to all staff and guests. Important contacts should at least include numbers of Swiss TPH key staff and office, partners and emergency services (fire, medical, police).

Each traveller should prepare its own personal list of important contact numbers to be prepared for all eventualities. For example: what if nobody came to pick me up at the airport? Who should I call if I feel unwell in my hotel room? Who should I call in case of a traffic accident? And don't forget the phone number of your embassy.

For some contacts, an assessment has to be done for medical facilities. For others, networking and coordination are needed, for example, if partners are ready to support us in case of emergency. This work has to be done by the local Swiss TPH team.

Contact in priority:

1. Local assistance (Swiss TPH local office or partners, if available)
2. Line Manager / your contact person at Swiss TPH
3. Swiss TPH 24/7 hotline

5.5 Communication protocol

Every trip needs a communication protocol in place.

A communication protocol defines to who and how often you report your safety status. The aim being, if the traveller fails at reporting, an emergency response is activated.

As each Swiss TPH trip is different from another, there is no standard communication schedule. It has to be defined with your focal person. It might vary from every 1 hour in high volatile areas to once a day or week in safer zones.

The communication methods can vary according to the means available: mobile data, SMS, phone, VHF radio or GPS tracking system.

5.6 Debriefings

Debriefings are to be conducted after each mission and can take place locally and/or at the headquarters upon return under the responsibility of the country focal persons or security managers.

Important information to collect is for example:

- Safety & Security threats or/and experiences
- Logistics and advises for routes, hotels, restaurants, places to stop, etc.
- How the whole process was experienced
- Any suggestions to improve
- Well-being

Any useful information should be documented. The traveller can write a short report or the person conducting the debriefing can put in written the content discussed.

In case of an incident, the debriefing of the staff involved should be done immediately or as soon as the persons involved are able to report on it. For any difficult or traumatic experience please refer to the chapter on Health below.

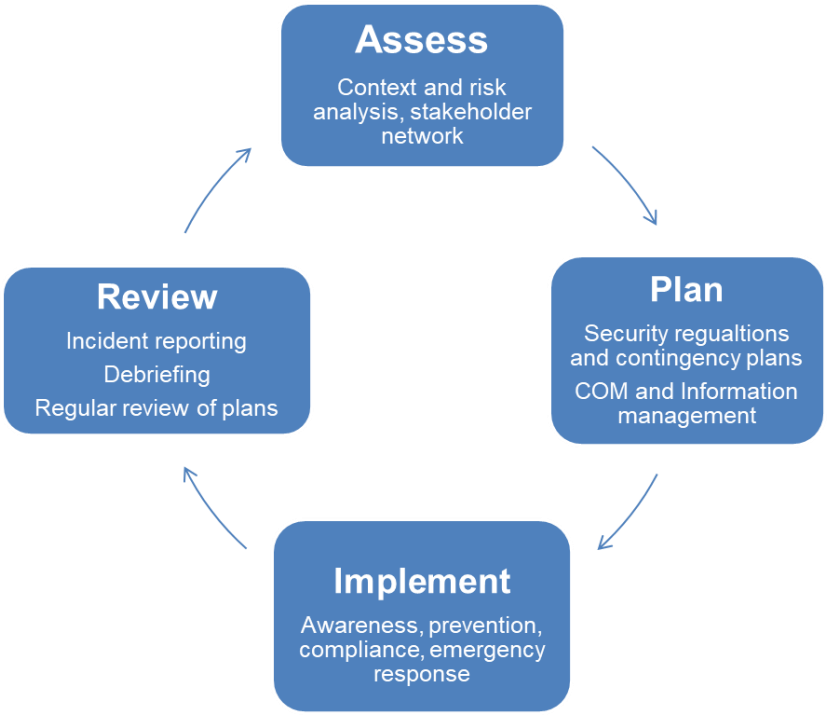
6 Safety & Security management in the field

Due to the wide range of Swiss TPH projects and activities, there are no standard setup of the Institute worldwide. Nevertheless, despite the diversity of the field deployments, there is a minimum safety & security standard to be respected.

Security management is influenced by the situation within which Swiss TPH operates. These influences can be both internal and external, and can affect all aspects of the management process. Managers must understand these influences and determine what impact they may have on decision-making and the management process.

Security strategies are expressed through each delegation’s individual security plan. A security plan consists of a number of components, typically including:

- Risk assessment
- Security strategies
- Security regulations
- Contingency plans
- Security guidelines and advice
- Security briefings and debriefings
- Critical incident management plan



6.1 Risk assessment and analysis

The risk assessment involves the logical analysis of the situation to identify the potential threats and Swiss TPH (and its project partners) vulnerability to those threats.

Once a threat and vulnerability analysis has been completed, the impact of the threat and the probability of it affecting the Institute are plotted on a risk matrix. The risk matrix enables risks to be prioritized, while actions are identified to mitigate them.

These actions are used to form key components of the security plan.

Swiss TPH has a tool to conduct a risk assessment and evaluate the risk level depending on the probability and the impact of the threat. For more information and instructions how to use it, please refer to the risk assessment and analysis tool annexed to this document (ANNEX 1).

During the risk assessment, it is important to keep in mind

- Environment which the team operates
- The type of activities
- The profile of the team members

The risk assessment should be updated every year and more often if necessary depending on the security environment.

A threat and vulnerability assessment can be conducted in different ways, but they all should answer the following questions:

- Why? could an attack happen (crime, political reasons, ransom, revenge)
- Who? poses the threat (criminals, army, armed factions, dissatisfied workers, beneficiaries)
- What? are the likely targets (expatriate staff, visitors, family members or local staff)
- How? could an attack happen (weapons, ambush, bombs, robbery, hostage taking)
- Where? are we most vulnerable and where are the likely locations for any attacks
- When? could an attack happen and when does the possibility of an attack increase

6.2 Local security plan

The aim of a security plan is to provide staff with an easy-to-use reference document, covering all common security advice, procedures and rules. A security plan is no substitute for training.

Based on the results of the risk assessment, a local security plan has to be developed for each country, region or office depending on the complexity of the context.

The responsibility of the local security plan relies on the project leader. The document has to be drafted together with the country or office responsible and the whole team. In countries where Swiss TPH works in a consortium with other partners, the security plan should be aligned with those of the institutions.

A security plan is an essential tool for developing and maintaining adequate security procedures and responses. The first phase of security planning is to identify the main risks (see chapter above) and determine which strategy (acceptance, protection and deterrence) can be utilized to minimize them. Not all the risks can be covered, therefore a list of priority risks has to be made. The plan must relate to the specific operational situation and will comprise a number of components including security regulations and guidelines; briefing and debriefing procedures; contingency planning; critical incident management. Formulation of the security plan should be conducted using input from all personnel within the team.

The local plan should include very precise and practical information on how to prevent an incident to happen and how to respond if an incident happens nonetheless. It is specific to a country or region and should not be more than 25 pages.

A template of the contents of such a local plan is available as annex to this document (ANNEX 2).

Security regulations should cover the following areas:

- Situation/threat assessment
- General conduct/behaviour
- Field movement control
- Driving regulations
- Communications/radio
- Incident reporting
- Contingency planning
- Medical procedures
- Office and site security
- Annexes (contact lists, map, relocation plan, etc.)

The local security plan should be updated at least once every year or if an important change in the context occurs (military putsch, outbreak of disease, etc.).

6.3 Contingency plan

Contingency planning should always be undertaken when there is an indication that there is a high risk or probability that a disaster or emergency situation will occur. These situations will be identified through the threat, vulnerability and risk assessment that must be undertaken at the start of any planning process.

Contingency planning is designed to ensure organizational readiness in anticipation of an emergency and to enable Swiss TPH office to react effectively in such a situation. For managers, this readiness includes plans for the management of people, finances, emergency supplies, communications, etc.

Plans should be based on specific events or known risks at local, national, regional or even global level (e.g., natural hazards, political crisis, population unrests or potential epidemics). At a minimum, the standard type of contingency plan to be developed in your country should include relocation and medical evacuation plans.

Regardless of the scale, there is a clearly defined process for developing a contingency plan. The steps you need to take when formulating contingency plans are to:

- Analyse the current situation by conducting a threat, vulnerability and risk analysis
- Identify high-risk scenarios (in some cases, these will be pre-defined)
- Determine options to address the situation created by the scenario

- Seek advice and direction from regional or global resources
- Formulate program scenarios
- Select the best option for the context
- Identify activities related to the option chosen in terms of:
    - Personnel – identify any required adjustments or specific skill requirements
    - Logistics – ensure readiness of specialist equipment, emergency supplies/stocks
    - Transport capacities
    - Communications equipment and procedures
    - Security – personnel, finance, logistics
- Coordination details (routes, key locations such as assembly points, timing, etc.)
- Assign roles
- Draft the plan

The contingency plan can take various form depending on the context. It can be integrated in the local security plan or it can be kept as a separate document. In some contexts it could be a confidential document.

Since a contingency plan is a response to an emergency, it is vital to coordinate this response with the other stakeholders Swiss TPH works with and align the plan with them.

6.3.1 Operational security phases

A four-color system of alert phases is often used by different organizations to standardize the terminology referring to operational phases used worldwide. The four phases in this system are:

Phases	Description of the situation	Recommendations/actions
White phase	Ideal working conditions, no limitations to operations.	No major security concerns, normal security regulations apply.
Yellow phase	Situation of heightened tension and security concern. Working conditions allow programs to continue, although there are some security concerns; a situation of heightened security awareness is initiated.	Heightened security awareness Initiated. Normal security regulations apply but with a heightened sense of security.
Orange phase	Emergency situation Working conditions do not allow proper access to project sites and beneficiaries; need to reduce number of staff and activities; tight security management is required.	Restriction of movement as well as reduction of activities and the number of staff.
Red phase	Security conditions do not allow work to be carried out; presence of staff is a liability and their relocation is necessary.	Conditions do not allow work. Risk to Swiss TPH is extreme. Relocation or hibernation is initiated.

Associated with these phases, the following actions could be taken to ensure the safety & security of Swiss TPH staff:

Suspension: Suspending program activities may be necessary simply to avoid a threat, which has recently emerged. It may be necessary in order to allow time for reflection on a changed security situation.

Hibernation: A longer period of suspension, where relocation is impossible or perceived too dangerous to undertake. The staff remains at home or in a safe place for a considerable time in order to allow danger to subside. Ensure that sufficient resources are available for the duration of the hibernation period.

Relocation or reduction of staff: An alternative to suspension or hibernation is to relocate staff to a safer location, within the same country or across an international border. After relocation, Swiss TPH may decide to continue some operations from the safer site. A further alternative is to reduce the numbers of staff working, to reduce risk.

Evacuation: It is the physical withdrawal of staff from a crisis spot, usually across an international border and the complete closure of office and suspension of the program. The physical withdrawal might include as well the staff's eligible dependents, family members, spouses and authorized visitors and assets. The decision to evacuate should not be taken lightly, since its consequences can be far-reaching and may include:

- Misunderstanding by local people
- Termination of employment for some staff
- Security situation and evacuation of local staff, what is possible?
- Loss of property if looting or theft follows evacuation
- Difficulty in re-establishing a program in the future

A more detailed description of deployment strategies according to emergency levels can be found in the ANNEX 4.

6.4 Implementation of the security plan

Implementation of the security plan and management of security is, perhaps, the most difficult part of the process. A key part of this process includes personnel being aware of all aspects of the plan as well as their roles and responsibilities within it.

Routine management involves ensuring personnel operate within the framework of the plan. However, managers must also be able to deal with incidents and areas that can occur outside the routine. These aspects of the process are made easier thanks to contingency planning and established incident management procedures like stated above.

6.5 Review

Local security plans must be monitored and continually evaluated to ensure their relevancy. This should occur as a matter of routine at least every year, but also whenever there is a change in the situation on which the plan was based, or if the analysis of security incidents highlights any gaps in the plan. To enable this process to occur, it is vital that managers ensure constant monitoring of the situation and are aware of any changes to their environment.

6.6 Information management and communication

6.6.1 Collecting information

Good information management is vital in any project, whether or not the area concerned is at high risk. During times of heightened security, the efficient gathering, processing and distribution of information will be critical to ensure the wellbeing and safety of the staff.

Basic activities that will contribute to beneficial information management with regard to security include:

- Regular external liaison with partners and other main actors in the context like the SDC, UN, ICRC, MSF, non-governmental organizations, embassies and other institutions working in the country/region
- Attending security meetings that are being held in the area of operation, and, if possible, obtaining regular security situation reports or operational updates
- Regular information-sharing and action coordination meetings with partners
- Obtaining information and news via other means (e.g., private and professional network, the internet, local news, trusted sources in the social media, etc.)

6.6.2 Communicating to external stakeholders

Each project or office has to make sure all staff is able to present Swiss TPH and its activity is an accurate but efficient manner with simple words and without professional jargon. The message should be adapted to the interlocutor.

If you are requested to give information by the press, direct the person to the person appointed to speak to the press. If you have no choice, speak about what Swiss TPH does and avoid giving sensitive information, talk about

6.6.3 Social media

In the past few years, the role of social media and digital technologies in operational context has grown exponentially. It is a precious source of information but also a quick vehicle for fake news and rumours that can be detrimental to the security of the staff.

Therefore:

- If you use public social media channels, use it for private purposes only
- Avoid at any time to state any opinions that might harm your security and the one of Swiss TPH, for example political, religious or any other controversial subjects.
- If a team wants to use any Swiss TPH channel in social media, it has to be done with the authorization and supervision of the communication department at the Swiss TPH headquarters.
- For collecting information, Twitter or Facebook can be extremely valuable source of information if you know your sources well and if you can trust them. Identifying some good organizations, journalists or influential persons that are serious can provide a lot of local immediate information in case of incidents.

6.7 Management of visiting staff and guests

It may be unreasonable to expect that staff visiting the operation for a short period become fully aware of everything in the security plan. In these cases, consideration should be given to producing a briefing or welcome pack that provides an overview of the key elements of the security plan that each visitor should be aware of. This might include:

- Short summary of the in-country situation
- Principal threats and risks in the area
- Key regulations, noting especially any curfews, restricted areas, field movement control procedures, communications requirements, etc.
- Key actions to undertake in emergency situations
- Key contact numbers for delegation personnel and emergency services

Visa information is important for all visitors. Each office has to be informed about the visa regulations for its country. What kind of visa allows a visit, which one allows to work? What are the procedures to obtain the visa? This information has to be forwarded to the Swiss TPH headquarters. Immigration authorities should be part of the basic network of stakeholders to be contacted by the Swiss TPH office.

6.8 Vehicles

For additional information on how to manage vehicles, please consult the *Administration Manual for Local Offices* (chapter 4.4 Vehicle Maintenance and Equipment).

6.8.1 Swiss TPH and project vehicles

All vehicles must be appropriately registered, insured, well maintained and suitable for the country, trip specific and seasonal road conditions. The vehicles can only be operated by authorized and insured persons with a valid driver's license, and under conditions that comply with the local legislation.

Non-national staff should always use local drivers, and should avoid driving vehicles themselves.

Driving motorbikes for non-national staff is not allowed, exceptions have to be authorized by the project leader. The use of a helmet is compulsory regardless of the country and legislation.

A Swiss TPH employee in the country should be contractually designated as responsible for proper maintenance of terrestrial vehicles fleet and proper training for Swiss TPH drivers. Drivers should be recruited according to a strict set of criteria and be permanently reassessed.

6.8.2 Rental vehicles

Rental vehicles are to correspond to the same legal, safety and security standards that apply to Swiss TPH owned vehicles. The country and/or regional hub office are responsible to ensure that the rental vehicles and operator have adequate insurance coverage.

6.8.3 Safe driving

Vehicles must be driven safely. The person operating a vehicle for Swiss TPH must recognize the limits of the vehicle, the risks the environment poses, and adjust the driving accordingly. Vehicles must be able to stop quickly and safely in an emergency, and therefore must be driven at a speed at which the vehicle is stable, which may be lower than the allowed speeding limit. Passengers in the vehicle are also responsible for their own safety and must express and highlight their concern, when the vehicle operator is not driving safely. The wearing of seatbelts is compulsory. Vehicle doors (including luggage or cargo doors) should be locked while driving.

Driving in a drunken condition and/or under the influence of stupefying substances is completely prohibited, regardless of what existing legislation in the concerned country may stipulate.

A first aid kit is compulsory in all cars. An extra first aid kit should always be ready in case a rental car doesn't have one. The driver has to check if the first aid kit is complete prior to each trip.

6.9 Field movement

Field movement presents one of the greatest risks to security in the field. Field travel does not have to be solely work-related travel. It includes any travel away from the office, residence or other work-related premises that could be defined as your home base. Travel within urban areas does not generally constitute field travel, although in insecure environments or during times of heightened awareness such movement may be subject to movement notification procedures.

The preparation of field trips will vary from one office to another depending on the nature of operations, the risk assessment of the operational area, road and environmental conditions and the distance between your home base and the field location. However, all Swiss TPH field movement procedures require some common considerations be taken into account when you are planning and/or conducting field trips.

Driving at nightfall outside urban areas is forbidden. Exceptions should be discussed and defined with the local and headquarters' management. Emergency movements during the night have to be communicated to the local security focal person or head of office.

6.9.1 Planning for field trips

Any field movements undertaken should be well planned and organized in order to keep the risk level at a minimum.

This includes:

- Knowing the exact route you will travel possible locations for an overnight stay
- The weather conditions
- Security information – understand the local situation including potential threats, local road conditions, the presence of checkpoints and other organizations operating in the area
- Being aware of your surroundings during any field movements; listen to the driver, local staff and the local population and, if there is any doubt about the safety of the trip, it should be terminated or postponed
- Field movements and any vehicle travel should correspond to an operational goal and, wherever possible, Swiss TPH staff should join up with other Swiss TPH staff visiting the same area.
- Is the vehicle roadworthy, do you have adequate supplies, communications equipment, updated first aid kit, and all relevant documents? Do you know how to use the communications equipment issued to you?
- Check and ensure that the vehicle to be used is mechanically sound and fully roadworthy.
- Fuel (including few spare litres), oil, water, tires (including functional spare tyre), etc., should be checked before departure.
- Communication equipment should be tested, battery charged and the driver and responsible staff must be fully familiar with the operation of the radio systems and radio procedures.

If deemed necessary due to security risks, a two-vehicles should be introduced and the vehicles should be within sight of each other at all times.

Be sure to have road maps, food and an adequate supply of drinking water with you, in addition to the basic equipment that must be in the vehicle as discussed in the previous chapter.

All travelling Swiss TPH staff should check to ensure they have the relevant papers or copies of mission orders, driving licenses, passports, identification cards, etc., with them.

All vehicle travel – whether private or work-related – must conform to any restrictions that may be in place.

The local office manager should always be informed about and give prior approval to any movement of Swiss TPH staff within the country of assignment.

6.9.2 Contingency planning

- If mechanical problems disable one vehicle, contact must be made with the base and approval obtained for any proposed course of action.
- If a field team does not return at a prearranged time and no communication with them is possible, then contingency plans must be in place on how to deal with such emergencies.
- Staff should also be fully familiar with emergency procedures, how to behave at checkpoints in cases of ambush and in areas that are mined.
- All Swiss TPH vehicles used for field movements should be within a safe area or back at the operational base at least one hour before nightfall. This deadline gives one hour of emergency preparation – should there be a need – before darkness falls. For longer field movements, this means you must plan your travel more precisely and, if necessary, add a day to the trip in order to abide by the security regulations.
- If an overnight stay is required, then details of the locations where you will be staying, contact points and contact schedules should be included in the mission order, or communicated to the local office manager prior to departure.

6.9.3 During field trips

All field movements should be authorized and monitored for their duration to ensure the security of Swiss TPH staff. This is only possible if there is full compliance with procedures, the most common of which are outlined below:

- Authorization of the trip by office head
- Clear identification of passengers, driver, destination and communication protocol
- Mission order in written form
- The communication protocol should mention the frequency or exact locations where a contact with the basis will be made

In some contexts, the information on exact movements should not be given to external stakeholders. Untrusted persons could use this information to setup up an attack on the vehicles. So due to the diversity of the contexts, please discuss these issues with the line management locally and at the headquarters to setup a safe procedure for communication.

6.9.4 Monitoring during trip

As all field vehicle movement must be monitored, the personnel travelling should make regular contact with the base using agreed and, if necessary, coded call signs and contact points.

- Any changes in routing, destination or timing of return must be announced to the delegation and approval must be given.
- Confirm arrival at your destination.
- Report when departing for home base.
- Confirm safe arrival at home base.
- On arrival at an overnight location, contact must be made with the base to confirm your safe arrival at the destination.

6.10 Incident reporting

Reporting and analysis of incidents, threats or risks is crucial for follow up as well as organizational learning when it comes to security management.

Every member of staff has the obligation to report any situation that challenged the safety and security of staff. This includes near-misses or developments in the context that in the future might affect the security situation. Every situation that qualifies as above must be reported through the agreed incident reporting channels.

All incidents have to be reported using the attached incident reporting form (ANNEX 7). This report should be addressed to the next line manager with a copy to the Safety & Security Officer for information and statistics. For every incident where action is still pending, a clear plan of action has to be established and communicated (with roles and responsibilities) in order to avoid duplication or uncoordinated efforts.

6.11 Incident management and analysis

For each incident it is important to respond in a proportional way. There are mostly 3 different levels:

1. Incident management: the incident doesn't present any live saving measures and has no broader impact on Swiss TPH operations or reputation. It can be managed with internal resources and procedures.

2. Emergency management: Emergencies require immediate action, often live saving or with serious potential impact on the Swiss TPH structures and operations. The usual action would be to notify, to call the emergency services or to transfer the person to a medical structure.

3. Crisis management: the incident can be or develop itself into a crisis whenever Swiss TPH operations, reputation and/or existence are at stake. Coordination of a crisis is conducted by the headquarters.

For each crisis, a Crisis Management Team (CMT) is put in place. The CMT is the central crisis coordination platform for Swiss TPH. The composition and role of the CMT differs according to the type of crisis. The role of the CMT is to mitigate the impact of an incident and ensure the operational continuity. For more details please refer to the document *Incident, emergency and crisis management at Swiss TPH*.

After an incident, managers should think through the events and consider whether there are any lessons to learn. For example, should staff be better briefed? Should procedures be adjusted? Should a

particular route be avoided? Should there be better liaison with the police? Should disciplinary action be taken against any member of staff?

Managers should consult relevant staff when considering lessons from an incident, to ensure that all possible lessons are identified and that staff support the conclusions reached.

Records of all security incidents should be kept and analysed from time to time. In most countries there are security coordination meetings organized by the UN or INSO, which are an excellent source of information and a networking opportunity.

7 Telecommunication systems

The main role of a telecommunications system is for operational and security purposes, such as transmitting work-related information, to report on security incidents or to obtain information about a potentially risky situation.

- An appropriate system based on operational needs and terrain
- Training of staff on the communications equipment issued to them and on the telecommunications procedures
- Having a redundancy (back-up) system in place

Mobile phones

In today's operations, the most commonly used communication equipment is the mobile telephone. Although most persons are very familiar with them, there are some considerations that need to be born in mind:

- Mobile telephone infrastructure, such as relay stations and antennas, are vulnerable to damage caused by natural disasters and conflicts
- Mobile services can be switched off by political or military decision
- In some areas it is worth to have a backup communication plan
- In some countries the prepaid plan is still popular so it is important to check that every staff has enough credit on his/her phone

Satellite communications

There are many different types of satellite communications equipment on the market, but the most commonly used by include Thuraya satellite phones, Mini-M satellite phones, Broadband Global Area Network (BGAN) and Global Positioning System (GPS). Make sure you have credits to call.

The advantage of the satellite communication is that the system is less dependent on the national network and disturbances. On the other hand:

- It is expensive
- It needs to be used outdoors for coverage
- Attractive for thieves and are easy to misplace
- The satellite service providers for each system (Nera, Iridium and Inmarsat) can turn off the connection so no signal can be reached in your area. This is not common, but governments can request that the provider blocks out signals in certain areas within their country because of military activity or visits by very important people (dignitaries, high-ranking government officials, diplomats, etc.) to your area.

HF and VHF radio

Using frequencies in the range of 3 to 30MHz, High Frequency (HF) can offer reliable communications over thousands of kilometres with independent and limited infrastructure. Although its usage has declined with the emergence of new terrestrial technology such as GSM networks, it is still considered as last resort communication and equips most vehicles and offices in countries where staff security is considered as a priority. The possibility to reach any humanitarian vehicle, no matter the location in a country and without any infrastructure (other than in the office and vehicle) remains HF's greatest asset.

It can also be used for operational voice communications, SMS type text messaging, GPS tracking and communications with aircrafts.

Very High Frequency (VHF) and Ultra High Frequency (UHF) bands cover the range of 30 - 300MHz and 300 - 3000 MHz, respectively. Within these ranges, commercial two - way radio operate in 146 - 174MHz (VHF) and 403 - 470MHz (UHF). VHF and UHF communications are primarily used for local communications related to security and/or for operations. Typically UN agencies (and often NGOs) share a common infrastructure (network of repeaters; common channels) and radio - rooms, where operators make the daily or weekly security checks and monitor all vehicle movements.

Global Positioning System (GPS) tracking

GPS uses a satellite global positioning device that can receive signals from a number of orbiting satellites, allowing the user to determine, among other things, the receiver's exact location, speed, elevation and direction.

All these communication systems can be used in Swiss TPH deployments. Each project or office has to determine its needs and allocate enough funding to purchase the most adapted option. The legislation on the use of satellite phone or radio communications varies from country to country. In some countries, it has usage or commercial restrictions; in others, it is even forbidden. It is therefore important to consult these regulations before making a decision.

8 Health

Basic health and hygiene precautions greatly reduce the chances of illness. All staff should be briefed on these, and managers should check, as appropriate, that staff are taking the precautions.

The most likely health issues one could encounter while travelling are the following:

- Cumulative stress
- Food and water-borne diseases
- Insect and vector-borne diseases
- Exacerbation of chronic diseases
- Accidents
- Injuries
- Risky behaviour
- Sexually transmitted diseases, including HIV
- Excessive smoking, excessive alcohol consumption and other substance abuse

More information you can find in the document *Stay healthy while travelling*. Contact a Swiss TPH doctor if you have individual needs and questions (appointments at +41 61 284 82 55).

It is good practice for staff to carry in their purse or wallet a record of basic medical data and any special medical requirements they may have, including blood group, allergies (e.g. to antibiotics), any existing disorders or medication currently being taken.

The Swiss TPH emergency hotline (on the emergency card) is a medical helpline as well. If you need any medical opinion during your trip, you can call +41 61 284 81 44.

8.1 First aid

The Head of local office, or if not available the Project Leader, has to make sure that first aid equipment is present in every office and car. The driver has to make sure that the first aid kit is always complete. A list of items that are recommended can be found in the attached ANNEX 11.

Attending first aid training is highly recommended, especially in areas where emergency services are non-existent. Once a year Swiss TPH organizes a training session for first aid in remote areas, please contact the travel safety manager for more information.

8.2 Medical emergencies

All staff should be aware of which local medical facilities are recommended, and which should be avoided. This implies that the Head of office, or in his/her absence the Project Leader, should check the quality of local facilities. The address and number of these identified medical structures should be distributed to the staff and visitors (ideally in form of an emergency card together with other vital and important numbers).

For all staff and visitors check that appropriate medical insurance is in place.

Further recommendations for prevention and response to medical emergencies can be found in Chapter 10.3.

8.3 Medical evacuation (Medevac)

If a staff member is injured or ill and local medical facilities cannot provide sufficient treatment, medical evacuation may be needed. This happens in a coordinated decision between the local doctor, the Swiss TPH doctor and the insurance company.

Swiss TPH has a travel insurance that covers the costs of Medevac for staff travelling abroad, this includes staff based in Basel who are travelling outside Switzerland as well as staff based in another country and on mission in a third county. However, it does not cover local staff operating in their own country. It is vital that all relevant staff know the procedure for making use of these, especially the insurance name, emergency and policy number (all on the emergency card).

8.4 Stress

Staff should be aware of the dangers of excessive or prolonged stress, and watch for signs of it in their colleagues. People suffering from stress are likely to manage their security less well, increasing the risks for themselves and their colleagues. Managers should aim to prevent excessive stress, and to spot early on when a colleague is suffering from it. Likewise, they should set up work and living arrangements in such a way as to minimize stress and its effects.

Be aware of the need to monitor your own stress levels and be prepared to acknowledge and do something about excessive stress. This is not only important for you but also your colleagues who may be relying upon you to perform well.

Different types of staff may show different signs of stress, because of cultural or personality differences. Their families may also be affected.

8.5 Trauma

In case of any incident that leads to a trauma, there is a neutral care team at the Swiss TPH headquarters that offers a first (confidential) session to debrief such incidents. To make use of this service the Travel Safety & Services Manager cam be contacted (+41 61 284 83 47)

Managers should note any signs of stress among staff, bearing in mind the possibility of Post-Traumatic Stress Disorder (PTSD) or other stress-related illness. If stress-related illness is suspected, professional advice should be sought – a stress debriefing conducted by someone who is not properly trained may do more harm than good.

Therefore, if the result of a first discussion is the need for psychological services, the employee has the possibility to be referred to an external psychological professional.

9 Administrative issues

For general Guidelines on how to manage a local office, please refer to the Swiss TPH's *Administration Manual for Local Offices*.

9.1 Premises

Before deciding to use a building, it should be assessed for its security. Security at an office, warehouse or other building is made up of a number of factors including:

1. **General location**
- Vulnerability to crime,
- Vulnerability to natural disaster (for example, floods),
- Good access to airport, to evacuation routes in case of emergencies
- Accessible to beneficiaries or partners
- Profile of neighbours that can pose a direct or indirect safety (fuel storage) and security threat (sensitive embassy or authority generating demonstrations)

2. **Physical security of the building**
- Walls (height and quality),
- Windows (secured), doors, locks
- Fire escape
- Quality of the construction (earthquake)
- Lights

3. **Local infrastructure**
- State of the roads leading to the building
- Power and water supply
- Shops, restaurant

4. **Arrangements for receiving visitors**
- Park space
- Place for guards and security checking

5. **Identity of the owner**
- Reputation
- Connections

9.2 Managing keys

Good locks are not effective unless keys are managed properly. All keys should be accounted for, with staff signing for receipt of each key. If a key is lost, locks should be changed.

9.3 Identity badges

It is good practice to provide photo identification cards for all staff. They should clearly show an expiry date: this prevents former staff from continuing to use the badge, and limits the damage if a badge is lost or stolen.

9.4 Financial security

Fraud, theft or mismanagement involves sometimes large sums of money. These problems can be greatly reduced by insisting on sound financial procedures from the start. The procedures should be simple, and designed so as not to impose delay on operational programs. If they do cause delay, the

employees are more likely to ignore them. Guidance can be found in the Swiss TPH's *Administration Manual for Local Offices*.

A critical requirement is to ensure that a properly trained and briefed bookkeeper, accountant or financial manager, appropriate to the size and type of program, is present from the start, including during the planning of the operation.

9.5 Information security

Information security is ensuring that important information is not lost, and that confidential information remains confidential.

Filing system: An efficient filing system is essential. Without it, information will be lost, and will require considerable time and effort to find or re-create.

Security of files: Files should be kept in rooms not accessible to the public. Sensitive or confidential files should be clearly marked as such, and kept in unmarked, locked filing cabinets.

Backing up files: Any files whose loss would be costly or damaging should be copied ("backed up"), and the copies kept at a different location from the originals. It may be necessary to send the copies to HQ for safekeeping. Such files might include financial information, personnel files, and any files which will be required for reports to donors.

Files for evacuation: If evacuation is a possibility, a list should be made of the files which should be taken with the team when evacuating. In this way, the necessary files can be gathered quickly when the evacuation is decided on. Such files may include personnel files, financial files and inventories of equipment or stock, for example.

It is wise to prepare a draft authorization document (see annex for a sample), which can be rapidly signed in the event of evacuation, giving authority to a staff member to represent the organization and to manage its emergency operations.

Note that it may be dangerous to take certain types of information with the team when evacuating, as the team may be searched when attempting to leave the area.

Computer security: Information held on a computer is vulnerable to damage and theft, even if passwords are used. Files remain on computer disks and can be read, even once they appear to have been deleted. Disk corruption, viruses and other types of computer attack can damage or remove information.

Managers should ensure that all staff using computers regularly back up important information held on computers. Back-up disks/keys should be held in a different location. All computers should if possible be locked to a fixed point, to make theft more difficult.

Telephone and e-mail security: All telephone or email conversations can be listened to or read by others, even if encryption is used. There is no such thing as a totally secure encryption system. That said, some encryption systems are very good, so that it would require a highly trained specialist, and considerable time, to decode a message.

The simple way to avoid giving away sensitive or confidential information is not to send it. It is often possible to take the information in person, and communicate it directly to the person who needs to know it.

It may sometimes be unavoidable to send sensitive or confidential information. In these cases, be aware of the risks (to you and others, including local people) and weigh them against the benefits.

9.6 Archiving documents after programme closure

All security-related documents and reports should be archived properly (*see Administration Manual for Local Offices* Chapter 1.3). This enables accountability should any future investigation be made. It can also protect the organisation against any false claims.

In some very sensitive context, care should be taken when removing documents from the country. This should be coordinated between the office / project and the Swiss TPH HQ.

9.7 Procurement

The way one procures goods and services can have security implications. Many serious attacks, including murders of NGO staff, have been related to procurement issues. Unless procurement is carried out fairly, and is perceived as fair, some local traders and others are likely to feel aggrieved. In some contexts, “fair” may be interpreted as buying from local traders, even if their prices are higher. Depending on the situation, these grievances can be expressed in a variety of ways including threats to the safety of staff. They can also lead to costly and time-consuming legal action.

Great care should therefore be taken to ensure that procurement procedures are good, and followed. Retaining a good local lawyer can help in preventing problems and in defending against malicious or other claims.

9.8 Corruption

The security of the Institute can be threatened by corruption. For example, paying a bribe can lead to a threat if a similar bribe is withheld in future. Yet if civil servants are receiving no salaries, reasonable fees for their services may be seen as legitimate income. Swiss TPH should have no involvement with corruption. They should take the local situation into account when deciding – preferably in a coordinated manner with other organizations – whether certain fees are justified in a civil service or a commercial context.

All staff should be aware of the importance of avoiding corruption. Staff found to be involved in corruption should be disciplined. All relevant staff should be aware of practical ways of avoiding corrupt practices.

10 Prevention and response – How to…

10.1 Driving / Car accident

Preventive measures	Measures to be taken in the event of an incident
- General • Defensive driving is a must for everyone. • Wearing seat belts at all times is mandatory. • Regular maintenance of all vehicles and changing of tires • When in charge of a vehicle, the driver should be sufficiently rested and must not be under the influence of drugs, alcohol or medication. • The use of mobile phones is prohibited when driving (unless using a hands-free system). • Every driver must be in possession of the necessary authorisations/licences to operate the vehicle. • Driver training - Travel clearance • Each staff member leaving the greater city area on duty trip requires previous clearance by the local security focal point and approval by his/her line superior. • The clearance for duty trips can be done by using a “field trip form” and the process is indicated on the form. - Field trips by road - Vehicle check has to be conducted every time you intend to leave the greater city area and make sure your vehicle is equipped with the necessary tools. - The vehicle first aid kit should be available in each vehicle at all times and its content checked regularly. - Make sure you’re aware about the current security and weather condition of your route and destination prior to departure.	- Assess situation • Do not put yourself at risk. • If a crowd is forming, do not get out of the car and drive on to the nearest police station to report the incident. • If there is no possibility to leave the scene, keep a low profile and show empathy. - Call the Swiss TPH office or contact person for assistance: • Give as much detail as possible. Who: State name clearly. Where: exact location of accident What: type and gravity of accident number/age of casualties, injuries confirm number you are calling from - Make area safe • Warn other drivers and control traffic. • Stabilize vehicles (apply handbrake, put in gear etc.) - Assess casualties and give first aid • Deal first with those who have life-threatening injuries • Apply first aid scheme (ABC: airways – breathing – circulation). - After: document the accident • Request police to draw up an official report. • Take photos of position of car and note names and details of witnesses. • Remove all documents and goods, if the car has to be abandoned. • Fill in an incident form and hand it over to the Security Focal Point.

10.2 Medical emergencies

Preventive measures	Measures to be taken in the event of an incident
- General • Comply with the recommended vaccinations and health measures. • Familiarize with the representation's medical emergency procedures and make sure that all the staff knows the recommended referral facilities. • Make sure to carry a functioning communication mean (mobile, radio or satellite telephone depending on the situation/location) at all times so that in the case of an emergency help can be requested. • Have a first aid kit at hand (in offices and residences) • Attend to first-aid trainings • Ensure having an adequate stock of prescribed personal drugs available at all times. - Field trips by road • If possible use two vehicles when travelling outside the main city so that in the event of an accident or breakdown the second vehicle may be used to evacuate passengers or to continue the journey. • A first aid kit should be available in each vehicle at all times and its content should be checked prior to each trip.	- Assess the situation for danger - Alert and inform the local emergency services (police, ambulance service, medical services) with the following information: • Name of the caller • Time of accident/incident • Exact place, geographical location • Type of incident, description of incident • Persons involved, details of casualties • Situation on the ground (medical assistance, threats, security situation etc.) • Assistance and equipment required (ambulance, tow-car etc.) - If no emergency services are available, organize a transport to the next identified medical facility. - Give emergency first aid. - Contact the Swiss TPH office or the emergency Swiss TPH hotline for medical assistance - If a medical evacuation MEDEVAC is necessary call the Swiss TPH or the travel insurance hotlines.

10.3 Fire Hazard

Preventive measures	**Measures to be taken in the event of an incident**
• Always know where the nearest emergency exit and fire extinguisher is located and where the assembly point is. • Do not overload electrical sockets and routinely check wires from electrical tools. Replace damaged wires. • Discard cigarettes only in the provided ashtrays. • Do not lit candles in the office. • If using gas for cooking, ensure the gas flow is turned off when the cooking is finished. Have the stove and oven regularly serviced.	- Sound the alarm • Warn your colleagues by activating the fire alarm. • Call the fire brigade. - Fight the fire (if still possible) • Try to get out the fire with a fire extinguisher or a fire blanket. • Do not put your own safety at risk. - Escape • Shut off all electrical appliances. • Make sure all windows are closed. • Collect your personal belongings and head for the door. • Leave the room and close the door. • Follow the emergency exit and proceed to the assembly area. • Try to help others out of the building. • Never go back into dangerous areas. • Stay at the assembly until being told by officials that you can leave

10.4 Checkpoints

Before a trip it is important that the team agrees who will take the lead for the communication with checkpoint officials. All team members should comply to the instructions of the appointed team leader. Any wrong behaviour (panic, shouting, insulting) can have serious consequences on the safety and security of all the team members.

Approach slowly	• Check authenticity, • Reduce volume of radio/music, • Lock doors, • Remove sunglasses, • Have necessary documents ready. • Report to duty station only if not visible. • At night dip the cars headlight and turn on dome light.
Stop when told!	• Open window, • Show your hands, • Be slow moving.
Follow the instructions of the officials	• Do what Military/Police Officer tells to do. • Do not offer anything! • If your car is being searched, comply with the officials.
Answer questions in clear voice	• Be precise and truthful. • Do not start unnecessary arguments.
Be ready to explain your mission	• Who are you? Where are you coming from? Where are you going? What is your task?
Be ready to show documents	• Personal ID, driver's license, vehicle documents. Mission order
Verify all documents	• Be sure you receive all documents back.
Continue slowly	• Drive on as ordered.
Report to duty station	• If something urgent to report, do it immediately! • What / Where / When / Who is involved? How many are involved? What next

10.5 Burglary or Home invasion

Preventive measures	Measures to be taken in the event of an incident
One of the worst fears people have is of waking up or returning home to find an intruder in their home. However you react, your main goal must be to survive the ordeal without serious injury. To minimize the risk to yourself there are certain precautions you can take. - Choice of location and building • Choice of property location: e.g. is an apartment in a guarded tenant-occupied house safer than a single-family home? • Who are the next-door neighbors? • Are structural and technical security measures already in place? • Would the lessor be prepared to implement structural and technical measures? • Is there an alarm system connected to an intervention agency? - Organizational measures • Means of communication: carry properly functioning mobile telephones/radio telephones and ensure reception • Keep important contact numbers to hand • Are there escape routes? • Security guards: yes or no? - Further measures • Possible deterrents for use during lengthy absences: mail redirection, lights on a timer switch, light sensors for houses, etc. • On arriving home, be alert and observant. Examine your environment as you approach your home. Do not enter if you suspect that there might be an intruder in your home.	- If you are unsure if burglars are still on the premises, do not enter the building. Draw back and seek help e.g. call the police. - If burglars are still on the premises: • Don't take any risks/don't play the hero. Speak normally, stay calm • Cooperate (e.g. open the safe, hand over cash) and tell them what they want to know. Deceiving them about the whereabouts of keys, for instance, may lead to heightened aggression. • Police recommend that you say to the intruder very calmly, "Tell me what you want and I will give it to you." • If you do have to communicate with the intruder, tell them what you are going to do before you do it. For example “I am going to sit down.” • Treat the intruder as an equal. Do not be bossy or servile. Do not threaten or abuse him. Don't provoke him. • Do not make any sudden movements. Keep your hands where they can be seen. Do not crowd the intruder – try to keep a safe distance away. • Avoid physical and eye contact • Do not try to stop the intruder escaping. • Last resort: if the situation dictates it, defend yourself • Be observant and make a mental note of the intruder’s appearance and anything else about them. - When the intruder has left, secure your home, contact the police immediately and seek medical assistance if necessary. • Do not clean up before the police arrives

10.6 Armed robbery

Preventive measures	**Measures to be taken in the event of an incident**
Develop a sense of awareness and adjust your behavior accordingly, taking into account the surroundings and the possible risks they pose. - Observe your surroundings and be alert. - Be aware and assess the situation continuously. - To spot the unusual, you need to know the environment. - Be pro-active; consider ahead what could happen. - Keep in mind how to react, don't be taken by surprise. - Follow your instinct and use your common sense. - Act with confidence, even if you don't feel confident. - Act as if you know what you are doing or where you are going.	- Remain calm and assess the situation before acting. Do not react aggressively. - Obey any orders given, and always say what you intend to do. - Keep hands visible, remain passive and move with slow, precise gestures (be conscious of your body language). - Respond to demands, but do not offer more than what is asked. - Pay attention, and try to determine the attacker(s)'s agenda. - Maintain visual contact with your attacker(s), avoid making direct eye contact (eyes can show fear or anger and can trigger violence). - Memorize as many details as possible about the attacker(s). - Remember your life is not worth losing for material possessions Situational responses: - Passive resistance: keep talking to the attacker to try to occupy his mind or even persuade him to change his mind. - Active resistance: screaming; shouting for help; running away; fighting back (beating, scratching). - If you feel self-defense is the only option left then make your decision and act as swiftly and with as much force as possible. Shock is often a better weapon than force. However, self-defense techniques require regular training and constant practice. After action review: If someone has experienced physical force through a criminal act aimed at violating, damaging or abusing their person, it is important to have procedures available to assist the victim immediately. There are four major areas that need careful and competent management following an act of violence: (1) Reporting the attack (2) Psychological support (3) Medical care (4) Forensic evidence and legal pursuit These needs have to be fulfilled immediately and simultaneously. Therefore the necessary contacts should be made in advance. - Ensure that evidence is preserved (important for the investigation).

10.7 Carjacking

Preventive measures	Measures to be taken in the event of an incident
Collect information on: • potentially dangerous areas • the times of day when carjacking is at its most prevalent • carjacking methods used Based on this information, it is possible to apply the following measures: • Keep your windows closed. If you need to open a window, just leave a small gap open. • Lock the doors. • Systematically avoid carjacking hotspots. • Don't travel on the roads at night, dawn or dusk. • Never travel alone in high-risk areas – travel in convoy. • If you want to stop, never stop on the side of the road. Chose a protected place like restaurants, gas stations, hotels. • Make sure someone knows the time of your departure, your itinerary and your estimated time of arrival. • If necessary, arrange to get in touch with a third party more frequently during your journey (e.g. phone call every hour). • Make an objective judgement on who should or should not be informed of your movements (this information could be intercepted by criminal gangs, sold to others, etc.). • Try to mix up your routine by changing your vehicles, itineraries, schedules and days of travel. • Breaking down can place you in a vulnerable situation. It is therefore important to ensure proper maintenance of your vehicle. • Avoid using vehicles that attract attention. • Keep your car keys separate from your other keys. • Keep any valuables in the car out of view, preferably in the boot. Make sure no one can see what you have locked away there. • Never travel without a mobile phone, and make sure its battery is always charged. Find out about mobile phone coverage – if there are gaps in coverage during your journey, take a satellite phone (which you know how to use). Keep the satellite phone concealed on your person and put it in silent mode. If your phone signal is weak, remember that it may increase in strength on the roof of a house or on a hill, for example. • Make sure you know the relevant police emergency phone numbers; save these numbers on your phones in advance.	Any carjackers who approach your vehicle may be agitated or nervous. Avoid acting in a way that will exacerbate the situation: • Stop your vehicle without switching off the engine. • Put the gear in neutral and pull the handbrake. • Do not resist; keep your hands in view. • Avoid making any sudden movements. Take particular care when unfastening your seatbelt – explain to your assailants what you are about to do. • Obey the carjackers' instructions immediately and as best you can – your assailants will likely be nervous and armed, and will want to leave the scene as quickly as possible. • Give the assailants your valuables, e.g. jewellery, wallet, briefcase, if they demand them. • Keep calm and make it obvious that you intend to surrender your vehicle to them. • Do not speak to your assailants – only speak in answer to their questions. • Leave the vehicle as soon as the assailants want you to do so; get out calmly and leave the door open and the key in the ignition. • Do not try to take any belongings with you from the car. • Do not lose your temper, and avoid doing anything that may exacerbate the situation. • Avoid all eye contact with your assailants, because they may think you are trying to memorise their faces. However, stay alert and try to memorise their physical characteristics and the clothes they are wearing. • Turn around and move away from your car slowly if the assailants want you to do so. • Let the carjackers drive away without hindering them. • Notify your representation and report the incident quickly and accurately. • Recount the incident to the police as soon as possible. Only ever consider making a getaway if your life is in danger. Only people trained in executing getaways by car should take the risk if necessary.

10.8 Ambush

An ambush can loosely be described as a surprise attack on the road. Each possible ambush situation will vary in the methods used, as well as the reaction by the driver and passengers of the vehicle.

Preventive measures	**Measures to be taken in the event of an incident**
An ambush can be initiated in a variety of ways: • by an obstacle placed on the road to slow down or divert the vehicle; • by a staged accident or injured person to stop the car for help; • by a roadside bomb or concentrated gunfire aimed at the vehicle. The terrain influences the location of ambush sites and type of ambush: • poor roads and steep inclines may limit vehicle speed and manoeuvrability, hence increasing its vulnerability; • blind curves, or sharp 90-degree turns are opportunities for the bandits to hide and act by surprise; • environment features, such as large rocks in the desert, or isolated houses, also provide opportunities to hide before attacking the vehicle by surprise. Some points that could help to minimise the risk: • make an accurate monitoring of stretches subject to ambushes • pass only during certain times when there seems to be less risk • riding in a convoy could deter attackers • identify alternative routes • avoid routine	A driver will have to take decisions based on many factors, and this in a very short time. It may even be more a question of reflexes than of well-thought through decisions. Being aware of the possible options and reactions will help suggest the safest reaction in these critical seconds: • If your vehicle comes under direct fire, you could accelerate rapidly and drive straight through the ambush until you reach a safe area. • If it is not safe to drive through the ambush because of an obstacle in the road or assailants directly ahead with weapons pointed at you, you may have no choice but to stop the vehicle and comply with the attackers' instructions. If the ambush is for the purpose of a robbery/car-jacking then this is most likely to be the safest option for your own physical person. • If you encounter a situation where an incident occurs in front of the vehicle, then you should stop and reverse/turn around as safely and quickly as possible. If it is not safe to do so, or if it is not possible because there are cars behind (etc.), stop the vehicle, leave the keys and get out on the side furthest from the incident. Take immediate cover; lie flat and crawl (using elbows and toes to propel you forward) to the nearest cover (ditch, hollows, solid wall etc. – beware of danger of landmines). If there is no cover from shooting, find cover from view (tree, bush etc.). Do not get up until the firing has stopped and you think it is safe to do so. • When safe to do so and protection is available, make your escape away from the immediate area. Do not resist if the attackers approach you.

10.9 Shooting

Do	Don'ts
As soon as you hear gunfire, move immediately to the nearest available hard cover. Bullets will go straight through wood, sheet metal and even brick, so look for a deep ditch, a solid concrete wall (min. 30cm) or similar solid cover. • If there is no hard cover, then cover from sight (light cover) may be your only option. • Keep as low as possible and try to work out where the fire is coming from by looking around (i.e. to the side of) the hard cover, rather than looking over it. Once you have had a look, get back behind hard cover and, if you can, move your position slightly away from where you were. • Once you know where the fire is coming from, decide if there are any safe escape routes. If possible, an escape route should be out of the line of fire. If that is not possible, select a route that is well protected from the gunmen's sight and fire for as long as possible. • It may be safer for you to stay as you are, behind hard cover, and wait for assistance. If you decide you have to move, do so quickly. Speed is generally better than zigzagging.	• Don't hang around, even if you think the firing is not directed at you. • If you are inside a building, don't stand near windows or doors. Find hard cover and communicate.

10.10 Landmines

Preventive measures	Measures to be taken in the event of an incident
• Never attempt to move or even touch a mine. • Vitally important: do not be tempted to move onto the verge of the main road to get past some obstacle or even to allow another vehicle through. The verges may contain mines. If necessary, reverse back to a wider area and let the other vehicle pass. • Landmines have different shapes and different detonation mechanisms. Depending on the context where you had been deployed inform yourself about the location where landmines were used, types of landmines and how local people mark these dangerous areas. Sometimes there are signboards indicating the danger or mines but more often there are only signs setup by the local population using sticks, stones, cloth or specific colours. There are numerous sources of advice: • your colleagues, local staff (especially the drivers); • local authorities, including the police and military; • public transport organizations; • other NGOs and UN personnel; • check-points; • hospitals; • and, especially, the local population. Always seek local advice if moving into a new area or one that has been the scene of recent fighting. Be on your guard against “cleared areas”. The military may declare an area clear of mines, but they cannot be 100% certain. Roads, main squares, etc. might be clear but it requires an enormous number of men to physically clear even a small village.	• If for some reason you are in the middle of a mine infested area: STOP AND SEEK FOR HELP. Ideally, a demining team would assist you. Therefore, it is important to carry key phone numbers with you. • If you are in the lead vehicle and you spot mines, stop immediately and inform the second vehicle. • Reversing taking the same way you just used, following the exactly same track should only be the solution of last resort. Foot tracks or vehicle tracks are not always fully visible and detonations can still happen. • Do not try to turn your vehicle round. Do not get out of your vehicle. • If a road is obviously blocked by something (for example, a tree or a vehicle) in a likely mined area, do not be tempted to drive onto the verge or hard shoulder to get by. It could contain mines. Turn back.

10.11 Explosives suspicious deliveries

Preventive measures	Measures to be taken in the event of an incident
The following signs are a useful guide to identifying suspicious mail: • Origin and address: a letter or package addressed by hand, often in an unusual style of handwriting, mailed from a location unfamiliar to the recipient. • Excessive amount of stamps: a letter that contains many more stamps than normally required. • Used stamps: if the stamps on the envelope have previously been used on another mail delivery. • Thickness: a letter that is thicker than normal. • Weight: a letter/package that is heavier than you would normally expect for its size. • Stiffness: a letter that is stiffer or more rigid than normal. Do not bend. • Grease marks: dark, greasy stains on a letter/package caused by the explosive "sweating". • Tape: tape around the edges and sealing of the flaps of an envelope or parcel. • Smell: a letter/parcel that smells like almond (or marzipan) or has some other unusual smell. • Balance: a lopsided letter/package, heavier at one end than the other. • Enclosures: a sealed enclosure inside the outer mailing envelope. • Wire or metal bits: if protruding from the letter or parcel.	If a letter or parcel is identified as suspicious: • Do not attempt to open it. • Place it gently on the ground or table. • Clear all personnel from the immediate area. • Clear the building and evacuate to the designated safe area out of the building, • Call the police or special bomb disposal unit. • Keep staff as calm as possible. • If possible and safe to do so, remove all vehicles away from the building. • No one is to re-enter the building once evacuated. • Conduct a headcount to ensure everyone is accounted for. • Assign staff to ensure access routes and roadways are clear for emergency vehicles.

10.12 Bomb goes off

Do	Don'ts
• Remember that terrorists sometimes follow up bomb blasts with shooting attacks so, if you are able to do so, move away from the scene of the blast to a secure area. This may mean going inside a building to an area that you can consider hard cover – in other words, behind something very solid, and away from windows and doors. • Keep away from glass or other sources of shrapnel. • Once you are in a safe area, communicate and summon help. • Remember that terrorists commonly plant a second bomb in a place where crowds, security forces or injured victims may congregate after the first blast.	• Do not hang around in these sorts of areas – either stay in your safe place or move well away from the scene of the blast if you can. • Don't stay near common hiding places for bombs, such as bins, cars, lorries, bicycles. Keep a wary eye out for cars or lorries that are heavily laden or have unnecessary antennae.

10.13 Robbery

Do	Don'ts
• If somebody attempts to rob you with violence, remember the golden rule. Don't resist in order to protect your possessions. • Keep calm, and keep other people around you calm. • Try to remember what the robbers looked like, so you can give a description to the police afterwards.	• Don't antagonize the robbers or make any sudden moves that they might think are threatening. Note: If you are being beaten without any attempt at robbery, you may decide to fight back. But only start to fight back if you believe you can win. Fighting back against an overwhelming opposition will probably only make things worse for you.

10.14 You are being followed

Do	Don'ts
• Keep calm. • Act on it – don't worry that you may be overreacting. There are many stories of people who suspected they were being followed by criminals, who didn't do anything about it and now regret it. • Go immediately to a safe place, and ask for help. A safe place might be, for instance, crowded places, a large hotel, a friend's house or police station. Don't leave there until you are sure you are safe. • Report the incident.	• Don't confront the person(s) following you. Try not to make it clear you know they are following you. • Don't continue walking or driving to places where your followers could attack you, e.g., to places where there are few people, or there is poor lighting.

10.15 Kidnapping / Abduction

Do	- **Don'ts**
• Remember that the vast majority of kidnap victims are released safely. • Remember that your family, friends and colleagues will do all they possibly can to get you released as quickly as possible. • Maintain your dignity – be friendly and cooperative, but not servile. • Establish a rapport with the kidnappers, if you can. It may come in useful! • Play down your own importance. • Tell the kidnappers your basic needs and inform them of any medication you need. • Establish a daily routine, and keep fit, both mentally and physically. • Use your mind constructively and think of what you will do when you are safely home. • Eat as much as you can – it is an important part of maintaining your strength. • Keep in mind that you may be kept in captivity for some considerable time. • Keep track of time. • Decide on the safest place in the event of a rescue. If there is a rescue, go to that safe place, stay still and do not get up until you are told to do so by your rescuers.	• Don't resist during the abduction. • Don't antagonize your kidnappers. • Don't try to negotiate your own release, or become involved in the negotiations. You are in no position to do so. • Try not to give any information that could help the kidnappers put pressure on your family or organization. • Don't allow yourself to think you have been forgotten – the kidnappers may try to convince you that that is the case, but it will not be true. • Don't try to escape unless there is no other alternative, or you are very confident that you can escape successfully. • Don't believe what the kidnappers tell you. They are very likely to lie to you. • The kidnappers may tell you to help them provide 'proof of life'. Do not refuse to do this. • Don't tell the kidnappers that you will recognize them, or be able to come after them after your release.

10.16 Sexual attack (women and men)

Recommendations
• Go to a safe place. • Communicate. Call a friend, a family member, a close colleague or someone else you trust who can come to you and give you support. • If you want to report the crime, notify the police immediately. Reporting the crime can help you regain a sense of personal power and control. • Preserve all physical evidence of the assault. Do not shower, bathe, douche, eat, drink, wash your hands or brush your teeth until after you have had a medical examination. Save all of the clothing you were wearing at the time of the assault. Place each item of clothing in a separate paper bag. Do not use plastic bags. Do not clean or disturb anything in the area where the assault occurred. • Get medical care as soon as possible. Go to a hospital emergency department or a specialized forensic clinic that provides treatment for sexual assault victims. Even if you think that you do not have any physical injuries, you should still have a medical examination and discuss with a health care provider the risk of exposure to sexually transmitted infections and the possibility of pregnancy resulting from the sexual assault. Having a medical exam is also a way for you to preserve physical evidence of a sexual assault. • If you suspect that you may have been given a “rape drug,” ask the hospital or clinic where you receive medical care to take a urine sample. Drugs, such as Rohypnol and GHB, are more likely to be detected in urine than in blood. • Write down as much as you can remember about the circumstances of the assault, including a description of the assailant. • Get information whenever you have questions or concerns. After a sexual assault, you have a lot of choices and decisions to make - e.g., about getting medical care, making a police report and telling other people. You may have concerns about the impact of the assault and the reactions of friends and family members. You can get information by calling a rape crisis center, a hotline or other victim assistance agencies. • Talk with a counsellor who is trained to assist rape victims.

10.17 Civil unrest

Preventive measures	Measures to be taken in the event of an incident
- Setup an alert system and network • An alert system (sending sms for example) can dispatch messages regularly to all staff of the office containing security related information. The alert system is also maintained over the weekend and during holidays. • The security focal point continuously evaluates the evolving situation and sends updates of the current status. - Take alternative routes • Think about and define escape routes for areas commonly known to be affected by public gatherings and violent demonstrations.	- Assess situation • Avoid gatherings, demonstrations and large crowds, and any other situation, which could become heated. • Inform the security focal point as quickly as possible if you have not yet received an alert about the event. - If you are on foot and become caught up in a hostile crowd • Turn around and walk briskly in the opposite direction – do not run. • In a moving crowd, stay on your feet, move with the crowd and keep (or move) to the edge of the crowd where it is safer. - If you are in a vehicle and become caught up in a hostile crowd • Turn around and drive away if possible. • If you are too close to a crowd and cannot turn around, drive to the side of the road if possible, park the car and if safe/possible to do so, get out and walk away from the crowd. Alternatively take the nearest safe side road and drive away slowly. - If the car is unable to move • Stop and turn the engine off. If it is safe/possible to leave the car, all passengers should do so and follow the recommendations for pedestrians. • Should the crowd start to shake the vehicle, remain polite and do not interfere. Try to leave the car as soon as possible and behave in such a way as not to antagonise the crowd.

10.18 Crowd

Do	Don’ts
• Remain calm and maintain your dignity. • Keep a low profile. • Look for friendly or non-hostile faces. • Walk (do not run) quietly away. • As soon as it is safe to do so, communicate and summon help.	• Don’t lose your temper or start shouting.

10.19 Siege or captured in a place

Do	Don'ts
• Remain calm and try to make sure others do the same. • Make yourself as inconspicuous as possible. You do not want to draw the attention of your captors. • Maintain your dignity, but be friendly and cooperative to your captors. • Ask your captors for any basic needs – e.g. toilets, washing, food, urgent medicines, etc. • Note any escape routes, or hiding places, which you can use in the event of an armed rescue. If there is an armed rescue, find the nearest cover (or simply lie down) and stay still until your rescuers tell you to move.	• Don't antagonize your captors or make any sudden movements that might alarm them. • Don't stand out from the crowd. • Don't try to escape or fight back unless you are very confident you (and others around you) can succeed.

10.20 Illegally detained

Do	Don'ts
• Keep calm and dignified. Keep your temper. • Be helpful. Explain that there has been a misunderstanding and suggest ways of resolving it through discussion. • Ask for a lawyer, colleague or embassy representation. Continue for as long as necessary to make this request. • Ensure that you verify the identity of anyone who arrives claiming to be your lawyer or a representative of the embassy. • Remember that your colleagues, family and friends will do all they can to get you released. You will not be forgotten!	• Don't be argumentative or abusive. Do not resist arrest. • Don't sign any piece of paper given to you by the authorities, unless it has first been seen and agreed by your embassy representative or lawyer. • Don't agree to any concessions in return for your release. If pressed, you could say that you will consider these concessions once you have been released. Then contact your embassy or lawyer as soon as you are released.

11 Annexes - Templates

11.1 ANNEX 1: Template Risk Assessment

11.2 ANNEX 2: Template Local security plan

11.3 ANNEX 3: Template / Checklist Contingency plan

11.4 ANNEX 4: Deployment strategies

11.5 ANNEX 5: Checklist Briefings

11.6 ANNEX 6: Checklist Debriefing

11.7 ANNEX 7: Pre-departure document sample

11.8 ANNEX 8: Incident Reporting Form

11.9 ANNEX 9: Mission order template

11.10 ANNEX 10: Vehicle Inspection list

11.11 ANNEX 11: Checklist for First Aid Material