actalliance

ACT Staff Safety and Security Guidelines

A Handbook for ACT Staff

Good security management is about good program management: Proactively managing risks and being better positioned to deal with crises enables us to work safely and securely. This benefits our staff, beneficiaries, and other stakeholders.

To provide practical resources ACT Alliance members, the Security Working Group (SWG) has developed the "ACT Safety and Security Guidelines: A Handbook for ACT staff" and the complementary "Staff Safety and Security Principles for the ACT Alliance". The Guidelines gives an overview of generic policies and procedures for the safety and security issues affecting most of our operations – as such, they can be used as a reference and resource. They are written for managers and staff. Since staff and managers have different roles and responsibilities, each chapter and annex starts with an explanation of the intended users and usage. The Guidelines was originally developed in June 2008 with the title "ACT Security Handbook". It was revised in March 2011 to take into account the change of name to ACT Alliance and the broader mandate of the ACT Alliance. This document can be found on: http://www.ACT Alliance.org/resources/policies-and-guidelines/security

Table of Content

Back to TOC

1. Introduction

Users and Usage: All readers are encouraged to familiarize themselves with this chapter so that they can understand the foundations of these Guidelines; the relationship between their individual and the organization's responsibilities; and the ACT Alliance's general approach to security.

1.1 The Purpose of these Guidelines and how it relates to ACT's security policies and plans.

The ACT Alliance is committed to staff safety and security. All levels of our organizations aim to integrate security in ways that are relevant and user-friendly. Good security management is about good program management – it enables us to work safely and securely. Proactively managing risks and being better positioned to deal with crises enables us to work safely and securely. This benefits our staff, beneficiaries, and other stakeholders.

To support ACT Alliance members with proactively managing security, the Security Working Group (SWG) has developed the "ACT Staff Safety and Security Guidelines: A Handbook for ACT Staff" (Guidelines) and the complementary "ACT Staff Safety and Security Principles". The Guidelines are written for managers and staff. It gives an overview of generic policies and procedures for the safety and security issues affecting most of our operations. These Guidelines are a reference and resource- both for agencies who do not already have security procedures in place and those who do. Since these generic guidelines, any agency specific policies and procedures overrule these. This document will be reviewed by the ACT Security Working Group every three years and revised as appropriate.

These Guidelines, together with the "ACT Staff Safety and Security Principles" and your organization's country-specific security plans, can form the cornerstone of your policy and guidelines on safety and security. These Guidelines and the Principles (as well as other resources) are available on the ACT Alliance website on http://www.actalliance.org/resources/policies-and-guidelines/security. To assist every operation with creating specific security plans, see Annex N.

The "ACT Staff Safety and Security Principles" commits ACT members to five key principles:

> **Principle 1**: Provide leadership, guidance and capacity to ensure that staff safety and security concerns are adequately addressed.
>
> **Principle 2:** Adopt a systematic approach towards identifying safety and security risks, and identify suitable preventive and control measures.
>
> **Principle 3**: Build staff capacity so that they are empowered to take personal responsibility for their own security
>
> **Principle 4**: Read, discuss and understand the ACT Staff Safety and Security Guidelines
>
> **Principle 5:** Provide psychosocial support to ACT staff that have experienced acute or prolonged stress during the course of their work.

1.2 ACT Alliance commitment, organizational duty of care, and individual responsibilities

The ACT Alliance views staff safety and security as one of the first and foremost concerns in its development, humanitarian and advocacy work. The sharp increase in attacks on aid workers in the past decade, particularly among humanitarian aid workers, makes it imperative that ACT members have measures in place to ensure the safety and security of their programme personnel (employed or volunteers) and resources.

Safety and security management is a collective responsibility. It involves participation by every person working for an ACT member. Trustees, Executive Officers, and Directors should ensure the member organizations exercise duty of care towards all staff. This commitment needs to be visible throughout the management line. Regional and country directors and their field managers will lead by example, demonstrating a systematic approach to assessing and managing safety and security. ACT Alliance members should use each other as resources, for example, sharing travel briefings.

Members are responsible to ensure their workforce is adequately prepared and equipped to manage the risks they face when delivering assistance to those who need our help. Directors and senior managers are responsible for the safety of their staff and must ensure staff have access to training and resources. Staff members are responsible for their individual well-being and should take their individual responsibility seriously.

The ACT members' security measures depend on each individual employee, visitor or consultant acting responsibly, using common sense, good judgement and the advice of experienced colleagues whenever necessary. Each staff member should stay aware of security risks, keep her or himself up to date on security procedures, and promote the security of other staff. All travellers are expected to use the advice from the agency's Security Plan (Annex K, annex N and for specific advice, consult the relevant sections below) and their experience and common sense to make sensible judgements on security issues when travelling, whether to a country of relief operations or to the headquarters of members in countries with no relief operations.

1.3 ACT Alliance's approach to security

In accordance with the Alliance's vision and mission and the values of its members, the ACT Alliance's approach to security is based on acceptance by the local population. If the members' work is known and valued by the local communities, it is less likely that they will be the victims of security incidents. This also refers to ACT members' pledge to honour quality and accountability, e.g. by adherence to the ACT Code of Conduct for the prevention of Sexual Exploitation and Abuse, Fraud and Corruption and Abuse of Power, the Code of Conduct for The International Red Cross and Red Crescent Movement and NGOs in Disaster Relief Red Cross Red Crescent Code of Conduct, the Sphere Humanitarian Charter and Minimum Standards, and any other policy principles and guidelines adopted by the ACT governance and members and therefore binding on all members.

Where there is a doubt about acceptance of the ACT member or other NGOs; where there are particular threats against the ACT member or similar organisations; or, where criminal threats affect the general population, protective security measures will probably still be necessary. Common protective measures include gates, guards, locks and safes. The protection measures used should be proportionate to the assessed risk in each location.

Due to various considerations, a member may seek to maintain a low profile as it supports the work of local partners. This may bring several benefits, including a reduction in the risk of working in that area.

In certain contexts, ACT believes that it has a duty to speak out to promote or defend the rights of poor and excluded people. Because speaking out can sometimes garner a strong counter response, which can have implications for the security of the people on whose behalf the statement is made. It can also have consequences for the ACT member's implementing partners, staff and property, and on other relief and development organisations. Therefore, before speaking out, the ACT member should always weigh these risks against the likely benefits, as far as possible in consultation with those likely to be affected.

Back to TOC

2. Essential Aspects of Proactive Security Management

Users and Usage: Security focal points and other managers with security responsibilities can use this chapter to understand the mechanics and issues of managing security. For staff, not all sections will be relevant to you. You should, at least, familiarize yourself with the security categories, risk assessment, security plan, training, briefing and debriefing, media and fire sections. Depending on your job and responsibilities, you may want to review other appropriate sections.

2.1 Security management in country-based programmes

The security of staff and assets depends on the threats in the environment and the organization's/ individual's ability to minimize risks. A crucial part of managing risks is to be proactively prepared with realistic plans, procedures and resources in place. This chapter aims to support your efforts by covering the essential aspects of security management.

2.2 ACT Member and Alliance Security Focal Points

Every ACT member should have a Security Focal Point, in country and at HQ, who have received in-depth training on safety and security issues. In some cases, Security Focal Point will be a dedicated Security Manager and in other locations it will be a senior manager. The Security Focal Point should be available to all staff to provide advice and other help in security management, as required. There should be, at least one appointed deputy and in some cases additional deputies. Contact details should be made available to all staff, and in the case of high risk countries, someone should be available for 24 hours a day. ACT Alliance members should know the names and contact details of the other Alliance members' Security Focal Points. The ACT members' Focal Points should know each other and be in regular contact about security and safety issues.

In countries where insecurity is high, an "ACT Alliance Security Focal Point" should be nominated by the members of an existing national or regional ACT Forum from within the staff of the Forum members. The focal point responsibility is envisaged as additional to, or part of, the nominated staff member's position in their organisation, rather than as a separate position. It is not an additional funded position. It is expected that the Security focal point will be a non-rotating position where possible. Working on behalf of the whole ACT Forum, this person will be the primary link with the chair of the global ACT Security Working Group (SWG) for support and information sharing on security-related matters (see Annex Z)

2.3 Security risks categories

It is a good practice to maintain an updated list of the security categories for each area of operation for an organisation. The categories are a simple way of describing the approximate level of risk for each country/ area, as assessed by the member or members. In the case of a national ACT member, this is determined by the director of their main office in the regional or national capital. Where ACT forums are pooling their security work, it would be the directors at their main offices either overseas or in the capital. The ACT Secretariat will also keep an updated list of security category codes. The security risks categories are listed below:

2.3.1 Category 1 (blue) – Minimal Risk

In this category are countries with exceptionally low crime rate and efficient crime prevention and emergency services.

2.3.2 Category 2 (green) – Low Risk

Category 2 countries typically enjoy a stable political system and a relatively good internal security and emergency services infrastructure. Threats from terrorism, crime, civil unrest are typically moderate and are generally mitigated by the capacities of internal security agencies.

2.3.3 Category 3 (yellow) – Medium Risk

Category 3 applies to countries with High crime rate, or problems within the country due to current political, military, or social problems, or natural phenomena etc. It means that there is no immediate danger to programme staff, but that background security problems have increased. The programme can continue operating. However, it may be necessary to restrict travel to some areas, and the hours of the curfew (if any) may change.

2.3.4 Category 4 (orange) – High Risk

Countries in this category typically suffer chronic instability and lawlessness. When a country is designated category four, all staff are to return to the office during working hours or to the staff house or hotel outside of working hours, after which all staff movement may be restricted to safe areas only. It may be necessary to suspend the programme completely and to evacuate non-essential staff from the country.

2.3.5 Category 5 (red) – Extreme Risk

Countries classified as category 5 may be engaged in civil or transitional conflict; government control is minimal, non-existent or threatened; violent transformation of the government is on-going through military coup or revolution. Corruption is typically endemic and the state has failed or threatens to fail. When a country or region is declared category 5 staff evacuation should take place as soon s possible as per the country's evacuation plan.

Areas considered Category 5 are those in which the presence of expatriate staff may not be possible due to persistent extreme risks.

Since the categories describe the approximate level of risk for each country/ area, they can be used to guide program decisions and actions. In the example below, the categories are linked to situational indicators and program decisions.

2.3.6 SAMPLE: Security risks categories linked to situational indicators and program decisions

Security Risks Categories	Indicators	Program's Security Decisions
Minimal (Blue)	• No security events	• Fully operative
Low (Green)	• Minor insignificant and isolated incidents, curfews, riots • No immediate threats in agency project areas and capital	• Fully operative • Relocation, evacuation, suspension and hibernation plans reviewed • Support partner agencies with their security plans
Medium (Yellow)	• Tension and minor incidents at checkpoints • Minor clashes between armed groups without civilian casualties • NGOs affected accidentally but no injuries on staff • Serious but isolated attacks on civilians (mine explosion) • Suicide bombings in agency project areas • Few aerial bombings outside agency project areas	• Fully operative but decision on whether to conduct monitoring visits should be considered by _____ and in some cases postponed. • Relocation, evacuation, suspension and hibernation plans drilled • Encourage Partners to drill their plans • Weekly security situation reports
High (Orange)	• Escalation of armed conflict in agency project areas • Major clashes between armed groups with civilian casualties • Communal violence affecting civilians directly • Serious but isolated attacks on civilians in capital (suicide bombs) • Aerial bombings in agency project areas	• Partly operative • Hand-over key activities and documents to partners. Discuss financial and program issues with them. • Local partners encouraged not to work in field (hibernation) • Ready for relocation, evacuation and care for the remaining national staff • Daily situation reports • Daily meeting regarding security decisions
Extreme (Red)	• Breakdown in law and order • Repeated attacks on civilians and vital installations in capital • Deliberate, repeated attacks on NGO staff • Full scale armed conflict in most districts	• Program suspended/ ended • Implement plans for staff relocation and evacuation and care of the remaining national staff

In Chapter 5, there is a similar matrix focusing on evacuation and relocation.

Another way that members can use the security categories is to link it closely with actions by managers, security focal points, and/ or staff. In the example below illustrates this for a manager.

2.3.7 SAMPLE: Security Measures Matrix (Manager)

SECURITY MEASURE	THREAT LEVEL				
Review risk factor matrix from security staff	🟦	🟩	🟨	🟧	🟥
Procedures for evacuation, suspension, relocation	🟦	🟩	🟨	🟧	🟥
Weekly/ bi-weekly communication about security with senior managers			🟨	🟧	🟥
Daily communication about security with senior managers				🟧	🟥

2.4 Risk assessment

A risk assessment should be carried out before any visit to any potentially insecure operational area or any action that could carry a security risk. A similar assessment is necessary before making public statements. (See 2.13 on Public Statements below.)

The designated security focal point for each country or regional programme should conduct a risk assessment as often as he or she deems necessary. For work starting in a new operational area, a risk assessment should be carried out before work begins or the initial visit takes place. Annex W has a standard format and guidance for carrying out a risk assessment. ACT implementing partners are encouraged to use this format unless a suitable alternative is provided which improves it. Context-specific Security Plans (see 2.5 and Annex N) for a country or area need to be based on the risk assessment.

While organizationally, ACT Alliance members are responsible for conducting timely risk assessments, individual staff are responsible for familiarizing themselves with the basic terms and being able to follow the security plan based on the risk assessment.

2.5 Security Plan

A Security Plan should be a concise document that sets out the security rules and procedures appropriate for the country/ location. All ACT members are encouraged to write Security Plans for their countries of operation, even in low risk countries there is often a threat of crime, banditry or other security threats.

There are two main kinds of documents that comprise a Security Plan: Standard Operational Procedures (SOPs)/ Guidelines/ Protocols and Contingency Plans/ Emergency Plans. The Security Plan can also incorporate or refer to other documents that play a role, for example certain HR policies.

SOPs are for day-to-day precautions. Contingencies are responsive plans for managing extra-ordinary events so to mitigate the impacts. In broad terms, SOPs are preventative and Contingencies are reactive.

Security documents should target specific end-users by being relevant, informative, and realistically addressing their needs, concerns, issues, and usage. Let's say the office is attacked by armed robbers, for example: Then the computers and petty-cash will be stolen but lives will be saved because all office staff will have been given advice and training on how to react. But the Office Manager, dealing with the aftermath of the incident, will have an additional set of instructions like calling the insurance company.

Having contingency plans is not enough: There needs to be preventive plans so that staff and assets will not be threatened. In this example, there should be SOPs on cash handling (section 3.9) and site security (Annex Y). The cash handling SOPs would be for the finance department and not shared with other staff. The existence of the cash handling SOPs, if followed, will probably mean that large sums of money were not kept in the office. The site security SOPs would be required reading for all staff but guards and some managers may have received extra points or specialized training. Preventive site security measures reduce the chance that the office will be targeted for an attack. Annex N details more advice on writing Security Plans.

The most senior staff member responsible for security should write or oversee the delegated staff writing a Security Plan. Your Security Plan needs to be context-specific and highlight organizational security rules and procedures, which apply to staff in, or travelling to, that country. Each organisation should also identify a Security Focal Point (section 2.2), whose responsibility it is to ensure that all staff are aware of and following the policies and procedures outlined in the Security Plan.

Each Security Plan should be based on the risk assessment (section 2.4) for that country/ location, so that its rules and procedures are tailored to the risks in that area. In low-risk locations, both the risk assessment and the Security Plan can be very short. In high-risk locations, both documents are likely to be more detailed. In all cases they should be as concise as possible, since busy staff may be tempted to ignore long documents. What is important is that they should be appropriate to the circumstances of the particular location that they refer to.

Annex N is a standard format and guidance for writing a Security Plan. When ACT members in a given location and also across the region and internationally, follow this basic format, then inter-agency coordination can be improved during crises.

2.6 Training

As stated in the *"ACT Staff Safety and Security Principles",* all ACT members are strongly encouraged to train their staff in the security risks and threats presented by their activities. This includes ensuring that staff receive security training as appropriate to the roles and responsibilities that come with their jobs. Indeed, nearly all staff serving in an implementing organisation require *some* type of security training, from the senior managers to the drivers, gardeners and domestic personnel. Different types of security training are required by different types of staff.

In the annexes, there are a package of trainings that can be modified to suit your organization and location.

- Security Foundation Course *(Annex R):* The primary purpose of the course is to give staff an overview of how your agency's policies, principles and regulations relate to security and safety.
- Personal Security Course *(Annex S):* The primary purpose of the course is to train staff on security procedures that will affect their work.
- Security Management Course *(Annex T):* The primary purpose of the course is to prepare and support managers with security responsibilities.
- Crisis Management Course or Exercise *(Annex U):* The primary purpose of the course is to familiarise managers with security responsibilities with the procedures and decision-making processes likely to be required if such a crisis occurs.

These courses can be conducted in-house, with the ACT Alliance or externally. In the annexes, there are suggestions to assist with developing and implementing the courses. The suggestions can also be used as guidance when you need to select the right external courses for your staff.

It is important that each member considers all of the staff of their organisation, and ensure that all receive appropriate security training. It is not enough for senior managers alone to receive training; it is only when all staff have learned about security principles and can put them into practice through their daily choices and behaviour, that the safety and security for staff and resources will be enhanced.

2.7 Briefings and debriefings

Briefings and debriefings allow for the quick and effective exchange of security and safety information between the organization and the persons it is responsible for.

2.7.1 Briefings

ACT members should ensure that appropriate security briefings are given to all individuals for whose security they are responsible. This includes staff, invited visitors and consultants, who are being hosted by the member. The aim of a security briefing is to enable someone to understand the local situation sufficiently to live, travel and work safely in it.

Locally based staff should receive a full security briefing before they start work, appropriate to the location. For all internationally recruited staff, invited visitors and consultants being hosted by the ACT member, they should get a security briefing before they travel to any location. The briefing should outline the current risks and the main precautions that need to be taken (see Annex M).

This briefing may be complemented by a follow up phone call with a manager working in the location to which they are travelling. It should be accompanied by at least basic written information (for example recent situation reports) to remind them of points that they may not have taken in during a face-to-face briefing. On arrival, an additional security briefing can give greater details.

Further security briefings should be given as often as necessary according to the judgement of the relevant line manager, including when people are moving to a new location. For example, in low-risk locations, an annual security briefing may be sufficient. In some high-risk locations a daily security briefing may be required.

2.7.2 Debriefings

On return from work-related travel to high risk areas, the line manager should debrief the recent traveller, to:

- Check the staff member's general well-being
- Identify any lessons relevant to good security management for future trips, or anything that may change the agency's risk/threat analysis of the given area (Annex W). These should be passed on to the member's organisation's Security Focal Point, and shared with other ACT members and the wider humanitarian community where possible and useful.
- Discuss any security-related difficulties experienced during the trip.
- Receive a completed incident report form (Annex F) from the traveller, if any incidents or near-misses occurred. 'Near-misses,' such as when the vehicle was confronted by threatening individuals with guns, though nothing actually occurred that harmed the staff, are equally important to capture on an incident report form.
- Ensure that the traveller who has been involved in an incident has the necessary medical checks, including psychological care, if necessary. It is important for managers to take a pro-active role to encourage and facilitate their staff receiving appropriate and adequate psychological care following exposure to a traumatic incident. Needs may differ with individuals depending on sex, age, culture, belief, or other such status.

2.8 HR Issues Related to Security

There are numerous places where security and human resource issues cross paths. This section maps out a few key areas.

2.8.1 Recruitment

Good security is dependent on good quality staff. It is essential to check references before a staff member receives a contract or starts work.

In fast-moving crises it may be difficult to check all references of urgently needed emergency response staff. It is essential however that at least the reference of the most recent employer is obtained at all times to ensure an overall assessment of the candidate and suitability for the job. Managers should also use their judgement to make whatever checks are possible.

Local employment laws should be carefully respected. Some NGOs have faced security threats from disgruntled former staff or their friends, particularly when personnel have been dismissed in what they regard as an illegal or unfair manner. It is therefore strongly recommended that a local employment lawyer be consulted for all employment related decisions.

2.8.2 Workplace harassment and violence

All staff, visitors, and others associated with ACT Alliance members have the right to not be harassed or subjected to violence by another staff member. Sexual harassment and/ or harassment based on nationality, ethnicity, religious and other differences will not be tolerated. Your organization should have a clear policy and means to communicate this to new staff and on a reoccurring basis for current staff. The HR and security personnel should highlight every individual's right to security and safety and underline the consequences for breaking policy.

2.8.3 Ending staff contracts

The process of contracts should be carefully planned and sensitively managed. In some circumstances, the termination of staff contracts, if poorly managed, can lead to security risks. So that staff know what to expect, contracts should be drawn up with the possibility of short notice being given in times of crisis.

Local employment laws and customs should be followed scrupulously. A local lawyer who has knowledge of national labour laws is recommended. Redundancy payments and other compensation may be appropriate, or obligatory by law.

Above all the process should be fair, and perceived to be fair. Managers should ensure that at all times there is clear communication about the process, and consultation where possible.

It is good practice for a manager to debrief all departing staff individually, particularly if they may have been subject to considerable stress. This enables the staff member to express any opinions or needs they may have. The manager can then address any needs as appropriate, and record any lessons for ACT to learn, while thanking the staff member for their service.

2.8.4 Staff handover

When managers or staff members with security responsibilities are unavailable due to absence or leave, s/he must delegate those responsibilities to a competent replacement. The responsibilities should be clearly explained, and understood by the replacement. This should also be communicated to the organisation at large, and all staff should be able to reach the functioning senior manager or Security Focal Point in the event of an emergency.

2.8.5 Staff records

ACT organisations and programmes are advised to keep up-to-date records of staff and their dependants. When new staff members are recruited ensure that at a minimum a copy of the employment contract and contact details to their next of kin are regularly updated and kept in a safe place, in some circumstances, your agency may want to also keep a back-up of this information in a secure, off-site location.

2.8.6 Stress

Staff should be aware of the dangers of excessive or prolonged stress, and watch for signs of it in their colleagues. In addition to risks to health and to work quality, 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 staff member is suffering from it.

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

Different types of staff may show different signs of stress, because of cultural or personality differences. Managers should set up work and living arrangements in such a way as to minimise stress and its effects. See Annex Q for more details on prevention, diagnosis, treatment and management of stress.

Within certain limits, the ACT member is encouraged to cover the cost of counselling for staff who have suffered stress as a result of their work, where this is appropriate and possible.

2.8.7 Rest and Recuperation (R&R)

Because humanitarian and development work can be stressful, especially for programmes and agencies operating in high risk environments, it is important for ACT members to develop a written R&R policy. Proper implementation of the R&R policy ensures that staff receive adequate time to rest and maintain their physical, emotional and psychological well being, and thus keep up their internal resilience and capacity for sound judgement. R&R policies vary by country and type of conflict, but a policy should balance the employees' need to maintain their well being with the need for the programmes to retain full operational capacity.

2.9 Relationships with other organisations

Good security management requires a good understanding of the local context and the key actors within it, with a special focus on the actors/ stakeholders/ relationships that influence our programs. These can include:

- Partner organisations
- Local authorities
- Local security forces
- Other relief and development organisations
- The UN security system, if present
- International military forces, if present
- International police force, if present
- Embassies

These relationships can be useful, depending on the circumstances, for the following purposes:

- Explaining the organisation's role
- Making clear the principles on which the organisation's work is based
- Increasing the organisation's security by winning greater acceptance for its work
- Obtaining any necessary permissions
- Establishing a mutually respectful relationship which may be helpful if lobbying is needed in future
- Obtaining any relevant information on the general situation
- Sharing security-related information with other relief and development organisations. In some cases it is helpful to organise systematic collation of security-related information, including security incidents, on a collaborative basis between relief and development organisations.

2.10 Relationships with military and police forces

ACT members should ensure that their contacts with the authorities, and especially with security forces, do not compromise their independence – either real or perceived.

If there is more than one security force, perhaps on different sides of a conflict, the senior staff member should decide whether to establish contact with all security forces, to show transparency and impartiality, or whether there is a good reason to avoid contact with one or more of them.

In cases where the security forces are oppressing the population or are unpopular for other reasons, local people should be given no reason to suspect that ACT members are close to, collaborating with or tacitly supporting the security forces. In these cases it is usually wise to avoid frequent meetings, social contact, joint statements or any other activity with security forces which could cause misunderstandings, since they could be dangerous for the agency and possibly other ACT member organisations. For agencies working in such environments, it is advisable to provide relevant staff with training in civil-military relations and coordination.

ACT security policy does not permit possession of, or handling weapons, explosives or ammunition when travelling, in the field, or when representing ACT members without authorisation from the relevant HQ.

The transportation of armed personnel (security forces, military, police or guards) in ACT vehicles is not recommended as it could put staff at greater risk. If, for exceptional reasons, a country manager thinks it necessary to use armed escorts, permission should first be obtained from his or her headquarters. In the case of a joint ACT security plan, the ACT forum members should be consulted. If this is not possible, they should be informed at the first opportunity. Whenever practicable, the escorts should travel in a separate vehicle. For additional advice, please refer to the ACT adopted paper: SCHR Position Paper on Humanitarian-Military Relations (2010) (http://www.ACT Alliance.org/resources/policies-and-guidelines/ghp-principles-of-partnership).

2.11 Public statements and media

Handling the media well is often a vital part of managing external perceptions that, in turn, can positively or negatively our security. Public statements may increase threats, reduce them, or alter them in some other way. Before making a public statement, carefully consider the security implications. Is the statement necessary? Which groups might be listening? Which groups could be affected in security terms? What interpretations or misinterpretations could be put on the statement? Have you allowed for cultural and religious perspectives? Can you reduce any potentially negative consequences and increase the positive ones, while still saying what you need to say?

Most importantly, before any public statement is made by an ACT member on a topic or situation, the person or agency making the statement must consult with the staff operating on the ground in the affected country to ensure that they authorise the communication and should not be placed at risk.

In short, does the likely benefit of making the statement outweigh the risk of doing so? Sometimes, the risk of not making a statement may be greater than the risk of doing so – for example if a false rumour about an ACT member needs to be squashed by a quick, accurate and appropriate statement to the media.

In general, you are also advised to remain aware of what the local media are saying: This enhances your understanding of the local situation, and enables you to assess the evolving security environment. Nominate a colleague who speaks the language to monitor the media and pass on relevant summaries to the Security Focal Point or equivalent so that this information can actively influence security decision-making. Additional advice is in Annex H.

2.12 Equipment

All staff and consultants should receive the equipment necessary for their security. The individual ACT member's Security Plan (see 2.5 and Annex N) or the joint ACT forum security plan should identify what equipment is necessary for each agency, staff member, vehicle, and property.

For general advice, suggested equipment checklists for individuals, for teams and for vehicles can be found in Annexes 8, 9 and 42 of the ECHO Generic Security Guide (available free online in English, French, Spanish and Arabic, at http://ec.europa.eu/echo/policies/evaluation/security_review.htm. Also see relevant sections in these Guidelines.

2.13 Regular reporting

Good quality regular reporting is vital for good security management. Monitoring the situation and making appropriate adjustments depends a lot on having the right information: Situation (sitreps) and incidents reports are a good source of information. The frequency and content of situation reports (sitreps) depends on each organization – Annex P gives a standard format. Managers should coach their staff, where necessary, in writing good quality, succinct reports.

Incident reporting is different from regular reporting: see the chapter on Essential Aspects of Incident Management and Annex F.

Back to TOC

3. Essential Aspects of Prevention

Users and Usage: This chapter covers various topics with the aim of assisting ACT members and staff with preventing security incidents. Since 60% of NGO security incidents occur while staff are travelling, the chapter starts with this critical area for NGOs to manage better. For managers and Security Focal Points responsible for vehicles and transport, section 3.1 gives practical checklists. Section 3.2, covering journey planning, preparation and procedures, is for all travelling staff and visitors. This should be used in conjunction with the basic personal security advice in Annex K. Managers and Security Focal Points may use that section as a starting point to create Standard Operating Procedures/ guidelines and contingency plans for staff and managers (2.5 and Annex N). Section 3.3 is for ACT members and staff who might face checkpoints, need convoy procedures and cope with travelling in armed conflict areas.

Section 3.4 deals with health and hygiene precautions, as such it should be read by both staff and managers. Section 3.5 addresses office and accommodation security. Since these are everyone's responsibility, then all are encouraged to read it. Additional information, specifically for managers, can be found in Annex Y. In section 3.6, there is a list of good fire safety precautions for managers and Safety/ Security Focal Points (staff can refer to Annex C for fire response advice). Sexual and gender-based violence (SGBV) preventions that an organization can take to protect its staff is addressed in Section 3.7. For individuals and managers of staff, there is information about response and reactions to SGBV in section 4.6.

Section 3.8 is a brief introduction to the topic of guards for managers: More details are given in Annex D. Regarding financial security, Section 3.9 reviews some of the staffing and procedural issues that managers may have to deal with. In an age when information is "king", section 3.10 touches upon some of the information security issues and questions facing NGO managers.

3.1 Vehicles and Transport

Vehicles are working tools, a means of transportation and in insecure environments a means of escaping danger. Therefore management should ensure that the guidelines of vehicle management are practiced and followed by all.

3.1.1 Documentation

Each organisation owned and/or operated vehicle should contain the necessary documents denoting:

- Ownership
- Registration
- Insurance
- Any other papers required by the local government.

All documents should be current and be kept valid (timely renewal).

3.1.2 Vehicle logbook

Vehicles must be regularly serviced to prevent breakdowns. Timely and proper maintenance is extremely important, especially in areas of conflict. To help ensure that each vehicle is properly maintained, your organisation should have a logbook for each vehicle, to be kept in the vehicle at all times, with a pen in working order attached to it. The vehicle logbook is used to record:

- Trips by date and time, and the total distance in km of each trip

- Daily mileage or distance in km
- Inspection/check-up and control: dates and items/aspects checked
- Maintenance schedule
- Repairs

The logbook should be used in combination with a Field Travel Authorisation form (Annex V), which provides all the details of each trip, such as the destinations, check points passed through, dates and hours, and the total distance in kilometre or miles for each trip.

Prior to leaving premises, each vehicle should be checked:

- To ensure the maintenance schedule has been respected.
- To determine all the necessary documentation is in the vehicle and that it is valid (up to date) until and including the expected date of return at the duty station.
- To ensure the required equipment is in the vehicle.
- To ensure there are no illegal items or substances on board.

3.1.3 Inspections

The items to be checked by drivers or staff members operating the vehicles during daily and monthly inspections include:

- Fuel level
- Oil level
- Radiator water level
- Brake fluid
- Power steering fluid
- Fan belts
- Battery fluid
- Lights: headlamps, tail lights, blinkers and back-up
- Tire thread and tire pressure
- Spare tire
- Tools
- Windows and doors
- First Aid kit
- Vehicle documents
- Cleanliness of interiors

Supervisors should inspect vehicles once a month to ensure compliance with maintenance.

3.1.4 Servicing and maintenance

- May be done by qualified staff. If serviced by staff, then vehicles should be checked by contracted mechanics at least every three months.
- May be done by contracted mechanics, but in high conflict situations, ensure mechanics have security clearance.
- Items to be regularly serviced every three months 4,500 km or 3,000 miles depending on the environment:

  - Oil and oil filter
  - Fuel filters
  - Grease
- Repairs should be completed by qualified mechanics.
- Vehicles should be inspected by competent staff or trusted competent contracted mechanics before travelling long distances or on excursions outside of major cities, especially in zones of conflict.

3.1.5 Vehicle Equipment

Each organisation-owned and operated vehicle should contain the following items:

- Seat belts
- Owner manual
- Spare tyre and tools to change tires.
- A set of tools consisting of:
  - Flathead screw drivers (sizes 1 & 2)
  - Philips (star) screw drivers (sizes 1 & 2)
  - Pliers (one)
  - Channel lock pliers (one medium size pair)
  - A set of appropriate sockets
  - Feeler gauges
  - Wire brush
- Spare parts
  - Extra fan belt
  - Extra radiator hoses
  - Tire gauge, tire pump, tow rope, shovel, jumper cables, flares, reflectors and/or flags
  - First Aid kit (Annex O)
  - Fire extinguisher

In zones of conflict, each vehicle should carry

- Extra fuel in proper containers
- Three days food/water rations for each person
- Radio equipment

3.1.6 Motor vehicle operation

- Anyone operating the organisation owned or rented vehicle should have a proper, accountable driver’s license.
- Each passenger position in the vehicle is required to have a seatbelt
- Each passenger is required to wear a seatbelt.
- Driving while under the influence of alcohol or drugs is expressly forbidden and should be grounds for immediate dismissal from the organization.
- Drivers should operate the vehicles responsibly and should obey the traffic rules for the country in which they are operating the vehicle.

3.1.7 Hired drivers – short and long termed

It is imperative to properly screen all drivers prior to hiring them. If possible, check with the local police, trusted Foreign Embassies, UN, or any other group who may be of assistance in background checks.

It is the driver's responsibility to:

- Complete daily inspections
- Ensure there is enough fuel in the vehicle
- Clean the vehicle
- Report defects
- Keep a log of technical check-ups and trips

It should be explained to any potential driver that the following could be grounds for immediate dismissal:

- Consumption of alcoholic beverages on the job or at any time when operating a motor vehicle.
- Falling asleep at the wheel.
- Theft of any kind.
- Use of the vehicle for personal reasons.
- Negligence resulting in an accident.

Repeated complaints of disobedience and lack of respect for the passengers he or she is transporting, be they guests or staff is a ground for warning, which may contribute to dismissal.

3.1.8 Accident Reporting

It should be the policy of the organisation to report all accidents to:

- The organisation manager or Security Focal Point
- The local authorities
- The appropriate embassy if applicable

To create an internal report of the accident, your organization can use an incident report form (Annex F).

3.2 Journey planning, preparations and procedures for staff

Preparing for a journey, even a short one, can make the difference between arriving at your destination safely or not arriving at all. Assessing the risks for individual journeys (Annex L) can help you be a safer traveller. This should be used in conjunction with basic personal security advice (Annex K) and any specific advice to address current risks. Plan and prepare for all trips to ensure your safety, the safety of others, and the safety of the mission.

3.2.1 Journey Plans and Preparations

The senior most staff person who is travelling in the vehicle should ensure that there is a pre-trip briefing. In it's most basic version it should cover:

- Destination and planned stops, using a map
- Departure and arrival times for each stop and the overall journey
- Risk assessment (2.4, Annex L and Annex W)

- Checking on the communication system: Usually this can simply be that every passenger has a local mobile phone, with the numbers of the other passengers and appropriate mangers along with local emergency numbers programmed into it. Remember to lend one to any visitors who may need it. Remember also that mobile phone networks can be switched off at no notice during a crisis or conflict so the more volatile the situation, the greater the need to have alternative communication systems.

For certain risks, the group will also need to discuss their preventive options and contingency plans. If there are checkpoints, for example, the team will need to agree, before departure, on who is the spokesperson and go over guidelines on how to behave. It is important to note that in some hostile situations, drivers can be pressured to give up information about the route plan or similar. In such environments, the agency should withhold information from the drivers in order to protect them.

While it is 'best practice' to do a pre-trip briefing for every trip, this may seem tiresome, especially in low-risk locations. Like with all security measures, you should modify the suggestions in these guidelines to suit the contextual realities. In some cases, it is enough to use less than five minutes on the pre-trip briefing and in other locations the briefing can take several minutes.

Prior to leaving the organisation's premises on any journey longer than 30 miles/ 50 km or the distance set by your organization, a journey plan should be filed with the manager in charge of transport. (In zones of conflict, a journey plan should be filed for all excursions, regardless of the distance.) Journey plans should include:

- The license plate number and Vehicle Identification Number (VIN) of the vehicle to be used.
- The names of all persons taking part in the journey.
- Proposed departure and arrival times
- Planned stops
    - Estimated times of arrival at each stop.
    - Estimated times of departure from each stop.

3.2.2 Journey procedures

A basic procedure that NGO's ought to follow, but too often do not, is to require staff to inform the appropriate office or base before starting on a journey and upon arrival at their destination and in some circumstances to report back at pre-defined intervals. In high-risk/ conflict zones, security check-ins should be conducted on an hourly basis and prior to and after passing through any police or military checkpoints. The office or base needs to take action if the party fails to check-in on time.

To ensure that each journey is for a good reason, and that staff are properly prepared for it, your organization may want to establish a travel authorisation process. It could be as simple as emailing the responsible line-manager before a trip. Whereas, in higher-risk countries, it may be wise to require a Travel Authorisation form (Annex V), which also acts as a route and communications plan to provide to the office or radio room. Whether such a system is necessary is at the discretion of the senior manager, who should include the requirement in the Security Plan.

If permissions for travel are required from local authorities, leaders or groups in insecure areas, then great care should be taken to ensure that those permissions are obtained, and the relevant documents carried by those travelling. In particular, clearance for flights, for crossings of lines of conflict, and for journeys through insecure areas should be rigorously checked by a responsible manager before travelling. Failure to do so can be extremely dangerous.

Note that passengers may be asked to show the contents of any personal bags to ensure no illegal items are contained in them. This is not to offend – the issue is that if contraband is found, everyone in the vehicle and/or on the journey has a problem.

3.2.3 Visitors and others travelling under the ACT members' auspices

The senior manager of the hosting agency is responsible for the security management of all visitors to that country. When people who are not employed by an ACT member are travelling under its auspices, or are given a ride in the context of partnership and good offices, they should sign a Traveller's Disclaimer Certificate (Annex X) and hand it to the leader of the party travelling before departure.

Employees and/or consultants with the local partners of ACT members should also sign this certificate if they travel in an ACT member's vehicle.

3.3 Guidelines for key travel threats

Not all ACT members face checkpoints, need convoy procedures and cope with travelling in armed conflict areas. But, for those who might or currently do, then below are generic guidelines that should be modified for your location. For example, your Security Focal Point may get to know the commanders and soldiers of the checkpoints that staff regularly cross, in order to gain acceptance of your organizations work and, on a practical level, get an agreement on quick processing of your agency's vehicles. In the contextualized guidelines, advice and procedures can inform staff of the local requirements (2.5 and Annex N). At the Personal Security Workshop (Annex S), the context may require that you highlight the dangers of leaving the planned path or roadways and/ or to stress that routine routes, at routine hours and days, increase the chance of victimisation.

3.3.1 Checkpoints

It is extremely important to recognize that there are different types of checkpoints. Under normal conditions, checkpoints are used to verify the safety of the vehicle, the authority of drivers to operate vehicles, to look for stolen vehicles and to verify vehicle documentation.

In insecure areas, checkpoints are established to identify vehicles and personnel and to determine the reason for transiting the area. These checkpoints also serve to detect the transport of illegal weapons, explosives and combatants.

Here are some basic rules to help you through checkpoints.

- Before travelling, check with others to determine any local checkpoint procedures in the area to which you are travelling.
- During the approach, quickly appraise the situation and choose a response:
  - Proceed to the checkpoint if everything looks appropriate.
  - Turn around (if this still possible at that point: keep in mind this may endanger you).
- Determine a spokesperson for the vehicle or convoy before approaching a checkpoint and let only that person be the sole person to speak for the group.
- Take off sunglasses, if applicable, before the approach.
- Turn off the radio or tape player.
- If stopped at night, turn off headlights and turn on the interior lights as you approach. This is done so the police or military can see you are not a threat.
- Stop if required to do so (recognized NGO vehicles may be waived through).
- Be friendly, polite, cooperative and alert
- Keep in mind that these people are usually armed and have the authority to ruin your day.
- Keep in mind that the checkpoint holders may be under the influence of drugs or alcohol.

- Provide all documents as requested but do not hand them over (unless you have to), as you may not get them back. Use copies if acceptable.
- Keep your hands visible at all times. Do not make sudden or furtive movements, like reaching in a jacket where they think a gun might be hidden.
- If vehicle and personal belongings are searched, watch closely to ensure nothing is stolen.
- As you pass through any checkpoint, keep a reasonable distance between vehicles in case one vehicle encounters problems, others may escape or call for help via radio.

3.3.2 Convoys use and procedures

Convoys have their advantage and disadvantages: Weigh these seriously prior to arranging convoys. On one hand, there can be safety in numbers. On the other hand, one should consider the image projected and the attractiveness of the target. By considering the security implications, you might decide that it may be safer to break the convoy into smaller, individual segments.

If convoys are used:

- Limit the size of the convoy to no more than eight vehicles.
- Determine a convoy leader.
- Check with local authorities to see if special permission is necessary to travel in this manner.
- If possible, reconnoitre the route(s) prior to departure.
- Prepare contingency plans:
    - Determine what to do in the event of one vehicle breaking down.
    - If a broken down vehicle is left behind, consider the security of any person/s left with it and if necessary consider leaving it unattended pending recovery.
- Do not travel after dark.
- File a journey plan.
- Have a vehicle recovery plan
- Decide on the position of each vehicle in the convoy.
    - Place slower vehicles in the front of the convoy.
    - Place one radio equipped vehicle in the front (second position) and one in the back (next to last). If only one vehicle is radio equipped, place it in the back.
    - Medical units, if included, should be placed towards the middle or rear.
    - Vehicles carrying spare parts should go in the middle or back of the convoy.
    - Place the convoy leader in the front radio car.

Convoy procedures:

- Have all vehicles arrive at the departure point two hours ahead of time.
- Drivers should be instructed to keep a specified distance between vehicles. The distance should be no less than 30 feet or about 10 meters.
- Each vehicle should be inspected:
    - For fuel levels
    - For mechanical reliability
    - For documentation
    - For required equipment
    - For contraband

NOTE: Written documentation of the inspection should be on file with the transport manager prior to the convoy's departure.

3.3.3 Armed Conflict: Shooting, Shelling and Bombing

In conflict zones or in highly volatile areas, it is possible to be caught in a combat situation. Your response to combat situations may depend on whether you, your vehicle, or your organization is considered a target for any of the combatants. Chances are, you personally, are not a target. Nonetheless, you could be in danger.

If shooting is encountered:

- Drive away if the road is clear. Do not wait to see if they are aiming at you.
- Passengers should get as low as possible.
- If the shots are fired in front of you, turn around to indicate a non-threatening manoeuvre. Be cautious, the sides of the road may be mined.
- Keep in mind that a moving target is difficult to hit. Speeding while driving off is not necessarily going to provide protection. It's more important to drive with care when leaving, to avoid wrecking the vehicle.
- If surrounded by shooting, turn off the engine and, if time permits, remove the radio. Seek cover or concealment. Remember ditches may be mined.
    - Concealment hides you, but does not protect you from bullets.
    - Cover hides you and protects you.

If shelling or bombing is encountered:

- Stop, take the radio/means to communicate if feasible, and take cover as far from the vehicle as possible.
- Stay behind cover until you are sure the danger is past.
- Go back to your vehicle and try to establish radio contact, if possible.
- Leave the area immediately.

3.4 Health and Hygiene Precautions

In ACT forums, hold a session on health and ensure that all ACT members are aware of the health risks. As a member of an ACT Forum, stress how important it is that everybody respects health precautions such as boiling and filtering water, using malaria prophylaxis, keep vaccinations updated, etc. ACT members should encourage staff and visitors to consult their doctor or medical professional for detailed advice on health, hygiene, first aid or other medical matters. National ACT members should encourage their staff and the staff of their local implementing partners to follow the health safety precautions their ministry of health promotes, or seek advice from medical NGOs and INGOs working in the area. During the Security Foundation Course (Annex R), sources of further information can be given to staff. These could include:

- International SOS website www.internationalsos.com
- World Health Organisation: see the section on International Travel and Health at www.who.int/ith
- Helpful travel health information website from the UK National Health Service, at www.fitfortravel.nhs.uk - see particularly the A to Z Index
- The Traveller's Good Health Guide (2002), by Dr Ted Lankester, who is also one of the founders of InterHealth (www.interhealth.org.uk).

In these Guidelines, Annexes G (field first aid), I (medical evacuation), O (contents of first aid kit), W (risk assessment) might be relevant.

3.4.1 Health precautions

Healthy staff tend to be more efficient, alert and safe. Therefore, it is vital that NGO staff take good care of their health and are rigorous about hygiene and other preventive measures. Typical health precautions include:

- Malaria precautions are essential, in areas where malaria is a risk. Malaria can kill, and often does. Take care to prevent mosquito bites. Precautions against malaria include:
    - Wear long sleeves, trousers and socks in the late afternoon and evening, to prevent bites
    - Wear insect repellent on any exposed areas of skin
    - Use a mosquito net correctly when sleeping
    - Burn anti-mosquito coils or tablets to kill mosquitoes inside buildings
    - Fit anti-mosquito netting to doors and windows
    - Take the appropriate malaria prophylaxis, on the advice of your doctor
    - Site buildings away from mosquito-breeding areas
- Vaccinations against serious diseases. Some countries require appropriate certificate of vaccination as part of entry requirement
- Verify the quality and capacity of local medical facilities. Ensure that all your staff knows which medical facilities can be trusted and where they are located. A medical NGO may be able to provide emergency cover.
- Precautions against HIV/AIDS, including
    - Availability of clean needles and syringes for medical purposes
    - Appropriate and responsible sexual behaviour
- Protection against the sun. Wear a hat, long sleeves and long trousers or skirt, and use sun protection cream.
- Avoid dehydration: drink enough. Carry a water bottle if necessary.

3.4.2 Hygiene precautions

- Clean water supply. If clean water is not guaranteed, filter water and boil for 5 minutes to make it safe for drinking.
- Keep a spare stock of water in case of failure of supply.
- Keep a stock of water purification tablets.
- Ensure food is sourced and prepared correctly.
- Wash hands frequently, and always before meals and always after using the toilet, for 20 seconds or more with soap and warm water. Do not accept a wash bowl in which several people wash hands before it gets changed.
- Ensure cooks wash their hands frequently while preparing meals and always after the toilet, and ensure there is always soap and running water at hand for them (see previous).
- Watch the cooks and kitchen personnel's health and check their vaccinations for validity. Be prepared to pay to get them updated.
- Ensure kitchen, washing and latrine areas are kept clean.
- Dispose of rubbish effectively.

Avoid eating fruit or vegetables that have not been thoroughly washed in clean water, and peel fruit after washing, using a clean knife, and cook most vegetables at least ten minutes.

3.5 Office and Accommodation Security

The senior management team is responsible for ensuring that all offices and accommodation are sufficiently secure. This is often delegated to the Security Focal Point. That said, it is not only the SFP's and guards responsibility to ensure office and accommodation security: All users are responsible.

This section is primarily focused on information that staff need to have. For security managers, an additional resource can be found in Annex Y, which covers the physical and procedural aspects to site security and provides a site survey form/ site security checklist.

3.5.1 Office Security

The type of information that the management team can provide staff with includes:

- Understand and follow the system for ensuring that visitors 'report in' and follow your visitors to the exit when their business is concluded
- If you see an unknown person without a purpose in the office, politely introduce yourself and ask her/him if you can be of help to the person
- Always lock the door to your room or office before leaving the office
- Everyone is responsible to close the windows and lock the outside doors of his/her room when leaving. The last person to leave the office should still check all the rooms before going
- At night and on weekends, only agency staff should be allowed to enter the office
- Know where the following materials are available and how to use in case of emergency:
    - Medical kit
    - Fire extinguisher
    - Blankets/mosquito nets
    - Dry biscuits
    - Sanitary and potable water
    - Water filters and chlorine
    - Reserve of gas for generator

The ECHO Generic Security Guide (available free online in English, French, Spanish and Arabic, at http://ec.europa.eu/echo/policies/evaluation/security_review.htm is good additional resource for Security Focal Points and managers. It has useful advice on building security in annex 1 categorized by the important factors of:

- General location
- Physical security of the building
- Local infrastructure
- Arrangements for receiving visitors
- Identity of the owner

3.5.2 Accommodation Security

Selecting a safe residence

- Find out about the area’s safety. If you are in doubt about the security of your residence, ask for advice
- Preferably choose a place where there are multiple ways to get to and from your residence. (e.g. living at the end of a dead end street severely limits your escape options)
- Seek advice on physical security (ie secure gates, high fences, not having accessible roof areas)

Basic daily security measures

- Make sure that closets, bathroom and balcony are not occupied
- Make sure that doors and escape routes are cleared
- Make sure that you've got a flashlight in your room in case of power cut
- Turn lights on after closing the curtains
- Hide valuables

Hotel security & safety

- Seek advice when choosing a hotel. In general larger hotels have more elaborate security but can be a target
- If the hotel staff say your name, organization, room number or other personal information loud enough for others to hear it in the lobby, then feel free to request a new room
- If possible, book a room between the second and seventh floors to prevent easy entrance from outside and low enough for fire equipment to reach in an emergency
- Choose a room near the elevator to avoid having to walk down a long, empty corridor
- Upon arrival to your room for the first time, check the quality of the door, quality of locks on door and windows, make sure the phone works, and have a quick look around
- Find out the nearest fire escape. Walk from your room counting the doors to the fire escape. Imagine how you would reach it if you were crawling in darkness and smoke. Read the hotel's fire instructions
- Use a rubber doorstop for added safety (we recommend that you carry one as part of your luggage). If not available, use a chair to jam the door
- If you are attending a conference, remove your name tag as soon as possible to avoid being identified
- If someone knocks on your door, call the front desk to double-check – don’t assume the person is who he/she claims to be. Always use the deadbolt and chain
- Beware of individuals posing as police or security officers who want you to accompany them to another location. Obtain proper identification and call the local police to verify. Ask the hotel desk to assist you in verifying identities. Before you accompany them, call your line-manager or Security Focal Point and advise him/her of the situation
- Do not enter your room if you find the door open or unlocked. Return to the desk and ask someone to accompany you to your room

3.6 Fire precautions

Fire poses a significant risk to health and safety, especially in countries where there is no fire brigade, buildings are not built to minimize fire hazards, and few people have fire-safety training. Fires in offices, warehouses, and residences can prove catastrophic and the threat of fire should be addressed in all safety and security risk assessments (Annex W). Most fires start small and can be extinguished if detected early. The best method for fighting fires is prevention through regular inspections, staff training and properly maintained fire-fighting equipment in all facilities.

All buildings should be checked for fire safety, including ensuring that staff can exit easily. Simple fire safety measures such as smoke detectors and fire extinguishers save lives. See Annex C for suggested fire safety procedures. ACT Alliance members are strongly encouraged to check each other's premises for fire hazards in a peer review manner.

To minimize the risk of fire, the management team should:

- Assess all buildings for fire safety
- Ensure there are sufficient fire escape routes
- Emergency exits should have emergency exit keys, preferably glassed-in in a box, near to the exit but hidden from exterior view
- Designate fire assembly points outside all buildings
- Fitting smoke alarms Accommodation buildings should normally have smoke detectors in all rooms except bathrooms and kitchens.
- Equip buildings, and vehicles where necessary, with fire extinguishers
- Train staff in the use of fire extinguishers
- Rehearse an evacuation of the building with regular fire drills and alarm testing
- Establish a system of fire wardens, where appropriate
- Ensure all staff know the procedure for calling for help in a fire (bear in mind that there may be no fire brigade).
- If you don't have a fire alarm procedure, introduce one and train your staff in it immediately.
- Store flammable materials correctly, and away from buildings

3.7 Sexual and Gender-based Violence Prevention

Sexual and gender-based violence (SGBV) can be found in every society and can be particularly high in complex emergencies, for the affected population but also for your staff. SGBV has both severe physical (STD, HIV/AIDS, unwanted pregnancy) as well as emotional health impacts.

How to reduce the risk of sexual and gender based violence? Adequate response to the threat of work related SGBV comprises of:

- Coordination
- Monitoring
- Protection

3.7.1 Coordination

Coordinate prevention with other agencies and include assessment and SGBV prevention directed activities in programming as well as in each security plan.

3.7.2 Monitoring

The security officer should keep updated on the level of SGBV in the country or in the area. There should be a trusted manager that staff can report sexual harassment and violence to, in confidence, regardless if it's another staff member (section 2.8.2) or someone external to the organization but work-related.

3.7.3 Protection

The protection of staff from SGBV is often linked to the protection and security of the beneficiaries of the programme. All staff should be trained in international standards and in the ACT International staff member Code of Conduct on the Prevention of Sexual Exploitation, Abuse of Power and Corruption. This Code of conduct should be signed by all staff and visitors. Rules for handling breach of Code of Conduct including firing of personnel should be well known to everyone in the program.

For individuals and managers of staff, there is more information about response and reactions to SGBV in section 4.6.

3.8 Guards

Guards need careful briefing, equipping and managing. Before hiring guards, consider the advantages and disadvantages thoroughly as there could be hidden implications (Annex D).

The use of armed guards or escorts by ACT Alliance members is strongly discouraged as having them could put lives in danger. Use of armed guards should only be considered in exceptional cases and local context where it is assessed that the ACT member is able to function responsibly with them and would not be able to function securely without them. The office requiring armed guards should seek the prior approval of their head office management. If permission is granted, the most senior most manager is responsible for ensuring that the guards fully understand and obey their rules for opening fire. These rules should conform to applicable local and national laws.

Annex D gives advice on recruiting, inducting, briefing, equipping, training, and managing guards, as well as when hiring private security companies or deciding on armed guards (also refer to the ACT adopted paper: SCHR Position Paper on Humanitarian-Military Relations (2010) available at: http://www.actalliance.org/resources/policies-and-guidelines/ghp-principles-of-partnership/153-SCHRPositionPaperonHumanitarianMilitaryRelationsJanuary2010.pdf/view

3.9 Financial security

Money attracts criminals and opportunists. Therefore, poor control over cash and other valuables increases security risks, negatively affecting programs and staff. External generic advice on financial procedures, including simple guides to NGO accounting, can be found at www.mango.org.uk and in the ECHO Generic Security Guide http://ec.europa.eu/echo/policies/evaluation/security_review.htm.

In general, rushed financial transactions are more vulnerable to errors and fraud. Wherever possible, insist that all normal procedures are followed without exception, unless someone has the explicit authority to overrule common procedures.

3.9.1 Staff

Recruit a properly trained and briefed bookkeeper, accountant or financial manager, appropriate to the size and type of programme, from the very beginning, when the operation is still in the planning stage. As far as possible, separate duties so that always more than one staff member is required to perform any transaction. This helps prevent collusion with outsiders. Bear in mind the potential danger posed by any disgruntled ex-employee.

3.9.2 Cash procedures

Keep the use of cash to a minimum, preferring bank transfers or cheques where possible. Minimise amounts of cash held by staff and in the office. Let it be known to all staff that the policy is not to hold large amounts of cash. Take appropriate precautions when cash is being collected from the bank. Only pay wages in cash if absolutely necessary. In such cases, stagger payment over several (non-consecutive) days to reduce amounts of cash withdrawn from the bank and held in the office at any one time. Ensure that all staff know that they should not risk their lives to protect cash and valuables.

Procedures

- All cash should be kept in a safe.
- Only two people should know the combination to the safe
- Cash is to be removed from the safe only for transfers or transactions.
- Transported cash:
    - Should be concealed upon an individual's person or in an appropriate bag such as a briefcase or backpack.
    - Large quantities of transported cash should be divided up into smaller bundles and transported by additional persons
    - Persons transporting cash on repeat occasions should avoid using the same times and routes.
- Do not refer to cash or cash transfers in a way that the information can be overheard, gleaned or otherwise obtained by outsiders. Information should be available only to those who need to know. It is in the best interests of all to reduce the number of those who should know to the strictest minimum.
- For additional considerations during an emergency, see 5.2.4 "Security risks categories linked to situational indicators and program decisions for each phase of the build up to an emergency situation."

3.9.3 Secure storage

Keep cash and valuables in appropriate safes and cash boxes. Safes should be secured to the wall or floor. The cashier should be in an area away from reception and public areas of the office. Restrict access to the building and rooms where valuables are kept. Do not keep all valuables in one place.

3.10 Information security

In an age where information is as powerful as a 'king', there are many areas of information security that NGOs should be aware of and take appropriate protective measures. Some of the issues and questions facing NGOs include:

- Which staff need what information, especially concerning sensitive information?
- How to balance the need for internal sharing of information with keeping discretion?
- What is the best way to protect computers, paper documents, emails, etc from those who may cause harm to staff, beneficiaries, and the NGO's reputation?
- During an evacuation, will we know which documents need to be destroyed and can we do this quick enough?

These are just a few of the considerations – for a more complete discussion please refer to the ECHO Generic Security Guide http://ec.europa.eu/echo/policies/evaluation/security_review.htm.

Back to TOC

4. Essential Aspects of Incident Management

Users and Usage: As there are different aspects of managing a safety or security incident, this chapter applies to different readers. The first sections are primarily for the senior management team: Staff need this information but it is up to the management team to package and reinforce the messages. The second set of sections cover responsive advice for key threats, as such, these sections can be read by staff in addition to managers. That said, the advice here is generic and it is preferable that staff receive a final version that has been appropriately modified and adjusted.

This chapter deals with incident management but it is important to underline that many organizational measures should be in place before an incident. For example, staff should know how to report an incident. Many NGOs assume that their competent staff will use common sense to relay vital information. But the reality is that a staff who has been performing first aid on a bloody colleague and watched the driver die in the car crash will be in shock. But, still they need to communicate essential information in order for the agency to send help. Section 4.1 lists the different types of incident reports and provides a format for these. Section 4.2 underlines the importance of acknowledging and learning from 'near-miss' incidents. For managers tasked with learning from incidents and writing the full report, section 4.3 provides questions that might assist you with the analysis and adjusting procedures. For those who might investigate serious security incidents, section 4.4 gives a few points.

Section 4.5 is for managers who might be called to be a part of the Crisis Management Team. Since dealing with a crisis requires dealing with multiple issues. Use sections 4.6 (Sexual Violence) and 4.7 (Kidnapping) to learn about key issues and advice on how to deal with them. These sections are primarily for managers to contextualize appropriately before making them a part of the Security Plans distributed to staff. But, concerned staff can already read the generic points here.

4.1 Reporting security incidents

The senior most staff member responsible for security should be informed of any security incident as soon as possible: Staff need to know this so that they automatically contact this person or their line-manager. If the security incident is serious (for example death, serious injury, kidnap, violence, sexual violence etc) the security or line- manager should inform the country director/ manager. The Security Focal Point on the HQ level (if applicable) should also be informed immediately. In most cases, the HQ level staff should support the country team to respond to the serious incident. However, in some cases, this person can take the lead.

A standard incident report format helps to ensure a quick and effective response to a security incident. It provides the essential information in a logical order, allowing managers to make sound decisions. It is important that an incident report states the facts and that any analysis or opinion is either clearly identified as such or left for the next stage of incident inquiry and analysis. Do not confuse fact and opinion. There are three types of incident report, 1. the immediate, 2. the follow-up, and 3. the full incident report.

4.1.1 Immediate incident report

Immediate incident report, sent as soon as safely possible (minutes or hours following the event – depending on when it is safe to report), often by phone or radio. It is done by staff who are directly or indirectly affected. It alerts colleagues to the incident and enables them to respond. If there is no time to send all of the above while the incident is ongoing, send whatever is possible – e.g. "Ambush!" – which gives colleagues some idea of what is happening. They may be able to work out how to respond, and how to avoid the same danger, from even the briefest of information, and this could save lives. For most incidents, however, call signs are the best way to communicate effectively.

4.1.2 Follow-up incident report

Follow-up incident report, giving more information as soon as possible, usually hours to 1-2 days after the event. Written is preferable, but it may be by radio or phone if necessary. Normally, the affected staff, sometimes with a manager, writes this report. Though in some cases, the manager submits the report.

4.1.3 Full incident report

Full incident report, written within a week, if not a few days after the incident. It informs what happened as well as analyzes probably reasons why it happened. Often, at this stage, the Security Focal Point or line-manager writes the report, usually in consensus process with others like the affected staff.

For all the incident reports they aim to provide answers so that the organization can improve it's procedures and staff training, which increases the organization's chances to continue it's ability to work. The questions are, with small adjustments, more or less the same for the reports, the amount of details and analysis increases going up the reporting chain. The standard format is as follows:

- **What?** – What type of incident?
- **Who?** – Who was involved in the incident?
- **When?** – When did the incident happen? When was the report submitted?
- **Where?** – Where did the incident happen?
- **What has happened?**
- **What actions taken?**
- **What help do you need?**
- **When is our next communication? How can you reached and alternative means?**

It is important to train staff in these in order to make it easy for them to follow during stressful events. For example, your agency can give staff a business sized card with these questions on one side and, on the other side, two/ three numbers they can call, preferably with 24 hours/ 7 days coverage, especially if staff work in high-risk locations. That said, the affected staff may be in shock, still in some danger, or similar so all other staff and especially managers who might receive such calls need to also carry this card on them.

4.2 'Near miss' incidents

'Near miss' incidents should also be reported. A 'near miss' is where it appears that a security incident came close to occurring but didn't due to the luck or skill of staff. They spotted an ambush and turned around in good time not to be seen – for many this is a 'non-incident', it didn't happen. But, for an agency and the wider NGO community, a report about this 'near-miss' provides vital information that gives the agency the chance to learn and improve before other staff are endangered. On the hand, if the agency isn't informed and/ or doesn't take preventive actions, then there could negative consequences.

Though a 'near miss' incident in some cases does not require an immediate or follow-up incident report, it should always result in a full incident report, so that lessons can be learned. It may reveal a weakness in security procedures, or new information about security threats.

4.3 Analysis of incidents and adjustment of procedures

After an incident, the relevant managers and staff should think through the events and consider whether there are any lessons to learn. For example:

- What were the causes of the incident?
- Was it deliberately targeted at one or more ACT members, or the coordinated ACT appeal programme?
- Did it have anything to do with the particular staff members themselves? (ethnic background, gender, age, religion, political or family connections)
- Should staff be better briefed?
- Should procedures be adjusted?
- Should a particular route be avoided?
- Should there be better liaison with the police or other government institutions, international organisations (e.g. UN, other NGOs) or other security entities?
- Is it safe for ACT to continue working in this location?
- What further action is required by ACT at this location, to avoid further incidents? Who should carry out this action?
- What further action is required by ACT at project, capital or HQ level? Who should carry out this action?
- Should disciplinary action be taken against any member of staff?
- Are there lessons or information from this incident to be shared with other agencies or actors?
- Are there any aspects of this incident or this analysis which need to be kept confidential? How should this be achieved?

Records of all security incidents should be kept, and analysed from time to time. Locations of incidents should be plotted on a map (though in same locations, take great care with openly displaying the map). What do the incidents reveal about the nature of the local situation and its threats? Is there a pattern? Can any trend be discerned? What action should be taken as a result?

A full incident report should be the final result of this process. It gives a complete written account of the incident, and should follow this format:

- Full chronological account of the incident
- Who was involved
- Reasons for any decisions taken
- Lessons to learn from the incident
- Identification of any failure of procedures or staff, and recommendations for any remedial or disciplinary action
- Date, author, role of author, and signature.

It is important to share reports of incidents with other appropriate organisations, so that all can benefit from increased knowledge of the security situation. This has to be done timely. It’s important to note that timely sharing with others does not mean that you have to provide sensitive details – use discretion especially concerning staff’s identity. A rape survivor will not want staff and NGO colleagues knowing about the incident.

4.4 Investigation of serious incidents

An investigation should be conducted of any incident of the following kinds:

- Death
- Sexual violence
- Serious injury
- Major Fraud
- Robbery
- Armed assault
- Any other incident which, in the view of the senior staff member in-country or more senior line manager, warrants an investigation.

The investigation should be carried out swiftly, by a suitable person not connected with the incident. It should aim to identify what caused the incident, and should recommend any disciplinary action necessary. It should ensure that there is accountability for serious loss or damage to staff or property. Guidelines on how to organize an investigation can be found at http://www.actalliance.org/resources/policies-and-guidelines/complaints-mechanism/Complaints%20and%20Investigation%20Guidelines%20July%202010x.pdf/view

4.5 Crisis management

Events that can trigger a crisis management response might be:

- Death or serious injury to a member of staff
- Disaster affecting the ability of the HQ of one or more ACT members to function
- Numerous casualties, in the field or at HQ of the local, national ACT member, or at the main office of an international ACT member in the country of operations
- Communications failure affecting an important operation
- Major fraud
- Kidnap
- Imprisonment of staff member
- Compensation claim against the organisation arising out of a security incident
- Any incident which has generated or is likely to generate media interest

In the event of a serious incident, a Crisis Management Team is likely to be necessary. There are different levels and types of a Crisis Management Team (CMT) response: organizational, within the Act Alliance, and with other NGOs. Each of these can be on the local, national and/ or international levels. The degree to which the affected office calls on the support from others will often depend on their ability to manage and cope with the crisis (which, in turn, is often influenced by whether or not the agency has good contingency plans in place – Annex N). Another factor in activating additional levels is the seriousness of the event: kidnappings always requires a wider response, for example.

Some members of a CMT may be pre-identified by the nature of their position (Country Director, Security Focal Point). However it is important to strive to make sure the composition of any CMT reflects the needs of the particular crisis. For example, if kidnapping or terrorism is involved, a representative of the relevant government Counter Terrorism Policy Department and/or Police Hostage and Crisis Negotiation Unit may be co-opted onto the team.

The following functions are normally covered by nominated staff: If feasible and appropriate, then a single person may be responsible for multiple tasks.

- Communications with other levels (e.g. the field)
- Human resources issues
- Responding to enquiries from the press and public
- Dealing with insurance companies and issues
- Contacting relevant embassies
- Administrative support
- Physical support (e.g. food, drink, accommodation)

The Crisis Management Team is normally responsible for all aspects of handling the crisis (they should, of course, have received prior training – Annex U). Dealing with a crisis requires dealing with multiple issues. Just some of the key issues are covered below: Medevac (4.5.1), informing next of kind (4.5.2), fatalities (4.5.3), media (4.5.4). In addition use sections 4.6 (Sexual Violence) and 4.7 (Kidnapping) to learn about key issues and advice on how to deal with them. No other staff member should take action relating to the crisis without the approval of the Crisis Management Team.

The CMT is likely to need its own demarcated working space, of a design and size appropriate to the crisis. They will need sufficient resources and support. For example, CMT members should have their normal responsibilities covered by colleagues for as long as necessary.

When a serious security incident has taken place involving one or more ACT members in a given country, a Crisis Management Team will be set up at ACT Secretariat, including the most suitable members of the Security Working Group (SWG) can be seconded. A CMT set up at the ACT Secretariat will only happen if all the involved members request it and ACT, as an organization, may get involved.

4.5.1 Medical evacuation (MedEvac)

Details of medical evacuation (Annex I) should be included in country security plans (Annex N). This may include in-country medical evacuation to the nearest good quality medical facilities. In the case of ACT forum common security plans, this aspect must be carefully described for the different types of contracts and members (national or international) in order to avoid unrealistic promises and expectations as regards medical "rights."

4.5.2 Informing Next of Kin

If a serious event happens to a staff member, for example if they are injured, kidnapped, imprisoned or killed, it is vital that next of kin are informed quickly and sensitively. This is right in principle, and is also wise in practice, since the staff member's family may hear soon from the media. They should hear from the ACT member employing him or her first. Annex J gives a suggested procedure for informing the next of kin.

4.5.3 Fatalities

If a staff member dies while working for an ACT member agency, the following procedure is recommended:

- Confirm the identity of the deceased (mistakes do happen);
- Decide whether it is necessary to set up a Crisis Management Team;
- Nominate a senior manager at HQ to manage the issue (and manage the Crisis Management Team, if there is one) on behalf of the ACT member agency, if necessary;
- Inform the next of kin (Annex J);
- Inform other staff;

- Inform the local authorities;
- Secure the body;
- Arrange for a post-mortem examination, if required;
- Arrange for repatriation of the body, if the person is outside his or her own country. This can be a complex and difficult bureaucratic process and depends on local laws and regulations.
- Cooperate with local authorities, in the event of a police or judicial investigation
- Inform the media, if and when appropriate;
- Ensure that any compensation or insurance payments are made swiftly;
- Provide assistance if appropriate to the deceased's next of kin and/or dependants;
- Conduct an investigation into the events leading to the death. Depending on the circumstances, this may be conducted internally or independently.
- Identify any lessons to be learned from the incident and adjust policies or procedures as necessary.

4.5.4 Media

The issues covered in section 2.11 and Annex H, like stressing to staff that only a designated spokesperson is authorized to speak with the media, also apply to crisis situations – the main difference is that crisis situations require even extra considerations and skills. To these, section 4.8.1 adds some specific points for a kidnap situation.

4.6 Sexual violence

Anyone who has survived sexual violence should be treated with great sensitivity. The incident should normally be treated with confidentiality and the wishes of the person affected should be respected as far as possible. In some cases, the management team who deals with the crisis are just a few – sometimes not even the rest of the senior management not given details even though they are involved with analysis and improving procedures.

It is strongly encouraged that all incidents of work-related sexual violence be reported to the organization. This allows for appropriate support to be offered and so that steps can be taken to try to prevent future incidents. If the person affected is unwilling to report the incident to his or her line manager, he or she should feel free to report it to any manager of his or her choice, who should respect this wish that the line manager is not informed, and who should arrange appropriate support. Psychological support should always be given.

For non-work related incidents, it is up to the staff member if they want to inform the organization or not – that said, they should be encouraged to do so to get support and help prevent other cases.

The advice below is labelled if it is for staff, managers or both. As with other examples in these Guidelines, it is advisable for the Security Focal Point or equivalent to modify these points accordingly and distribute to all staff.

4.6.1 Some facts about sexual violence – for staff and managers

- Often the best way to prevent sexual violence is to follow the General Personal Security guidelines (Annex K) and for the given context, be as informed and aware as possible.
- Everyone, male or female, is a potential victim of sexual assault but women and young girls are at a much higher risk.
- Women are often blamed for the assault or violence and are accused of "enticing" the man who assaults. It is important to make sure that no one takes that track of opinion.

- Sexual violence is a crime of power and violence. Sexual contact is just the vehicle for the attacker to prove he or at times she has power over you
- Most sexual assaults are committed by an acquaintance of the victim. Opportunistic attacks are rarer but do occur and can be higher prevalence in high-risk/ conflict zones.
- Sexual assaults are the least reported of all violent crimes.
- The attacker maintains control of the victim through:
    - Psychological pressure and fear
    - Threats
    - Force

4.6.2 Response and Recovery – for staff

There is no right or wrong way to react: The choice is strictly up to the person affected. REMEMBER THE PRIMARY OBJECTIVE IS TO SURVIVE.

In-situation Response

- **Submit**: If the person fears for her (his) life, she (he) may choose to submit to the crime.
- **Passive Resistance**: Do or say anything to "ruin" the attacker's desire to have sexual contact. Tell him you have an STD such as AIDS, diarrhoea, make yourself vomit, anything distasteful or disgusting.
- **Active Resistance**: Any type of physical force to fight off the attacker, such as striking, kicking, biting, scratching, shouting, and running away.

Immediate After Response

- Contact someone you trust.
- If it is work-related, contact a trusted manager. If it is non-work related, decide if you want to inform a manager or not.
- Report it to the police, if possible: in some countries, it is not advised to report a sexual assault to the local police. The security policy for each country should describe how to deal with sexual assaults in this country and especially how women who report will be treated.
    - Understand that the police will have to interrogate you. In some countries they may not believe you are a victim. They may believe it is your fault.
    - Understand you may be taken to the hospital for an examination and possible treatment for diseases. The security policy should state which hospital one has an agreement with.
    - Understand that regardless of whether or not the suspect is caught, you will have psychological and emotional responses

Recovery

Some facts you should know about recovery:

- Remember that you are not alone. Others have also been victims, survived, and can offer support.
- May be you blame yourself. **DON'T!** The assault was **NOT** your fault!
- You are likely to replay the event over and over again in your mind and wonder what you could have done different to prevent the attack. This is normal. Make sure you have someone patient and respectful to talk to and to come back to what happened as often as you need to come to grips with it.

- Your body may go through some physical changes as it recovers and heals. If you feel insecure about these changes and if it is possible, consult a trusted physician rather than discuss them with friends or colleagues.
- You will go through an array of emotions.
    - For a time you may not be able to think of anything other than the assault.
    - You may think you are going crazy…you're NOT. Almost any reaction is normal.
    - You have every right to cry, scream or be as upset as you feel.
    - You may become angry.
    - People's reactions may hurt you…they do not understand.
- Despite all this:
    - Remember you have been the victim of a crime.
    - Remember you are a good person.
    - Remember this is a serious incident. Take good care of yourself.
    - Remember you are a survivor.
    - Remember to seek professional help if you feel you are losing control or cannot handle it alone.
- Emotional first aid is important:
    - Do whatever makes you feel better.
    - Hang on. Take it five minutes at a time if you have to.
    - Take out your feelings on your attacker. Stand in the middle of the room and scream all things you want to tell him.
- If people are reacting to your assault in a manner that hurts you or upsets you, stop them and get away from them. Even if it is your parents or your husband or wife. You come first!
- Try to think of what would be good for you and do it!
- Make yourself talk about it to at least one sympathetic person with whom you feel safe, but be careful not to share it with a large number of people You MUST talk to one person that you trust to tell your story completely and without restraint.
- Remember you are safe.
- Remember there is nothing to be ashamed about.

4.6.3 Response – for managers

Upon receiving information about the sexual assault and deciding who amongst the senior managers need to know, then the responsible managers have a series of considerations – hopefully most of them will be already addressed in the contingency plans (2.5 and Annex N). Some of the response issues for managers include:

- Is the affected staff member(s) getting proper medical, psychological and physical care? How much does the agency pay and how much is covered by the insurance company?
- What are her or his wishes?
- Who should know what and how to maintain a 'need to know' basis? Internal and external.
- Does the organizational pay for legal support?
- How much time off work does the affected staff member need?
- How can the agency prevent this from happening again?

These types of questions are in addition to the general list of crisis management issues listed in section 4.5.

4.7 Detentions and kidnappings

NGO staff members may get detained or abducted for a variety of reasons. Detentions may be the result of an alleged crime committed or because of the programs being presented in-country. Likewise, abductions may be the result of grievances over the organization's programs, politics, terrorism, ransom, and sometimes for a combination of these reasons. Sometimes the motives should change, for example, hostage situations may start out as politically motivated, but in due course, it may turn into a ransom kidnapping.

Regardless of the reason for a detention or abduction most detained persons and hostages stand a good chance of surviving the ordeal and being released. Worldwide, 90% of kidnapped persons survive, which is not to say that they do not have physical or psychological injuries to cope with afterwards. As with other security incidents, normally, staff can avoid becoming a victim by following a few preventative measures (Annex K and Annex N) and being as security aware as the situation warrants.

Section 4.8.1 looks at some of the key strategy and response issues facing managers. For staff members, section 4.8.2 offers advice on the five typical stages and your response options.

4.7.1 Kidnap Policy, Strategy and Response – for managers

If a kidnapping occurs, it is recommended to set up a Crisis Management Team immediately. Some of the issues that CMT should start considering and addressing include:

Issues
Internal Issues to be addressed (not in order)

- Distribute CMT tasks: It should be made clear at once which manager has lead responsibility for managing the incident. And, just as important, identify the administrator. Next, delegate the other roles and tasks. These basic points should be in the contingency plans (2.5 and Annex N) but because every situation is different, then it is best to quickly and efficiently make sure that all critical functions are covered.
- Start an event log, recording what, who, when, etc
- Start a list of what know/ want to know and what actions taken/ actions to be taken next
- Establish, as soon as possible, the creditability of the report/ evidence of a kidnapping. Note, it is a worldwide trend for criminals to claim they are holding (and mistreating) someone but it's just a trick to gain 'easy' money.
- Inform staff: decide who should receive what information and how often
- Communicate with HQ: decide division of labour, communication expectations, etc
- Contact local kidnapping expert and develop negotiation strategy
- Media strategy
- Family contact strategy
- Inform or not the authorities and to what extent
- Financial resources and need of other resources
- Ensure that other operations still function
- Decide on general plan for communicating and negotiating with captors
- How to cope with a potentially drawn out event?

- Conduct post event debriefing and provide physical, psychological and emotional support

External Issues to be addressed (not in order)

- Contact with captors
- Implement media strategy
- Contact victims family
- Lawyers
- Inform (or not) partners, ACT Alliance, NGOs
- Decide use of 3rd party intermediaries – embassy, police, govt, ACT Alliance, NGOs

It is important to underline, again, the importance of having your Security Plan (2.5 and Annex N) in place before a serious incident. For example, while time is valuable in a kidnap situation, it is essential to have the contact details for staff members at hand and to have already formulated policy (ie pay or not ransom and salary of staff while detained).

Policy

No official policy on how to deal with kidnappings and detention of staff of ACT members has been adopted by the ACT Alliance, so the following is only advice. ACT recommends **NOT** to pay ransom for the release of staff members. While this may seem counter-intuitive, when the goal is to release the staff as soon as possible, with as little harm done as possible. However, paying ransom will probably put other staff/ other NGOs at risk. Still, ACT members should expend every effort to affect the safe release of the staff.

Neither ACT members and their partners, nor government authorities, or the hostage negotiators should reveal the exact strategies that are being employed during the negotiation process.

ACT Alliance Support

ACT members present in the same location and country should be the first line of support. At the same time, the Alliance can provide support if necessary and useful, either through ACT Secretariat, from member to member or through the ACT Security Working Group. The Alliance can give you moral, technical and practical support, but cannot back up you up financially to pay ransom.

Expectation Management

Managers, staff (in general and specifically those covering the responsibilities of the CMT members) and the family need to know that kidnappings can time a long time: 75% of all kidnappings take between 1-50 days and then there are those cases that last years.

Media Considerations

It should be assumed that kidnappers can and will be monitoring the media coverage of an incident, which means that anything said can have a direct impact (positive or negative) on the staff person who is being held. Key details about the staff person(s) including names, languages spoken and religious background can have a dramatic impact, intentional and unintentional, on a situation. For example, if it is communicated to the media that a staff person knows the local language -- while the person may have been pretending not to be fluent -- then there could be severe and unintended consequences.

Depending on the context, family members can play a useful role in a media strategy for a kidnapping, but they should be part of a well thought out process, and ideally they should not be engaging the media independently and without professional guidance. As the organisation for which the kidnapped staff person works and with the approval and acceptance of the family, the agency should professionally assume a "media buffer" responsibility for the family. Every context is different and there may be situations where the family members could be better perceived as independent from the organisation, for example, when an ACT member may unfortunately have a poor reputation within a community or country.

Attention should be given to investigate what is known and published about a kidnapped person on the Internet. For example, a person's CV, photo or other background details could be easily accessible by the media and also the kidnappers. Awareness of this reality should be acknowledged when developing a strategy for engagement with the media.

In incidents that could receive intense media attention on an international level, the ACT member should seek support from within the Alliance as early as possible.

In additional advice for dealing with the media can be found in sections 2.11 and 4.5.4 and Annex H.

Debriefing and Follow Up Care

After a security incident, the relevant manager should debrief all staff involved as a group if possible and usually within one day of the incident. This enables staff to say anything they need to say, and helps lesson-learning.

Debriefing also allows the manager to check on the staff member's general wellbeing. The manager suggest counselling to any staff member who may need it, even if sometimes the staff member does not seem to be aware of that need and even be hostile to the idea. Some stress reactions can appear after a delay, sometimes months later. If so, staff or managers should acknowledge them and arrange counselling or other help if necessary.

Medical help may be necessary for those who have survived an incident. Anyone who has suffered sexual violence may need post-exposure prophylaxis and a pregnancy test. But there is also a risk of HIV/AIDS infection. How and what to do about this is described in detail in the ACT policy on HIV and AIDS in emergencies (http://www.actalliance.org/resources/policies-and-guidelines/hiv).

4.7.2 Detention Policy, Strategy and Response – for managers

If a staff member is detained for lawful reasons, the ACT member should support the staff while allowing due process of law to take its course. If one or more staff are detained on false grounds, the relevant line manager should make strenuous and urgent efforts to secure their early release.

The best way to achieve this varies according to the circumstances. An early priority is to visit the staff member(s) in order to check that they are being properly treated, to discover what practical assistance they may need, to reassure them and to listen to their version of events. The visit should be carried out as soon as possible by the most senior manager available, and should be followed by frequent further visits. If the detained staff member is a woman, reflect on the gender implications. It may be advisable the office visitor is female, or that the most senior manager is accompanied by a female staff member when visiting the detainee.   The detaining authorities are less likely to abuse a detainee and are more likely to release him or her if they know that there is a high level of concern from senior members of the organisation.

The relevant line manager should apply all possible legitimate pressure on the detaining authorities to release the staff member immediately. Influential officials, diplomats, church leaders, community leaders and other friends may help to add to the pressure. The line manager should decide what approach to take to the media: in some cases it is best not to involve the media, in order to resolve the matter quietly. In other cases media attention can play a vital role in a campaign to secure the detainee's release.

In this type of event, the CMT may be activated but not all members will be active. It may be that that CMT is brought together to inform the relevant managers and to devise an appropriate strategy.

But, after that, only a few key managers work on the case on a daily basis, while keeping the whole CMT updated.

4.7.3 Kidnap Avoidance and Reaction Options – for staff

There are five typical stages of a kidnapping that you need to be aware of: At each stage, you have options. Some are listed here:

Planning & Surveillance

- Vary the times, routes, etc of your daily routine
- Look like a hard target
- Report your suspicions and improve your security measures

Attack

- Make a commotion
- Escape if it does not endanger you or others
- Try to remember details about the vehicle, persons, etc

Transport

- Regain your composure and calm
- Avoid eye contact and be low-key
- Follow rules

Captivity

- Maintain your dignity and be seen as a human being
- Expect to be poorly treated with threats, violence, psychological power games
- Give and win respect
- Set goals and keep up hope
- Know that your agency, family and friends are thinking of you and doing everything they can for your release. Your main task is to keep as physically and mentally healthy as possible.

Release

- Stay low - Expect shooting
- Show your hands
- Expect to be poorly treated until you identify yourself

As mentioned in the manager's section, you need to know that kidnappings can time a long time: 75% of all kidnappings take between 1-50 days and then there are those cases that last years. If you are captured, then keep up hope because 90% of kidnapped persons survive, which is not to say that they have not sustained physical or psychological injuries to cope with afterwards. The 10% who do not survive, generally die either in the attack or release stages or because they needed critical medicine during captivity. One implication is that if you are at risk of kidnapping and you take vital medicine, then carry a small supply of medicine with you at all times.

Back to TOC

5. Suspension, Hibernate, Relocation, Evacuation

Users and Usage: Primarily for the senior management team and Security Focal Points, the questions, issues and advice below are a summary of the definitions, decisions and considerations for suspension, hibernation, relocation and evacuation. There is a matrix that gives an overview of the program decisions for the security risks categories (also see 2.3). Use these, in conjunction with Annex B, to support you when designing and implementing evacuation plans and procedures.

Definitions

ECHO's Generic Security Guide (2004; p 41) defines suspension, hibernation, relocation and evacuation as follows:

> Stopping work temporarily is commonly known as **suspension** of the programme. Stopping work permanently and leaving the area is known as **evacuation**. A middle option, involving stopping work for a considerable time and keeping a low profile to allow the danger to subside, is sometimes known as **hibernation**. A final alternative is to **relocate** some or all staff, while remaining within the country.

5.1 Decisions

Deciding to suspend, hibernate, evacuate or relocate is difficult. Evacuation is likely to be necessary when the current situation is untenable for staff, intensified by strong emotions for their personal and family's safety, as well as feelings for the beneficiaries and country. For mangers, they will have to take numerous hard decisions like bearing in mind that evacuation may expose staff to danger while they are evacuating.

There is no clear-cut formula for this decision: only managers can decide, using their judgement and taking whatever advice they think necessary. The starting point for making the "best decision" in "worst case scenario" occurs long before the onset of an emergency. Below are questions and considerations for before, during and after an emergency. It is not an exhaustive list but together with Annex B, your organization will have a good starting point.

For different organizations, the decision is taken on different levels. Often though, on the advice of the responsible manager present in the field, HQ makes the decision because they ought to have a macro view of the situation. If it is not possible to contact the HQ, the responsible manager present in the field (or most senior manager responsible for the relevant country programme) may decide to evacuate if a decision is urgently required. In other cases, the Country Director or Regional Coordinator is authorized to make the decision, while keeping HQ informed.

Where more ACT members, national and international, work together in an appeal, this decision should be discussed with the other members, as withdrawal of one or more members has security and work related repercussions for all others.

5.1.1 Before an Emergency Decisions

- What criteria do we set to help answer: Do the risks outweigh the likely benefits of the programme (see 2.4 and Annex W)? If they do, then the work should stop. If they do not, the work should probably continue.
- Who has the authority to call for such a decision?
- Do we have plans that realistically address threats, risks and potential scenarios? In the organization's Security Plan (2.5 and Annex N), there should be at least a basic outline of the plans for suspension, hibernation, relocation and evacuation available to staff. That said, these plans can be sensitive so the senior management team might decide to withhold

certain details until the actual event of an emergency. As with nearly all security documents, there should be different documents for different staff levels. The majority of staff do not need to know, for example, the amount of money in the office safe – this could be a lot of money in times just before paying local staff three months salary to tie them over during the volatile period.

- Have you fulfilled your organizational obligation to appropriately inform staff of how the organization will treat and prepare them? Have you provided them with various checklists for personal kits (Annex O)? Which staff will be trained in crisis management, with what purpose?
- What special considerations should be given to pregnant and lactating women, children, people with disabilities?
- Has your organization established and tested communication systems to notify staff? Have you considered alternative plans in case the mobile service is down or other system failures that could affect your ability to communication and gather information? Decide if tying into other systems, such as warden systems for UN / NGO networks, or embassies, or contact ACT's SWG for advice on the best service for your region: What can you start doing on now to ensure that you are in a position to opt into external systems when the urgent need arises?
- Has your organization had an honest discussion and preparation for financial issues like having, at hand, salaries and other money required by local staff?
- What equipment might be needed by managers to deal with a crisis? What might staff need: Which items do they have to get on their own and which will the organization provide? How might the organization cope with the lost or theft of certain equipment?
- What do you need to do to ensure information security? Before an emergency it is important identify which files need to be backed up onto disks and kept safe on-sight and off-location, deleted or destroyed. **Be aware that deleted files still remain on a disk, and can be retrieved by computer specialists**.
- Who is responsible for making sure to stock the assembly area with appropriate supplies? These can include:
    - Food
    - Water
    - Candles and matches
    - Toilet and related supplies
    - Power source
    - Communications equipment
    - Torches
    - Cooking equipment
    - Reading material and society games such as a pack of cards
    - Spare fuel for vehicles
    - Calling cards for different mobile providers, if possible
    - What other tasks might an emergency situation demand and who is responsible for implementation? Consider creating a security measures matrix tailored to your organization (2.3) so that at least senior managers know what is expected of them and what to expect other managers and staff to be doing.

5.1.2 During an Emergency Decisions

- How is the situation likely to change in the near future?
- Is it feasible to suspend, hibernate, or evacuate?
- What other security measures could be considered, which might enable the programme to continue?
- Rather than stopping work, would it be enough to reduce staff levels, reduce travel, 'hibernate' or hunker down, relocate, alter procedures or reduce visibility so as to reduce risks?
- What are other relevant organisations planning to do?
- Is any further information needed in order to reach a decision?

5.1.3 After an Emergency Decisions

Return and resumption after an evacuation may be quick or take a long time. Although delays will be frustrating, the safety of staff, beneficiaries and organizational assets is primary: Therefore allow sufficient time and resources for risk assessments (2.4 and Annex W).

Also it may take time to restore relationships with local staff left behind, beneficiaries, local authorities, etc. Emotions may be strong.

5.1.4 SAMPLE: Security risks categories linked to situational indicators and program decisions for each phase of the build up to an emergency situation

Security Risks Categories	**Indicators**	**Program's Security Decisions for Each Phase of the Build up to an Emergency Situation**
Minimal (Blue)	• No security events	• **Phase One: planning stage** ○ Who should evacuated or relocated and to where? ○ Who is responsible for which tasks? • Fully operative • Relocation, evacuation, suspension and hibernation plans reviewed • Support Partner agencies with their security plans
Low (Green)	• Minor insignificant and isolated incidents, curfews, riots • No immediate threats in agency project areas and capital	
Medium (Yellow)	• Tension and minor incidents at checkpoints • Minor clashes between armed groups without civilian casualties • NGOs affected accidentally but no injuries on staff • Serious but isolated attacks on civilians (mine explosion) • Suicide bombings in agency project areas • Few aerial bombings outside agency project areas	• **Phase Two: alert** ○ Have communication system been tested? ○ Have staff prepared their grab bag and keep it near? • Fully operative but decision on whether to conduct monitoring visits should be considered by _____ and in some cases postponed. • Relocation, evacuation, suspension and hibernation plans drilled • Weekly security situation reports • Encourage Partners to drill their plans
High (Orange)	• Escalation of armed conflict in agency project areas • Major clashes between armed groups with civilian casualties • Communal violence affecting civilians directly • Serious but isolated attacks on civilians in capital (suicide bombs) • Aerial bombings in agency project areas	• **Phase Three: evacuation imminent** ○ How to continue communication with remaining staff? ○ How to distribute salary advances in the safest way? • Partly operative • Hand-over key activities and documents to partners • Local partners encouraged not to work in field (hibernation) • Ready for relocation, evacuation and care for the remaining national staff • Daily situation reports • Daily meeting regarding security decisions
Extreme (Red)	• Breakdown in law and order • Repeated attacks on civilians and vital installations in capital • Deliberate, repeated attacks on NGO staff • Full scale armed conflict in most districts	• Phase Four: Evacuation ○ How safe is the evacuation route? Alternative routes? ○ Which threats might staff face during the evacuation process and how to mitigate these? ○ Which threat might remaining staff face? • Program suspended/ ended • Implement plans for staff relocation and evacuation and care of the remaining national staff

It is important to note that emergencies rarely occur in a neat sequence of increasing intensity, giving you plenty of time to make difficult decisions and prepare things: Therefore, all ACT members are encouraged to lay out plans early on. Annex B gives more details about the phases and the associated decisions and issues.

5.2 Suspension, hibernation, relocation

Suspending operational activities may be necessary to avoid a threat which has recently emerged. It may also be necessary in order to allow time for reflection on a changed security situation. Another possible reason is to send a signal or protest to local authorities or to other groups. If this is the reason, great care is needed, as such an action may have unintended consequences.

Suspension in order to send a signal is likely to be more effective if carried out by all similar or related organisations at the same time, and for the same stated reasons.

Suspension may be announced in the media. Alternatively it may be unannounced, depending on the circumstances, the threats, and on the purpose of the suspension.

An alternative to suspension is to relocate staff to a safer location, without leaving the country. A further alternative is to hibernate which involves stopping work and keeping a low profile for a considerable time. Sometimes this might mean leaving activities entirely in the hands of national ACT members and their local partners, with less support than usual. Ideally, this should be discussed and decided in an ACT Forum consultation. In any case, before making such a decision, consider the capacity and track record of the national ACT members and their partners concerned, particularly since it is likely that you should not be able to verify activities in the normal way – and listen to the views of the communities affected. In extremely insecure situations this may be too difficult or too risky for the partners who have to stay in country to accept or lend any support at all, be it to provide information or an opinion or to accept to take over programme assets.

To summarise, the options are:

1. Suspension: discreetly or openly;
2. Hibernation: transfer of responsibility for programme to national ACT member(s), through the ACT forum or bilaterally
3. Relocation: in-country or
4. Evacuation: to a neighbouring country.

In all cases, it is clear that the more thorough the detailed practical arrangements for programme continuity have been discussed with other ACT members, through the forum or otherwise, the more chance that the affected populations suffer less from the suspension/relocation measure.

5.3 Evacuation

When the situation is too dangerous for staff to remain, evacuation is necessary. The decision to evacuate should not be taken lightly, since its consequences can be far-reaching and also affect other ACT members, national and international. When the situation is too dangerous for all and international staff is being evacuated, local staff may have to be moved to a safer location in-country. National ACT members should discuss this option and international members provide advice and logistical support where necessary.

Specific details of an evacuation plan or evacuation plans (in the case of a joint ACT forum security plan with several international members) should form part of each country security plan (2.5 and Annex N).

ANNEXES

Back to TOC

Annex A - ACT Staff Security and Safety Principles

Users and Usage: All readers are encouraged to familiarize yourself with the “ACT Staff Security and Safety Principles” so that you can understand the foundations of the ACT Alliance’s general approach to security.

ACT has adopted the following five principles that guide the ACT Alliance approach to staff safety and security. Below are the principles with some explanation, for the full document go to: http://www.actalliance.org/resources/policies-and-guidelines/security/ACTPASSFinalJune08.pdf/view

Principle 1: Provide leadership, guidance and capacity to ensure that staff safety and security concerns are adequately addressed.

The senior management of each ACT organisation (member or Secretariat) is responsible for ensuring a safe environment for staff and promoting a culture of safety and security awareness and understanding within its organisation.

Therefore, at a minimum, ACT members and the ACT Secretariat should:

- Have a policy and procedures addressing key security and safety issues. This will demonstrate that ACT organisations are addressing their duty of care. Policies and procedures should acknowledge the special security needs and threats that may be linked with gender, age and diversity, and will ensure that such specific needs and vulnerabilities are taken into account when deciding on safety and security measures and procedures.
- Establish clear lines of authority and decision-making mechanisms on safety and security-related issues to ensure an effective and efficient response in an emergency.
- Nominate an incident manager who will be is responsible for all aspects of the handling of the kidnap particularly given the sharp increase in kidnapping in recent years. This person must have received expert training on how to achieve the safe return of a kidnap victim. No other staff member should take action relating to the kidnap without the approval of the incident manager – see ACT guidance on management response to kidnapping.
- Formally and regularly discuss and explain the policy and procedures to staff.
- Have security plans at country level – national and sub-national - which are regularly updated based on risk assessment.
- Ensure that the organisation has human and financial capacity to adequately implement policies and procedures, or co-opt external support if necessary.
- Ensure that staff are trained to cope with the safety and security issues at their posts of assignment, support them during their service, and address post assignment security sequel related issues.
- Ensure that all staff being deployed are given a security briefing relevant to their location and are debriefed on return for the purpose of improving security procedures.

- Lead by example by putting the safety and security principles into practice in their own lives and particularly in the work environment.

Principle 2: Adopt a systematic approach towards identifying safety and security risks, and identify suitable preventive and control measures.

A comprehensive risk, threat and vulnerabilities assessment should be at the heart of all ACT work. This applies to development, humanitarian and advocacy work at country programme level as well as headquarters level of all ACT organizations. Assessing and addressing risk demonstrates an organisation's commitment to safeguarding staff by reducing the chances of those risks actually arising.

ACT recognises that risk cannot be eliminated altogether. But it can be reduced, in two main ways, by: a) reducing the threat; and, b) reducing a person's *vulnerability* to the threat.

Therefore, at a minimum, ACT organisations should:

- Ensure that programme decisions are informed by appropriate safety and security considerations at all levels from programme identification, design, planning, implementation and, and monitoring and evaluation phases.
- Undertake a comprehensive risk, threat and vulnerabilities security assessment prior to…
  - Initiating any development or humanitarian programme in any country or region
  - Visiting a potentially insecure operational area or any area that is recognised as volatile
  - Expanding activities to a new location within a country
  - Making public advocacy statements.
- Carry out a health and safety risk assessment annually in each field office. At a minimum,
  - Ensure that staff are aware that in many cases health threats (e.g. malaria, HIV) pose the most serious risk to life, and staff should take precautions accordingly.
  - Efforts must be made to reduce the risk of sexual and gender based violence as the most immediate and dangerous security concern for female staff is sexual violence
  - Adopt strict fire prevention and response measures as fire poses a significant risk to health and safety, especially in countries where there is no fire brigade, buildings are not built to minimize fire hazards, and few people have fire-safety training.
- Develop a comprehensive, realistic plan for risk reduction and control measures.

Principle 3: Build staff capacity so that they are empowered to take personal responsibility for their own security

ACT recognises that safety and security is everyone's responsibility. It also recognizes that it is management's responsibility to ensure that both national and international staff are equipped and receive adequate training on safety and security issues to better prepare then for insecure situations.

Therefore, at a minimum, ACT management and staff should:

- Have mandatory, formal training for all staff on personal security and First Aid at least every three years. Staff should not be deployed to an insecure area without formal security training particularly geared to the priority risks in the receiving area.
- Ensure staff are equipped with or have access to functioning communications equipment during deployment.
- Identify a 'security' focal point within each ACT organisation and ensure that security focal points have additional and specialized training on a range of safety and security issues.
- Ensure that formal 'security' and 'health' staff link regulatory on safety and security issues.
- Have a clear understanding of the responsibilities and duties of all staff and address what are acceptable and unacceptable levels of risk.

Principle 4: Read, discuss and understand the *ACT Staff Safety and Security Guidelines*

The ACT Staff Safety and Security Guidelines: A Handbook for ACT staff (formerly known as the ACT Security Handbook) was developed by the ACT Security Working Group to provide security and safety guidelines to members of the ACT Alliance.

Therefore, at a minimum, all ACT staff should:

- Be aware of and understand the ACT Staff Safety and Security Guidelines and seek advice from management on areas of concern. At a minimum, staff should know "what to do" and where appropriate, "what not to do" in the following situations:
    - Traffic accidents
    - Disease and ill-health (e.g. malaria, typhoid, sexually transmitted diseases, etc)
    - Shooting, aerial and ground bombing, fire
    - Evacuation, including medical evacuation
    - Detentions and kidnapping, etc.
    - Tips for handling the media
    - Use of military escorts and private security companies.
- Know how to report an incident or potential incidents.

Principle 5: Provide psychosocial support to ACT staff who have experienced acute or prolonged stress during the course of their work

Stress is a risk to health, and to security. Managers and staff should aim to prevent stress, and should be alert for signs of it among their team. It affects different people, and people from different cultures, in different ways. Staff can become stressed for many reasons, such as: personal loss, overwork, or high-pressure work environment, conflicting job demands, multiple supervisors to name but a few. Traumatic stress can be brought on by exposure to emotionally powerful events or "critical incidents". It can produce a very intense response, including fear and/or helplessness, which may overwhelm the individual's coping mechanisms. Such a response is a normal reaction to an abnormal situation. It does not necessarily indicate that the person has developed a psychiatric disorder. Nonetheless, such exposure can lead to the development of post-traumatic stress disorder.

Therefore, to prevent, diagnose, treat and manage stress, ACT management and staff should at a minimum:

- Be aware of the dangers of excessive or prolonged stress, and understand signs of it in colleagues for whom they are responsible.
- Managers should at a minimum, ensure that staff have adequate working and living conditions, take annual leave due to them in a timely way, have realistic work plans and working hours, and know that they have the full support and encouragement of their manager in their work environment. Building a positive team spirit is central to the stress reduction process.
- Debriefing during and at the end of deployments should be done by a trained person if possible and improvements made where necessary based on feedback received.
- Ensure that staff who have been in, or witnessed, traumatic incidents receive specialist and professional support.
- Within certain limits, ACT management is encouraged to cover the cost of counselling for staff who have suffered stress as a result of their work, where this is appropriate and possible.
- If an accident, injury, illness, death or other serious event happens to a staff member, and if that person is unable to contact their next of kin, in most cases the employing organisation has at least an ethical duty to inform them. This is obviously a very sensitive process, and it is important that organisations have a clear procedure for it.

Back to TOC

Annex B – Evacuation – points to consider

Users and Usage: For the senior management team and Security Focal Points, below is an outline of some the considerations, by phase, associated with relocation and evacuation. This, in conjunction with Chapter 5, can support you with designing and implementing evacuation plans and procedures.

Phase one - planning stage

Evacuation planning and rehearsals should be carried out regularly. In many contexts the safety and security situation can deteriorate rapidly, often without warning. The evacuation plan should be written, and an outline included as a section within the Security Plan issued to all staff. When writing the evacuation plan, at least the following issues should be considered.

Who should be evacuated – Your organization is responsible for making sure that all staff members clearly understand their and their families' eligibility for evacuation or relocation assistance. The senior management team should determine which staff members are 'essential'; essential staff members are those required to conduct final coordination (Finance Officer for example), office closure, or limited, basic operations. Determine the evacuation order with Priority 1 evacuating first and Priority 3 last.

- **Priority 1** – Staff members who are in immediate personal danger due to the conditions of the crisis. International staff's dependents should be considered for an early departure.
- **Priority 2** – Individuals other than essential staff
- **Priority 3** – Essential staff

Where should staff be evacuated to? Identify a first-choice destination and an alternate destination for evacuation or relocation. Determine visa requirements, and the logistics that should be needed upon arrival at the destination(s).

How should staff be evacuated? Establish a notification system to ensure everyone is informed of the impending evacuation. Determine and verify an assembly point where staff should gather after notification. Detail the method of evacuation. Identify potential evacuation routes to airports, seaports, or land borders. Check to ensure that these routes can be travelled under emergency conditions. Inspect border crossings and safe areas. Coordinate plans with embassies, UN agencies, and other NGOs as appropriate.

What goes and what stays? Identify which documents, such as contracts, payroll records, etc, should be needed to re-establish operations once relocated or upon re-entry. Other documents should be marked for destruction, or left behind, as appropriate. Consider how evacuated documents should be perceived if seized by a particular person or group. They may contain information that could put the evacuating individual(s) at risk due to misinterpretation, and would be better destroyed or left behind.

Who is responsible for the various tasks during an evacuation? During crises key staff will be fully occupied so it is imperative that tasks and responsibilities for evacuation be clearly defined during the planning stage.

What could be the possible impact of evacuation on the operation? Should the office be closed and, if so, how and by whom? What are the policies and plans for continuing operations through locally employed staff members and ACT members' partners?

Phase two - alert

Mounting tensions and/or instability may lead the Regional Representative or Country Representative, in consultation with the International Director for the region, to decide to limit operations, increase security measures, and review the evacuation plan of staff of ACT members. The ACT members will discuss this with the national members of the ACT forum and together decide what may be appropriate for the local members. Work outside the immediate vicinity of the field office may be suspended. Tasks during this stage include the following.

- Brief all local and international staff on the situation, if possible;
- Communication systems for notification of staff should be finalized and tested.
- Prepare salaries and other money required by local staff
- Back up important files onto disks, delete and destroy sensitive documents.
- Staff members and their dependents should check that they have personal documentation with them at all times
- As appropriate, identify the equipment to be evacuated and responsibility for each item. Plan how high-value equipment which should remain should be hidden or otherwise protected.
- Designate which person will be responsible for the evacuation of which item
- Potential evacuees should assemble personal belongings to be taken during an evacuation, and keep these ready at all times, in a bag that the evacuee can carry without help. These personal effects should include:
  - Passport and visa
  - Driver's licence and other identification papers, as well as important personal documents such as diplomas etc.
  - Extra cash (convertible currency)
  - Hand-held radio with extra batteries (or satellite phone if more appropriate)
  - Mobile phone
  - Contact list
  - Any medical essentials
  - The 'grab bag' holdall must contain the following (it should not weigh more than 15 kg, for baggage space on evacuation means of transport is limited. It must also be swiftly manageable and the evacuee must be able to carry it without help, so children and tiny adults should have lighter bags if possible).
  - 2-4 litres water
  - Food: Select foods that require no refrigeration, preparation or cooking and little or no water, store at least a two day supply of non-perishable food, Select items that are compact and lightweight.
  - Clothing, as appropriate: e.g. warm waterproof jacket that packs small, hat for sun protection…
  - Personal first aid and sterile needle kit any personal prescription drugs as necessary
  - Whistle
  - Torch with spare batteries
  - Toilet paper, soap tooth brush etc
  - Pen, paper, photocopies of passport and visas
  - Sunscreen and mosquito repellent

  - Maps
  - Change your stored water supply regularly so it stays fresh. Replace your stored food every six months. Re-think your kit and personal needs according to the operational environment.
- Potential evacuees should ensure that they do not take with them any information or equipment that might be interpreted as incriminating
- Stock the assembly area with appropriate supplies (section 5.2.1)
- Assign each evacuee to a specific vehicle so that anyone missing may be readily identified, and ensure that all vehicles are ready, and that each evacuee recognises the vehicle to which he or she is assigned

Phase three - evacuation imminent

Potential evacuees may be relocated to a pre-selected staging or safe area. Remote staff may be recalled or relocated. Staff currently outside the region should remain in a safe place and not be allowed to return to the area to be evacuated unless for very exceptional compassionate or logistical reasons. Non-essential personnel may be evacuated. Tasks during this phase, which may last weeks or only a few hours, include:

- Keep all staff fully informed
- Coordinate closely with embassies, other NGOs, the UN, and other agencies as appropriate
- Pay salaries to local staff, with salary advances if possible
- Hide high-value property which should remain. Options may include distributing among trusted staff if it should not put them at unacceptable risk; hiding in roof spaces; or burying. Remove logos from vehicles which may be stolen. Ensure you keep copies of serial numbers of high-value equipment.
- Give clear instructions regarding responsibilities and leadership roles to those staff staying behind. Establish a means of continued communication between remaining staff and those evacuating. Provide authorisation documents to key locally employed staff if necessary.

Phase four – evacuation

Once evacuation or relocation has begun, it should take precedence over all other activities. The field office may continue operations through local staff or by national ACT members and their local partners, or may close completely. Considerations during evacuation may include:

- Ensure effective communication with local staff left behind
- If there is a risk of looting, consider disabling radios, equipment and vehicles. Empty and leave open all safes.
- All evacuees move to pre-designated assembly area
- Evacuate by the safest means possible, maintaining good order and remaining in communication with all groups evacuating
- Keep in contact with key local staff as far as possible
- Once evacuation is complete, inform the International Director for the region, relevant embassies, and key local staff, and the national ACT members which remained in country.

If a decision is made to close the office completely, care should be taken to ensure humane and correct termination or reassignment of staff contracts, both local and international, and the disposal of assets. This should have been discussed in the national ACT forum well before there is any need for evacuation.

Special considerations during evacuation

An evacuation is not easy for the evacuees or for those staying behind. It is a very emotional event, giving rise to feelings of guilt, hurt, frustration, and powerlessness. The departure of international staff can have a variety of meanings to the local population, including the removal of a symbolic or real safety barrier. Thus, an evacuation is not a neutral act and may even aggravate a crisis. When a field team evacuates, the senior management team should consider providing a statement for the media and others explaining the organisation's reasoning and any continuation or possible resumption of programmes.

Self-evacuation

Individuals who are working remotely from a local office, or who find themselves isolated during a crisis should use their judgement concerning the safety in their area. All staff members should be authorised to evacuate on their own authority, in accordance with established criteria and procedures, when they feel their safety is threatened. Every effort should be made to communicate with their manager during the process, and once in a safe area the individual should contact their manager or the Country Director immediately. No one may re-enter an area after evacuation without specific authorization from their line manager.

Locally employed staff evacuation or relocation

Normally, local staff will not be evacuated from their own country. But your organization should endeavour to move any staff, and their immediate family, to a place of safety if they are at risk because of their employment with an ACT member, their nationality, their ethnic origin or if they are the target of a serious threat.

Return and resumption of activities

This may occur soon after evacuation or take a long time. Re-establishing operations after an evacuation can be difficult. Local staff who did not evacuate may have experienced hardship and threats to themselves and their families. They may resent this. Restoring relationships with local staff left behind and with the staff of other members of the ACT forum, local authorities, beneficiaries, and the local population can be made easier if honesty, tact, and transparency are used prior to and during the evacuation, and on return.

Back to TOC

Annex C - Fire safety procedures

Users and Usage: For all staff, advice on how to respond to a fire in different situations.

Immediate action for fire response

It is important not to panic when confronted with fire. There are many things that can be done to prevent a fire from spreading and minimize damage and potential loss of life. The steps to take are:

- Sound the alarm. Shout for help, summon aid, and activate the fire alarm. Staff should not endanger their lives.
- Do not attempt to fight the fire if you do not have adequate equipment.
- For small fires priority may be to extinguish the fire quickly before it spreads.
- Determine the cause of fire and what is available to fight it. If it is an electrical fire, it is important to first turn off the electricity, if possible.
- Attempt to fight the fire but under no circumstances risk injury in the process
- If fighting the fire, position yourself with the exit to your back
- If successful, continue monitoring the site to prevent flare-ups until help arrives
- If unable to fight the fire, evacuate quickly, closing doors and windows, if possible, ensuring no one remains in the building;
- Give information to and cooperate with the fire brigade when they arrive.

Fires in buildings

Fires in buildings can spread quickly, trapping people inside. It is important to respond immediately to any fire alarm or evacuation order. Do not assume it is a practice drill. Staff should plan ahead and learn the emergency exit routes from residences and offices. In hotels or when travelling, look for the suggested evacuation route and rehearse it, if necessary. When evacuating a building remember the following:

- Think ahead what the route should look like – smoke may obscure vision;
- Stay low and move as quickly as possible. It may be necessary to crawl to avoid smoke and heat.
- Do not take the lifts/elevators – use the stairs;
- Cover yourself with a non-synthetic blanket, coat or other cloth, preferably wet;
- Before opening doors, feel the door for heat. There may be fire on the other side that should flare when the door is opened. Close doors behind you to help contain the fire.
- Avoid routes that are exposed to falling objects;
- Jumping from more than two stories can be fatal and should only be done as a last resort. If unable to exit a tall building, make your way to the roof. Offices or residences should not be located in tall buildings that do not have adequate means of evacuation during emergencies.

Remaining inside should only be an option when there is absolutely no means to escape. If unable to exit, prepare to remain in the building by doing the following:

- There should be identified shelter stations at each floor, in rooms with windows to the exterior. But whether you can reach that designated shelter or not, go to a room with an exterior window and **mark it clearly** to summon assistance. Stay in that room. The necessary items to mark windows should be kept in each room with an exterior window as a preparedness measure; it could be a strong vividly coloured rope, for instance.

- Close the main entry door and any interior door to the room
- Place blankets and clothes at the base of the doors to keep smoke out. If possible, use wet cloth to make a better seal. For preparedness, keep a non-synthetic blanket in each room.
- If possible, wet non-synthetic blankets, coats or other clothes for possible use later
- Stay low near an open window and continue signalling for help.
- If fire spreads to the room, get under two or more layers of blankets or clothes with the outer layers wet, if possible

If a person is on fire

If you or someone near you is on fire, remember - **stop, drop and roll**.

Stop. Don't panic and don't allow others to run about if they are on fire. Remove burning clothes, if possible and if you are not in danger.

Drop. Fall quickly to the ground or floor. If someone else is on fire, try to get them to do so. "Tackle" them only if you should not catch fire yourself.

Roll. Roll flat over and over (back and forth if in a room) until the fire is extinguished. The rolling should smother and scatter the fire in most cases. If someone else is on fire, have them roll. You can use water, sand, or a blanket to help smother the fire while they are rolling. Do not attempt to beat the fire out with bare hands; continue rolling instead.

Once the fire is extinguished, summon help and begin first aid.

Back to TOC

Annex D – Guards

Users and Usage: Guards are necessary in a great number of insecure situations. A reliable team of guards can be a major help with the smooth running of a programme. Whereas, poorly managed guards can lead to theft, be a danger to staff, and be an extra burden on managers. It is therefore worth investing time and effort to ensure that guards are managed well. This annex is for managers who have either overall responsibility or are direct line-managers of guards. Please also refer to the ACT adopted paper: SCHR Position Paper on Humanitarian-Military Relations (2010) http://www.actalliance.org/resources/policies-and-guidelines/ghp-principles-of-partnership.

Recruiting

Recruiting good quality people is crucial to success. Do not take shortcuts: use the proper recruiting procedure. Insist on checking references before a new guard is allowed to start work. Make sure that the guards can speak the working language of the field team, so that all staff are able to communicate with them. It is good practice to agree on pay scales for guards (and indeed other staff categories) with other NGOs in the area, to avoid creating tension between guards working for different employers.

Induction

All guards should have a full induction, involving briefing, equipping, and training where necessary. Written instructions should be provided in their language and the working language of the organization.

Briefing

Explain what the organisation does, and the values that it upholds. Describe the reputation that it wishes to have among local people. Make clear the importance of the guards, not only in protecting people and property but also in enabling the relief operation to help many others. Encourage them to feel part of the team.

Guards should be briefed clearly and thoroughly on their tasks. Do not assume that anything is obvious to them. Detailed briefing points should include:

- Most of the normal induction points that other staff would receive
- Their routine duties
- Hours and shifts
- The importance of remaining at their post even if the guard due to take over from them does not appear
- How to communicate with their manager, and with other staff
- Action to take in the event of different types of incident
- How to deal with visitors. The disciplinary system, and a warning that disciplinary action should be taken if a guard neglects his duties
- Guards should not risk their lives trying to protect property. Their role is to detect intrusion and to raise the alarm;
- Guards should receive clear guidelines to deal with trespassers in a professional manner-with firmness and clarity but without undue aggressiveness.

Equipping

The appropriate equipment will vary according to the circumstances but may include the following:

- Identity card

- Torch/flashlight
- Whistle
- Aerosol fog horn or other loud alarm
- Radio and spare battery
- Battery charger
- Mobile phone
- Watch
- Coat
- Stick (if justified by the threat and locally appropriate)
- Shelter
- Name badge
- Visitors' book

Training

Assess and provide for any training needs that the guards have. Rehearse with them the actions they should take in the case of the most serious security incidents such as armed robbery.

Keeping a few dogs to accompany the guards can be a very effective deterrent to intruders, particularly in cultures where dogs are feared – if used, guards must be trained to manage the dogs properly.

Managing guards

An experienced local staff member is likely to be the most appropriate line manager of the guards. He or she should keep a close eye on their performance, and should make random unannounced visits to check that all is well.

In some locations, it is almost standard practice for guards to sleep during the night. If this is the case, and if the security situation means that this would be dangerous, consider the following suggestions:

- Work out why they are falling asleep: for example, do they have a second job? Are their shifts too long? Do they have a long journey to and from work? Are they eating enough?
- Put two or more guards on duty overnight
- Appoint an overseer and hold him accountable for ensuring all guards stay awake
- Remove anything that could be used as a bed
- Summarily dismiss any guard found asleep on duty
- Shorten the length of shifts
- Visit guards unannounced in the middle of the night, so that they resist the temptation to go to sleep for fear of being caught

Private security companies

Many NGOs hire a local security company to provide guards. This is likely to be more expensive than employing guards directly. If the company is good, it can have several advantages including:

- Reduced administration: you do not need to recruit or manage guards
- Greater reliability: the company ensures that the guards are well trained and equipped, and turn up on time
- Replace guards immediately if one is sick or absent

- In many cases a quick reaction force is available, to respond to emergency calls (check whether the quick reaction team is armed, and if so, whether this is appropriate and justified, and what you should do when you call them – e.g. lie on the floor, stay away from windows, etc.). However, this can be really tricky and backfire as guards may overreact and hurt intruders far more than what you as an agency and ACT member, pledged to respect the sanctity of life, may consider appropriate: there is a need for clear rules of engagement prior to calling them in.
- Flexibility: easy to increase or decrease the number of guards, as the needs of the operation change
- No need to make guards redundant at the end of the operation.

It is vital to check the reputation and efficiency of a private security company before making an agreement. Are their procedures suitable for an organisation like yours? Should they use force only when necessary? Who is liable for harm done when they do? What kind of arms do they use? Is the company, or is any of its owners, connected to individuals or groups that you do not wish to be associated with? This could severely compromise your medium and long-term security. Are they honest?

There can be disadvantages in using private security companies. They usually cost significantly more than employing your own guards, while the security firms pay their guards less than an NGO would pay if employing them directly. Private security guards sometimes have no training for their role. Their presence can give the impression that an NGO is cutting itself off from local people. In some cases the loyalty of their staff can be weak. Consider these and any other possible disadvantages before making your decision.

Armed guards

Unless an exceptional situation warrants it, ACT members should not resort to armed guards or escorts. In such cases, thorough consultation with the ACT members working in the same country and/or emergency setting is needed.

If some NGOs use armed guards but others do not, those that do not can become greater targets while those that do can become associated with an implied threat of violence, and with a greater isolation from the local community. In a few situations, it may look ‘out of place’ not to have armed guards. If possible, all NGOs should reach the same decision on armed guards by consensus. They should consider how to minimise any negative local perceptions that might result. ACT members should engage in a thorough discussion about this with each other, local or international, where possible through the ACT forum and otherwise by talking to all members together in an ad hoc meeting.

Management of armed guards needs to be especially strict, with severe penalties for misuse of weapons. It is vital that the organisation supplying armed guards is reputable and reliable, and perceived as such among the local population. Check whether the organisation is connected to individuals or groups that you do not wish to be associated with.

Other issues to consider include:

- Checking that the guards are capable of doing their job
- Strict discipline, including a ban on the use of drugs or alcohol
- What happens if and when the need for armed protection ends?
- What happens if a guard injures or kills someone?
- Is your staff getting used to this high level of protection so that it may be difficult to stop using armed guards at a later stage?

Back to TOC

Annex E – Accident Contingencies for Staff

Users and Usage: For staff members but ideally these points have been adapted for the location situation by the Security Focal Point before distributed to staff.

Depending on the country in which the accident occurs, you may advise your staff to stop or not when they involved in an accident, even when people are injured – this should be assessed in the contextual risk analysis process (2.4 and Annex W) and communicated with staff. In some countries, stopping may result in your personal injury or death from the local people at the scene.

If you intend to stop:

- Check the immediate scene and determine whether it is safe to stop. (Keep in mind that someone may have staged the accident with intent to ambush or kidnap selected targets.)
- If it is safe to stop, render first aid immediately, if allowed to do so. Some countries forbid anyone to provide first aid unless the person is licensed to do so. Many countries do not have a "Good Samaritan" law. Wait for the police to arrive, but remember, in some countries you may have to get them.
- Inform your office of your actions.

If you decide that it is **not** safe to stop,

- Immediately contact your supervisor or manager. Advise them of the situation and that you are going to the police station to report the incident. Explain as clearly as possible which police station you intend to go to.
- Go to the nearest police station that is likely to handle this competently and file a report.
  - Tell the police you were "involved" in an accident.
  - Tell the police the location
  - Tell the police if there were any injuries
  - Provide your driver's license and any other required documents
  - DO NOT try to explain what happened or justify your actions. Keep in mind that ANYTHING you say can and probably will be used against you.

Back to TOC

Annex F – Incident report form

Users and Usage: For managers or Security Focal Points, this form is a template of key points to include. Your finalized form should be completed by the affected staff or trip leader and sent to the appropriate manager.

It is important that an incident report states the facts and that any analysis or opinion is either clearly identified (e.g. COMMENT……..COMMENT ENDS) or left for the next stage of incident inquiry and analysis. Staff should be trained and advised on how to write incident report forms.

'Near miss' incidents should also be reported. A 'near miss' is where it appears that a security incident came close to occurring. It may reveal a weakness in security procedures, or new information about security threats. Though a 'near miss' incident in some cases does not require an immediate or follow-up incident report, it should always result in a full incident report, so that lessons can be learned. All incident reports also help the Security Focal Point to build an accurate picture of current risks and future trends.

Who? Personnel involved (staff and others). Indicate female (F) or male (M) behind each name.
When? Date and time of incident
Where? Incident location (attach map / sketch / diagram if necessary)
What has happened? Description of incident
What have you done about it?
What help do you need?
Add any other important information here

Name	Signature	Date
Position		

While completing the form and in the follow up analysis, consider if relevant:

- Did the incident appear to be deliberately targeted at the organisation?
- Do you know who the perpetrators were? (Give details of appearance, behaviour, etc)
- What property was damaged, lost or stolen?
- Whom have you reported the incident to locally? E.g. authorities, police, other agencies, community.
- What reactions have there been from authorities, police, local people, other agencies etc?
- Have the media taken an interest? Might they?

All incident reports should be sent to the relevant line manager and be copied to the HQ security focal point as well as shared with other ACT members in the same location.

Back to TOC

Annex G – Field First Aid

Users and Usage: All staff and managers should read this annex, as basic field first aid can save lives. The information has been provided by Humanitrain (2010) www.humanitrain.com

Assessing danger

The first rule of first aid also applies anywhere in the field. Becoming a casualty due to not assessing danger is a real hazard. Effective hostile fire, no cover or concealment, leaking gas or fuel, downed electrical lines, hostile bystanders, traffic, unstable buildings and secondary incendiary devices at an improvised explosive device (IED) site are just some of the dangers in a conflict zone.

Incident Management

Check for DANGER. Confident, calm leadership of a team is essential. Assess the casualties one by one. Communicate with the rest of the team as to who should do what. Treat the most seriously injured first, not necessarily the ones making the most noise. Set tasks for the team and continuously review the situation for danger as well as additional assistance that may be required. Communicate with emergency personnel if available, certainly with line manager.

Rapid trauma survey

In a critical situation, quick decisions and actions can make the difference between life and death. The rapid trauma survey starts with checking for danger from the casualties themselves and well as external threats. Use protective gloves or non-return valve if resuscitation is required. Check for response by shouting and tapping the shoulders of the casualty. Open the airway by tilting the head back and lifting the chin. Look at the chest, listen at the mouth and feel on your cheek for breathing. If there is no effective breathing present, start chest compressions, do 30 compressions at the rate of 120 compressions per minute. Press the chest down 5 cms. Then open the airway, pinch the nostrils closed, make a seal around the casualty´s mouth and give two normal breaths. Control of bleeding, followed by the sealing of a sucking chest wound (with a plastic dressing and tape on the upper side and sides, leaving the lower edge open), the stabilisation of a flail chest and/or impaled objects follows.

Starting from the head, moving to the neck, the chest, the abdomen, the lower extremities and the upper extremities, assess the body for the following; Deformities, contusions, abrasions, puncture, perforations, burns, tenderness, lacerations, swelling.

Remember that bleeding is the most common cause of hypovolaemic shock. Massive hemorrhage takes precedent over the airway.

When to use a tourniquet

After exposing the wound, putting on a dressing, a pressure bandage, putting pressure on it manually, elevating it, using indirect pressure points plus another bandage, if the bleeding cannot be stopped and the casualty must be moved because the location poses more danger than the evacuation, then a temporary tourniquet can be used. The decision to use it must be taken fast.

It should be 5cm thick. Remember that it cannot be placed over a joint and that a pad should be placed underneath it. A tourniquet should remain bandaged but not covered (by a blanket or clothes). A ‘T’ should be written on the forehead. Evacuation must take place as a matter of urgency. If the bleeding can be controlled then the tourniquet could be removed within fifteen minutes. However, after fifteen minutes the affected limb will compromised. It should not be touched until the casualty reaches professional assistance.

Mechanisms of injury

Understanding what has taken place (blast, fall, blunt or penetrating trauma, burns, gunshot) is key to treatment and evacuation in an appropriate and timely manner. Mechanisms of injury relate to the amount of force, length of time force was applied and the areas of the body insulted.

Conflict situation

By ascertaining the type of weapon used, the distance from where the weapon was fired in relation to the casualty, it is possible to use this information as an indicator of the high or low probability of injuries to other parts of the body.

Check for tenderness, instability and crepitus (broken bones grating together).

When checking the head, look for blood and secretions in the ear, nose or mouth. Check behind the ears for Battle’s sign or the face for racoon eyes, which would indicate a head trauma has taken place (after twenty-four hours).

Assess for cyanosis (blue lips, extremities). Inspect and palpate chest, listen for equal breath sounds. Check for entry or exit wound. Inspect pelvis, assess for stability, priapism (continual penile erection indicating spinal injury). When looking at extremities, check for a pulse, motor and sensory function.

Spinal Injury

While only 1.4% of battle injuries involve the spine, road traffic accidents, bomb blasts, head trauma, any deceleration trauma, falls and assault can cause spinal injury. The neck must be immobilised well and immediately. The casualty should be log-rolled (moved from side to side, keeping the neck immobilised and the back straight) in order to evaluate their back during the rapid trauma survey. If evacuated, it must be on a hard board, well strapped down for transfer.

Evacuation

It is essential that a proper assessment by qualified medical personnel is made as soon as possible. Reassurance and making the casualty as comfortable as possible is key to maintaining their status.

If you are able to make radio contact with medic, do so and describe the casualty´s condition. If you are able to position them well, this can aid pain relief. If you are permitted to give oral fluids, give oral rehydration solution. Make sure that the casualty is accompanied, has their travel documents, insurance information and next of kin contact numbers. Ensure that everyone who needs to know the status of the casualty is informed.

Snake bites

Take preventative measures by being snake smart; avoiding areas where snakes inhabit, wear proper shoes, do not move at night without a strong light, take extra care in the rainy season. Ensure proper medevac procedures are in place.

Should a snake bite occur in a developing country, without advanced medical infrastructure, do not take extraordinary measures to identify the snake. If you can identify it, make sure that information goes with the casualty when they are evacuated. Do not put yourself in danger in order to identify it. Communicate the medical emergency, specifying what has happened and when, to who. While most snake bites do not involve envenoming, every snake bite should be considered venomous.

Keep the casualty calm, reassure them. Clean the wound of venom or teeth. Remove potentially constricting clothing and jewellery. Do not use a tourniquet, cut the wound, suck out the venom or use anything except water. Put a tight bandage on the affected limb, from joint to joint. Elevate the limb, but keep it lower than the heart. Evacuate the casualty as soon as possible, anti-venom saves lives.

Back to TOC

Annex H – Media: Tips on Handling Them

Users and Usage: This annex is for senior managers and others authorized to communicate with the media. It briefly outlines the advantages and disadvantages, followed by practical advice. Regarding who should communicate with the media, it is recommended that ACT members, big or small, should nominate a spokesperson for the organization and inform all staff to refer the media to that person. Staff will need to know that the agency is not trying to muffle them but that dealing with the media can have serious consequences so it is important not to have to mixed messages or confusion – this is best achieved by having a spokesperson. The spokesperson can be the senior most manager or someone with special language or communication skills.

The media can sometimes have a negative impact on NGO security. By reporting details of a sensitive programme they may arouse the anger of groups who wish to see the programme stopped. They may attract the attention of hostile armed forces. They may simply alert criminals to the presence of high-value goods to steal.

On the positive side, the media can enhance security by reporting accurate information about an NGO, winning local goodwill. After a security incident, the media can be used to disseminate accurate reports, thus squashing exaggerated rumours that may be circulating. Involving the media can also attract international attention to a forgotten humanitarian situation, bringing the possibility of funding, security intervention or political pressure.

Managers should therefore be aware of media reporting, and able to use the media effectively when appropriate. Points to bear in mind may include:

- Know what message you want to get across, and ensure that you do so during the interview. Be able to express it briefly and clearly. In the Western media, expressing your message in a 'sound bite' of 8 seconds or less greatly increases the chances of it being broadcast. You may also discuss with the ACT forum members what the best message is for the local media.
- Ensure that you always tell the truth. This is right in principle, and wise in practice. It builds up a reputation for honesty, and false information is usually found out in the end. Telling the truth is not the same as telling all – be truthful, but don't feel pressure to tell more than you want to nor to move away from your message.
- If you are not sure of a fact, don't publish it. If you don't know the answer to a question, say you don't know. If you have to publish unconfirmed information, state clearly that it is unconfirmed.
- After a major security incident, consider making an early statement to the media as soon as you have some confirmed facts to tell them. This should help to prevent false rumours from growing.
- It is not a good idea to say "no comment" to a question from the media. This looks defensive, and leaves an information gap that they may try to fill with less reliable information. You can instead repeat the key points from your message or inform the journalist that you will get back to them once you know more.
- In general, openness works better than a defensive attitude towards the media. They have a legitimate job to do, and they can help your operation. An ideal working relationship should be respectful, professional and open but not too familiar, since the media may be tempted to take advantage of too close a relationship.
- If you become aware of a false rumour concerning your organisation, consider how best to correct it. Assess whether it could become the cause of an increased threat to your organisation if it is left uncorrected.
- Avoid commenting on the government, political or military situation unless there are overriding reasons to do so.

Back to TOC

Annex I - Medical evacuation (medevac) procedure

Users and Usage: This annex is primarily for managers who are responsible for ensuring that medevac procedures are included in your agency's Security Plan (Annex N). Once the details are settled for your particular agency in it's specific situation, then this type of information needs to be shared with staff.

The Security Plan (Annex N) for each country should detail the procedure for medical evacuation (Medevac) including in-country medical relocation or evacuation to nearest medical facility

- All staff should know the procedure for medical relocation and evacuation
- There should be clarity as to which staff are entitled to Medevac, and what medical arrangements are available for any staff who are not entitled to Medevac

Medevac routes should be checked. Will the roads you intend to use be open if there is a deteriorating security situation? What alternative routes are there? Will the local airfield or airport be open, accessible, and secure? What alternative airfields are there?

A medical NGO operating in the same area may be able to help during medical emergencies. Discuss this possibility with them before an emergency arises.

Back to TOC

Annex J - Procedure for informing Next of Kin

Users and Usage: For managers or staff who have been designated this responsibility, this annex gives practical advice for informing a staff member's next of kin in the event of an accident, serious security incident, or death. Much of the advice is taken from the ECHO Generic Security Guide, as it is a good resource for NGOs. It is available free online in English, French, Spanish and Arabic, at http://ec.europa.eu/echo/policies/evaluation/security_review.htm.

If an accident, injury, illness, death or other serious event happens to a staff member, and if that person is unable to contact their next of kin, in most cases the employing organisation has at least an ethical duty to inform them. This is obviously a very sensitive process, and it is important to have a clear procedure for it.

The procedure is likely to include at least the following points:

- Who should inform the Next of Kin? In serious cases such as death, it should usually be a senior manager who informs the Next of Kin, to show the importance that the organisation attaches to the event, and to supporting the family and friends of the staff member.
- By what means should the Next of Kin be informed? If the staff member has died or is seriously ill, a personal visit is likely to be essential. In some cases, for example where the Next of Kin lives in another country, a rapid personal visit may not be possible, in which case a senior manager should decide whether a telephone call is appropriate.
- Advice to those who have to communicate the news to the Next of Kin

Communicating with Next of Kin

The following tips may be helpful:

- If you do not speak the same language, ensure that a good interpreter is available, and consider whether a colleague who does speak the same language would be more appropriate to break the news
- (If visiting) Dress respectfully. If the Next of Kin is a woman, ensure that the visit is by a woman, or if there is more than one visitor, at least one of them is a woman – and vice versa.
- (If telephoning) Ask the person if they are alone. If they are not, request that they go to a room where they can be alone.
- (If visiting or telephoning) In the case of death or other serious event, you may wish to have a trained counsellor take part in the visit or call
- Say that you have some bad news. Invite them to sit down.
- Look at them directly (if visiting). Tell them simply and clearly what has happened to the person concerned. For example, "I am very sorry to say that John is dead." This is usually far better than a longwinded sentence, or delaying the moment when they hear the bad news. They have probably guessed it already.
- At this point, be prepared to offer support to the person. Their reaction may take many different forms, ranging from silence all the way through to hysterical grief or even violence. What is important is that you remain calm, supportive, sympathetic and gentle. Depending on their mood, a physical sign of support may be appropriate, from someone of the same gender: for example, an arm round the shoulder. It is helpful if you come with a supply of handkerchiefs.
- If and when they wish to hear the whole story, tell it simply and clearly, preparing to pause if they cannot hear any more.

- Use your judgement as to whether it is appropriate to tell them a long version of the story, or a shorter version. A shorter version inevitably is more selective, but it may be all that they can cope with at this stage.
- Make sure that everything you say is truthful. If you don't know the answer to a question, say that you don't know. It can be very damaging for relatives to discover later that they were misled, whether intentionally or unintentionally.
- Once they understand the situation and are calm enough to think of practical matters, inform them what action the organisation has taken (e.g. taken the injured person to hospital; recovered the dead person's body, etc). Suggest what action they might wish to take (e.g. fly out to see the injured person). Say what help the organisation should give (e.g. pay for airfare; ensure that any insurance payment happens rapidly – but check that you only give totally accurate information on financial matters, and make no promises that you cannot keep). Take plenty of time to reassure them as much as possible.
- Ask if they have family or friends who can provide emotional support, and offer to contact them on their behalf
- If they need you to stay for a long time, be prepared to do so. If the news is of a death, they should not normally be left alone; instead, wait until a friend or family member has arrived to support them. Once they are ready for you to leave, express your sympathy again, and reassure them that you will help in every way possible. Give them your name and full contact details. Give them the name and contact details (including evenings and weekends) of the person who will be their main contact within the organisation (if it is not you).
- Ensure that you (or the main contact person) contacts the Next of Kin the next day, and as frequently as appropriate thereafter. Organisations sometimes find it easier to offer immediate support, but harder to remember the ongoing support that is vital – both for the good of the Next of Kin, and for the reputation of the organisation. The family of a dead staff member is likely to make severe criticism of any employer who appears to forget them.
- Verify what financial and other help is due from the organisation, or from an insurance company, to the Next of Kin. Ensure that this is communicated with total accuracy, and without delay, to the Next of Kin. Arrange for this help to arrive as soon as possible.
- A senior manager should remain in charge of the whole process, to ensure that high standards are maintained.

Back to TOC

Annex K – General Personal Security

Users and Usage: For all staff, visitors and managers below are general personal security tips for prevention and reaction. For Security Focal Points or equivalent, you can use this as a template that should be modified accordingly and distributed. As these are general points, they should be supplemented with advice dealing with specific threats and risks (Annex N and W).

Tips for Prevention

- Generally be aware of your surroundings and radiate security awareness.
- Be informed and aware of security risks by assessing the risks of your activities (Annex L) and following organizational advice.
- Inform the designated manager of your travel plans. Only tell other people of your travel plans on a need to know basis.
- Plan outdoor activities (shopping, dinning out, exercising) with your security in mind.
- Carry your mobile phone with you. Make sure it is fully charged and operational.
- Keep emergency contact numbers with you, in your mobile and in paper form.
- Keep your ID cards and travel documents with you and keep extra copies in your house/office/online as well with HR.
- Avoid public gatherings such as political and religious demonstrations so be aware of when and where they might occur.
- In most cases, photography of women and strategic locations, military hardware and personnel should not be done.
- Dress appropriately and respectful of sensitivities, especially when in rural areas.
- Respect local customs at all times. It is important to remain patient, polite and even-tempered.
- Do not carry prohibited or un-licensed arms.
- Do not try to influence peoples' religious or political views. Conversations on these topics should be limited to friends.
- No staff member or visitor should become intoxicated or drink before driving or a public dealing.
- Keep an inventory list of your valuables.

Tips for Reaction

- Follow your instincts, if you feel uncomfortable about the situation leave immediately or consult with others.
- Report suspicious behaviour to authority and supervisor.
- Make mental notes of what happened, who, when, where, how situation developed.
- Ask your supervisor about the professional support services that your agency can provide.
- Submit an incident report.

Back to TOC

Annex L - Risk assessment for individual journeys

Users and Usage: All readers are recommended to know how to conduct a basic risk assessment before a journey.

Risk, threat and vulnerability

Risks cannot be eliminated altogether. But they can be reduced, in two main ways:

- Reduce the threat
- Reduce your vulnerability to the threat

For example, you can reduce the threat of robbery by avoiding parts of town notorious for robbery. Or you can reduce your vulnerability to it by not showing attractive items like jewellery or a mobile phone.

In a safety example, you can reduce the threat of a vehicle accident by ensuring the car is in a roadworthy condition and that it has a good, careful driver. Or you can reduce your vulnerability to an accident by wearing a seatbelt. Best of all, reduce both the threat, and reduce your vulnerability to it.

Assessing the risk of a proposed journey

When assessing the risk of an individual journey, use the following simple process:

- List the threats or risks that the journey involves, including risks from accidents, health issues, military or civil instability, terrorism and crime.
    - Get a security briefing before going to a new location/ country and before each journey (see Annex M)
    - Compare advice from those who know the area, such as ACT colleagues, partners, church people, staff of other NGOs, local people, diplomats etc.
    - For areas you don’t know at all, the internet can be helpful including:
        - International Crisis Group www.crisisweb.org
        - UN Integrated Regional Information Network (IRIN) http://www.irinnews.org/
        - ReliefWeb www.reliefweb
        - UN Humanitarian Information Centres (HICs) www.humanitarianinfo.org
        - The UK Foreign and Commonwealth Office www.fco.gov.uk
        - AlertNet www.alertnet.org
- Assess the likelihood of each threat occurring; its likely impact if it occurred; and your vulnerability to it
- Decide what security measures you should take, to:
    - Reduce the threats (for example, by avoiding those which can be avoided), and
    - Reduce your vulnerability to the threats (for example, by being accompanied by someone familiar with the area)

The above process should give you a good idea of the risks involved, and how they can be reduced. But still there will probably be some risks. Following the security plans for each location (see Annex N), will further reduce risks. The key question to ask is: Does the likely benefit of the planned journey outweigh the risk? If it does, the journey is probably justified. If it does not, the journey should not go ahead.

If, having gone through this process, you are in doubt, ask advice from an experienced person, for example from your line-manager, Security Focal Point or other ACT members who may have access to good information. There is no formula which ensures an accurate risk assessment: it always involves a judgement. But by following the process above you are more likely to arrive at a decision that is well informed and well thought through, and therefore more likely to result in a safe and successful trip.

Back to TOC

Annex M - Security briefing checklist

Users and Usage: The aim of a security briefing is to enable staff to understand the local situation sufficiently to live and work safely in it. Security Focal Points and managers with security responsibilities are normally given this task.

A security briefing should be given to all internationally-recruited staff before they travel to an insecure location. This briefing should be as thorough as possible, but usually can not be as detailed as a security briefing on the ground. On arrival, a further security briefing should be given which goes into greater detail and gives fully up-to-date information on the situation. Local ACT members' staff may also be invited to such a briefing, or the briefing can be organised by the ACT forum.

Local staff should receive a full security briefing before they start work, appropriate to the location. In low-risk locations this is likely to take very little time; in high-risk locations it may take several hours.

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, and to give them written instructions or an edited version of the Security Plan, if necessary.

The length and content of security briefings should vary according to the situation, the knowledge of the person being briefed, and the job that they are doing. But in general, most initial security briefings for people new to the situation are likely to cover the following topics.

- Local geography: major features; centres of population; routes; condition of roads; natural hazards such as flood, earthquake, eruption; any other aspect that may affect security. Considerable effort should be made to obtain good maps of the area to permit effective briefing.
- History of the area, particularly as it affects the current political and security situation
- Political situation and any political trends, issues or sensitivities
- Ethnic groups in the area, their different histories, characteristics and aspirations
- Culture and custom in the area, including acceptable methods of greeting, languages used, dress codes, actions and phrases to avoid. ACT forums, especially their national and local members, can help to constitute a good checklist.
- Key local personalities and entities, including political, cultural, religious and other leaders
- Local laws and national legislation, as these affect expatriate and local staff and/or international organisations and interagency collaboration between international and national ACT members;
- Local police and other relevant officials
- Armed forces and other armed groups in the area
- Driving rules, practices and habits; and organizational policies
- Likely threats to ACT and/or to other similar organisations
- Guidelines and procedures to respond to those threats
- Recent security incidents
- Location of local medical facilities
- Evacuation routes and procedures, including specific tasks of each individual as well as individual responsibility
- Other ACT members in country and other relevant organisations (NGO, UN Red Cross, Church, government) in the area
- Phone numbers and/or radio channels and call signs to call in an emergency

- The background to ACT's programme in the area, and the role of each ACT member therein
- Any permissions necessary from local authorities
- Issue of identity documents and explanation of when they are required
- Security Plan, including all security-related rules and procedures
- Communications and IT security
- Enough time for any questions to be fully answered

Local staff should already be aware of some of the above information: it is up to the manager to judge which parts of the briefing can be skipped for them.

Best is for the briefer to prepare a written orientation briefing document, containing some basic information on the situation. It may contain, for example:

- Name of Head of State
- Name of Prime Minister
- Governing Party/Parties and their leaders
- Government in force since [date]
- Government mandate expires on [date]
- Opposition Parties and their leaders
- Local government authorities relevant to ACT's work; their functions; names of key officials; their contact details
- Description of the conflict, if any
- Description of local crime situation
- Names of military, paramilitary or bandit forces in the area
- Contact details of local Embassies or Consulates
- All local and national staff need to be briefed if travelling out of their area of operation.
- Locally employed staff may have little or no need to be briefed on the local situation. But locally employed staff of national or international ACT forum members may have a skewed view of the local situation, for the very reason that they are rooted in it and accustomed to it, so that their knowledge may be biased and incomplete. This also applies to the ACT members that are local and national church and church related agencies. Furthermore, national staff of national agencies are almost as expatriate as expatriates from overseas if they normally live and work in the capital and now are transferred to the area of relief activities in another part of the country.

Annex N – Security Plan: Basic Template

Users and Usage: The most senior staff member responsible for security should write or oversee the delegated staff writing a Security Plan. Your Security Plan needs to be context-specific and highlight organizational security rules and procedures, which apply to staff in, or travelling to, that country. Each organisation should also identify a Security Focal Point (this may or may not be the most senior staff member responsible), whose responsibility it is to ensure that all staff are aware of and following the policies and procedures outlined in the Security Plan. The Template below lists key points that you may want to include or consider.

For staff without security responsibilities, you may opt to skip this section or briefly review it.

What is a Security Plan?

The aim of a Security Plan is to provide staff, consultants and visitors with a concise document that sets out the security rules and procedures applying to the country/ location where they are working or visiting.

There are two main kinds of documents that comprise a Security Plan: Standard Operational Procedures (SOPs)/ Guidelines/ Protocols and Contingency Plans/ Emergency Plans. SOPs are for day-to-day precautions. Contingencies are for managing extra-ordinary events so to mitigate the impacts. In general, SOPs are preventative and Contingencies are reactive. Overall, the Security Plan should not be overly prescriptive at the same time it should clearly explain what to do, why to do it, when to do it, what others should be doing, and what equipment is needed. These documents should target specific end-users by being relevant, informative, and realistically addressing their needs, concerns, issues, and usage.

The generic security advice in these Guidelines, covered under specific threats, and from other sources like ECHO's Generic Security Guidelines, should be modified and supplemented in order to be as context-specific and relevant as possible. Each Security Plan should be based on the risk assessment for that country/ location, tailored to the risks in that area (Annex W). In low-risk locations, both the risk assessment and the Security Plan can be very short. In high-risk locations, both documents are likely to be more detailed. In all cases they should be as concise as possible, since busy staff may be tempted to ignore long documents. The Security Plan shall be updated at least annually. To be a 'learning organization', the plan should reviewed regularly in high-risk locations, and immediately if changes in the security situation requires it.

- When writing these plans questions to ask include:
- Does it address the threat? Other threats?
- Could implementing this plan create additional threats?
- Who is vulnerable? In what ways?
- How could implementing this plan affect our programs?
- What resources are needed?
- Is it in line with our principles?

Template for writing Country and Local Security Plans

From the outset, the Security Plan should clearly map out the:

- Its purpose, intended users and usage
- Line of Authority (Field and Head Office) and organizational and individual responsibilities – can refer to key ACT Alliance documents like the "ACT Staff Safety and Security Principles".
- Geographical Coverage of the Security Plan

- Background and introduction to the Field operation / Project
- Context Analysis, usually in the introduction, should cover demographics (population, religious groups, ethnic groups, etc), historical, social, cultural, economic, climate/ environmental, political issues
- Risk analysis overview
- Appendices could include:
    - Maps
    - Key contacts
    - Incident reporting form (Annex F)
    - "ACT Staff Safety and Security Principles" (Annex A)
- Security documents should state who was the primary author, where appropriate or possible, who authorized it, when created and lasted updated.

This type of information can be in the main body of the plan and referred to in other documents, thereby keeping the documents concise and interconnected. After the main body of the Security Plan, then you can include the SOPs and Contingencies.

An example of formatting the key advice in prevention and reaction tips for staff is below.

SAMPLE: Grenade/ Bomb Attacks SOPS and Contingencies for Staff

Since parts of YYYYY suffer from terrorism and sectarian violence, it is advisable to know the places and circumstances to avoid and to how know to react if there is the threat of an explosion. For information about and pictures of grenades, see http://www.howstuffworks.com/grenade.htm

Grenade Attacks	
Tips for Prevention	**Tips for Reaction**
• Learn about areas where grenade/ bomb attacks have previously occurred and places where riots/ demonstrations might occur • Be extra careful on symbolic dates (anniversaries, elections) and near potential targets (government buildings, symbolic locations) • Know that such attacks tend to come in a series of bombs	• Get down – preferably lay on your stomach, cross your legs, put your face between your arms so that your face is off the ground and each ear if covered by a forearm • Stay away from glass • Put solid things between you and danger (while this is good to do, getting down quickly is the most important thing you can do) • Do Not use your mobile and turn it off until the authorities inform you can (mobile frequencies can trigger some bombs) • Stay away from vans and large containers • Only get up from your safe place when the authorities have given you permission • As soon as it's safe, report the incident

While SOPs and Contingencies for managers and staff will be different and there might be differences between different staffing groups, the topics will generally be the same. Depending on the realities of the environment, topics could include:

Basic	Risks and threat related
• Political, cultural and religious issues, behaviours, etc • Relations with the local community • Driving and traffic • Health and hygiene issues • Handling of cash • Office safety and security • Document and information security • Communication and contact lists • Incident report process and forms	• Crime – street, violent • Land Mines / UXOs • Natural hazards • Check points – legal and illegal • Unrest / War / Riots • Kidnapping, hi-jacking and hostage

For the special cases of extreme emergencies and evacuation situations, the contingency plan should cover:

- Who may order evacuation
- Crisis evacuation routines
- Routines for local staff left behind
- Quick run bag: contents and location
- Assembly points
- Other relevant procedures

During a crisis, several headquarters may be involved simultaneously, both in-country and abroad in the case of the international ACT members present. All staff in-country should possess instructions on how to react to emergencies, and should be able to contact the senior staff member very quickly, in case of emergency. The names and contact details of the relevant line manager(s) at headquarters should be made available to the ACT SWG, by communicating them to the ACT alliance secretariat humanitarian policy officer or to the chair of the ACT SWG, or to the Director of ACT Alliance (for current telephone numbers and e-mail addresses see Annex Z).

The SOPs and Contingencies, together with other related information, should be contained in one Security Plan. But to make them even friendlier to the end-user, the individual topics can be issued separately, as required. Or summarized on wallet sized cards. Too often Security Plans sit on a shelf after completion: Good security management is more than writing a Security Plan and checking that task of the list. Good security management needs an 'a live' Security Plan to help make staff aware of how to work safely and securely.

Annex O - Contents of first aid kit

Users and Usage: Below are several first aid checklists. The first list is for staff working in remote locations and conflict zones. The next two are for managers who are responsible for first aid supplies in the office and vehicles and the special case of working in conflict areas.

Personal travel kit for remote locations and conflict zones:

Item	Quantity
Trauma Dressing	1
Crepe Bandage	1
Tuffcut shears	1
Vacuum Compressed Gauze	1
Examination Gloves	2 pairs
Plasters, various	I or 2 packs, depending on contents
Alcohol wipes	1 or 2 packs, depending on contents
Vent aid	1
Wound Closures	I pack
Micropore tape	1
Safety pins	4
Disposable thermometer strips	5
Burn Gel	1 tube
Disposable forceps	1
Antiseptic cream	1
Melolin 5X5 cm	1
Melolin 10X10 cm	1

Standard kits for field offices and vehicles:

Item	Quantity
Inspection Gloves	1
Tuffcut Shears	1
Merlin Face Mask and Case	1
Triangular Bandages	2
Plasters (Waterproof)	1
Plasters (Fabric)	1
Micropore Tape	1
Crepe Bandage	3
Wipes (pack of 10)	1
Blunt End Forceps	1
Disposable Scalpel	1
Watergel Burns Dressing	1
Steropad	1
Mini Maglite	1
Safety Pins	1
Field Dressings	3

Swabs (pack of 5)	1
Emergency Foil Blanket	1
Casualty Straps	1

Trauma first Aid kits for conflict zones:

Item	**Quantity**
Tuffcut Shears	1
Disposable Airways (Sizes 1-4)	4
Pocket Face Mask	1
Triangular Bandages	6
Sam Splint	1
Pkt Fabric Plasters	1
Pkt Washproof Plasters	1
Micropore Tape	1
Leukocrepe Bandages	6
Pkt 10 Alcohol-free Wipes	2
Scissors	1
Forceps	1
Hypodermic Needles (Assorted sizes)	24
Hypodermic Syringes (Assorted sizes)	24
Baxters Sterile IV-giving Set	1
Blood-giving Set	1
Ported IV Cannulas (Assorted Sizes)	6
Disposable Scalpels	2
Waterjel Burn Dressings	3
Pkt 5 Steropads	5
Res-Q-Vac Aspirator	1
Res-Q-Vac Adult Cartridge	1
Hartmann's Solution	2
Support Collar	1
Maglite	1
Pkt 4 Leukostrips	1
Assorted Safety Pins	1
Field Dressings	6
Sterile Latex Gloves	2
Set Cas Straps	1
Emergency Blankets	3
Pkt 5 Swabs	4
Asherman's Chest Seal	1
Pkts Quick Clot	6

Back to TOC

Annex P - Situation report (sitrep): standard format

Users and Usage: The sitrep may be filled out by the Security Focal Point or appropriate line-managers. However, the senior management team should be involved with defining the key points and setting the frequency of the reports.

A standard sitrep format, used throughout an organization or branch office, helps managers and staff to find the information they need, easily and quickly. Your organization's standard format should include:

Local situation, including any changes in the situation of:

- Local population (describe sub-groups as appropriate and significant from a security perspective). Give all data gender and age disaggregated and include any new development issues or humanitarian needs also related to gender.
- Politics
- Local authorities
- Security, including actions of armed groups
- Economy
- Action by other relevant organisations

ACT member programmes and other activities, including:

- Action taken in the reporting period. The "reporting period" is the period to which the sitrep relates. For example, a weekly sitrep may be dated 24 March, covering the period 16 to 23 March. The reporting period is therefore 16 to 23 March. To avoid any confusion, it is always useful to state the exact period covered as well.
- How that action compares with the action that was planned
- Successes
- Problems

Administration, including:

- Personnel
- Finance
- Logistics

Action requested

- From line manager
- From Country Director
- Possibly from the International Director for the region
- From other in country ACT members
- From the ACT Alliance through ACT Secretariat
- From any others

Non-routine sitreps, such as an emergency sitrep on a new crisis, may adapt the format of the routine sitrep if appropriate. Note that sitreps, including emergency sitreps, are different than an incident report (Annex F).

In recognition that reporting does take time, one 'short-cut' could be to simply write 'no change' when appropriate and refer to the original inputs included in an earlier report.

Back to TOC

Annex Q – Stress

Users and Usage: All readers are encouraged to review and reflect on the points raised.

Stress is a risk to health, and to security. Managers and staff should aim to prevent stress, and should be alert for signs of it among their team. It affects different people, and people from different cultures, in widely varying ways. The points below are suggestions only, and should be selected and adapted according to the situation and culture.

Causes of stress

The causes of stress may include many things, such as:

- Personal loss
- Overwork, or high-pressure work environment
- Conflicting job demands
- Multiple supervisors
- Lack of clarity about responsibilities or expectations
- Job insecurity
- Trauma
- Failure of a programme or other activities
- Feeling overwhelmed by the scale of need around
- Human error
- Misunderstanding
- Illness
- Inter-personal difficulties
- Antagonism from authorities or local people
- Unsatisfactory personal relations, not necessarily work or security related

Prevention of stress

Stress can often be prevented by taking a few simple precautions, including:

- Realistic work plans and working hours
- Clear briefing
- Efficient, caring management
- Listening regularly to staff, particularly when they are under pressure
- Keeping staff fully informed
- Encouraging staff and praising them for good work
- Rapid resolution of any grievances or complaints
- Sufficient rest, including a weekly day off in all but the most acute emergencies, and enforced Rest and Recuperation (R&R) in periods of high pressure
- Enabling staff to see their families and/or phone home, if they are away from home
- Efficient mail service, and private access to personal e-mail, where possible
- Privacy in living accommodation
- Little luxuries, such as books, magazines, videos, good quality soap

- Eating properly, with a variety of menus
- Building team spirit
- Friendships
- Exercise
- Recognition, praise and reward for good work
- Allow for joint prayer or other forms of accepted, shared spirituality/religiosity
- Adequate pay
- Secure home environment
- Fresh air and outdoors activity

Signs of stress

Managers and staff should look out for signs of stress in themselves and among their colleagues. Common signs include:

- Uncharacteristic or erratic behaviour
- Talking much more or much less than normal
- Irritable moods or short-tempered outbursts
- Headaches
- Depression or anxiety
- Apathy
- Unexplained aches and pains
- Skin problems
- Overwork
- Disregard for security, risky behaviour
- Indecisiveness, inconsistency
- Reduced efficiency at work
- Inability to concentrate
- Frequent absence from work
- Recurrent minor illnesses
- Disillusionment with work
- Extended fatigue
- Disrupted sleep or oversleeping
- Over- or under-eating
- Alcohol and/or drug abuse

Treating stress

A doctor or trained person should advise on treating stress. Debriefing should be done by a trained person if possible. In the absence of a trained person, the following tips are often found helpful, but the appropriate action may vary widely according to the individual and the culture:

- Take time to talk with persons suffering stress. Encourage them to express how they are feeling. Reassure and encourage them. Allay or deal with any worries they may have. Find out if they would benefit from any changes to work practices. Do they need more help with their tasks? Are there other pressures on them, for example bad news from home?

- Enable the person suffering stress to take time out from high-pressure work, but not to stop work completely. Suggest useful tasks that they can do, which are not stressful. This can help them to feel useful and valued, and can be part of the healing process.
- Ensure they have access to recreational or religious facilities, and counselling if desired
- Encourage them to look after themselves: eating well, taking exercise, frequent rest, etc
- Keep talking with them regularly – or ensure that a sympathetic colleague does so
- After a short while, depending on the circumstances, it is often possible for them to resume their normal work. Indeed returning to work, after a sensible pause and without overloading them, can help recovery.
- Continue to monitor them and to listen to how they are getting on
- If they do not respond, or if they are not able to return to work, seek medical advice

Traumatic stress

Any event that is very distressing and outside the realm of normal human experience can result in traumatic stress. Traumatic stress usually produces a very intense response, including fear and/or helplessness, which may overwhelm the individual's coping mechanisms. Such a response is a normal reaction to an abnormal situation. It does not necessarily indicate that the person has developed a psychiatric disorder. Nonetheless, such exposure can lead to the development of post-traumatic stress disorder.

Traumatic stress is brought on by exposure to emotionally powerful events or "critical incidents". The event may be sudden and unexpected or ongoing in nature.

Some staff may experience 'vicarious' or indirect trauma through witnessing trauma or violence, or being associated with a tragic event such as acute disaster recovery efforts. Others may experience 'compassion fatigue' as a result of exposure to human suffering or tragic situations that are more chronic and long-term. In many cases, the symptoms of vicarious trauma or compassion fatigue resemble those of victims experiencing direct trauma. Individuals with a prior history of significant trauma, instability in current life circumstances, or other vulnerabilities may be at highest risk.

Regardless of the source, traumatic stress may be one of the more serious occupation hazards experienced by staff. Dealing with traumatic stress is a specialist area and requires professional attention.

Burnout

'Burnout' is often used to describe a person who has become exhausted. Some signs of burnout are similar to the signs of stress, though are likely to be more severe. Signs of burnout within a team may include high turnover of staff; lack of team unity; a culture of blame; reluctance to take the initiative; increased sick leave; and decreasing effectiveness. Managers should watch out for these signs, and take action accordingly. Best of all, they should put in place working practices which prevent stress and burnout from occurring.

For further information see Managing the Stress of Humanitarian Emergencies, a UNHCR guide, by Sheila Platt[1]. Also see Humanitarian Action and Armed Conflict: Coping with Stress, by Barthold Bierens de Haan, published by the ICRC[2].

[1] Published 2001. Available at www.the-ecentre.net/resources/e_library/index.cfm or by using a search engine.

[2] Published 2001 (3rd edition). Available from www.icrc.org.

Back to TOC

Annex R - Syllabus for a Security Foundation Course

Users and Usage: The senior management team should actively ensure that a Security Foundation Course is developed specifically for your organization and that new staff attend the course and current staff can either demonstrate knowledge of the course's content or also attend. For staff who are responsible for developing and/ or implementing the course, a basic outline of the course is listed below. To supplement and support you with developing and/ or implementing the course, you can utilize the posters and DVD providing for the Security Awareness Week (23-27 May 2011).

Preparation: Security Foundation Course is an in-house course that normally lasts a few hours and up to one day. It is not only as a chance to inform staff about the organizational perspective but also as an opportunity to engage, activate and listen to staff.

The primary purpose of the course is to give staff an overview of how your agency's policies, principles and regulations relate to security and safety. While a discussion about what ways procedures are linked to policies, principles and regulations, a detailed examination of procedures should be reserved for the personal security and the security and crisis management courses. At each course, there should be a brief explanation about the different courses and who is expected to attend.

Before the course, all participants should have read:

- "ACT Staff Safety and Security Principles" (Annex A)
- Their organisation's policies that relate to security (section 2.8)
- The overall Security Plan, paying particular attention to the parts that relate to their specific jobs
- And, at least familiarised themselves with the outline of the ACT Safety and Security Guidelines .

Syllabus: As the Security Foundation Course is an opportunity to engage, activate and listen to staff, try to find the right balance between giving information and leaving space and time for questions and discussions.

- Introduce the main documents: Explain the purpose of each. Wherever possible, you should refer staff to the organization's plans and policies or ACT Alliance materials so they know which resources are available to them.
- 'Enliven' the main documents. Highlight how these documents relate the work of the organization and individuals. Depending on your agency's specific circumstances, you may want to reserve sufficient time to give certain issues extra attention like:
    - Implementing an acceptance strategy;
    - Relations with military, police, media or other agencies, particularly ACT members;
    - Communication systems, structures and equipment;
    - Incident reporting; or,
    - Medical evacuation (Medevac).

Such courses can raise a lot of questions and issues so make sure you follow up on these and report back to staff.

Back to TOC

Annex S - Syllabus for a Personal Security Course

Users and Usage: For the senior management team and staff who are responsible for developing and/ or implementing the course, the syllabus lists the topics that are normally included.

Preparation: Personal Security Course can be conducted in-house, with the ACT Alliance or externally. It can take a few hours and up to three days.

The primary purpose of the course is to train staff on security procedures that will affect their work. As this course applies all staff, all staff should be required to attend. That said, you may provide tailored courses for specific staff. For example, drivers require more details about vehicle maintenance and defensive driving than normal travelling staff. In such cases, you can opt to have drivers take part in a Personal Security Course and then attend extra sessions to cover their specific issues. Or, you might decide to create a modified Personal Security Course just for them.

As your organization probably will provide different types security courses, there should be a brief explanation about the courses and who is expected to attend. To supplement and support you with developing and/ or implementing the course, you can utilize the posters and DVD providing for the Security Awareness Week (23-27 May 2011).

Before the course, all participants should:

- Review their Security Foundation Course notes and readings (Annex R)
- Read the organization's Security Plan, paying particular attention to the parts that relate to their specific jobs

Syllabus: The syllabus below outlines the content of a typical Personal Security Course. These points are suggestions that should be modified to suit your organization and location.

1 Introduction to security risk management

1.2 Understand that risk is a product of both threat and vulnerability, and that lowering either threat or vulnerability can lower the risk

1.3 Understand that NGO security is usually based on acceptance by the local population, and that the perception of the NGO in the eyes of the local population is therefore vitally important

1.4 Be able to assess risk in a hostile environment

1.5 Be able to select appropriate security measures based on risk assessment

1.6 Understand the need to weigh risk against benefit – the 'risk-benefit calculation'

2 Personal Behaviour and Awareness

2.1 Understand the influence that personal behaviour has on security

2.2 Be aware of the importance of respecting local culture, and of some common pitfalls when it is not respected

2.3 Understand the need to dress appropriately to the local situation and culture

2.4 Be aware of the local situation and its implications for personal security

2.5 Tips for personal security including:

- When on foot, while walking
- Relaxing in the evenings and weekends
- In local restaurants, bars etc

- Relationships with local people
- Responsible sexual behaviour
- Awareness of local perceptions

2.6 Understand why bribery should be avoided, and be able to avoid paying bribes when under moderate pressure to do so

2.7 Special precautions and readiness for extreme emergencies and evacuation

3 Communications and Information Security

3.1 Briefed on communication systems, structures, and equipment

3.2 How to make e-mail more secure.

3.2.1 If appropriate, be able to use a VHF radio to a basic level, including:

- Send and receive simple messages
- Charge and care for batteries
- Speak securely, accurately and briefly on the radio
- Know the phonetic alphabet
- Be aware of the causes of ‘dead spots’ and how to deal with them
- Be aware of the approximate ranges of handheld, vehicle-borne and base unit VHF radios

3.3 Be aware of the need in many situations to have at least two independent means of communication with you at all times

3.4 Be able to send a basic situation report (sitrep) and/ incident report by radio or mobile

4 Travel

4.1 Understand basic travel procedures including:

- Risk-benefit calculation in deciding whether to make a specific journey and the importance of go/no-go decisions
- Travel authorisation
- Booking in and out
- Reporting on departure; at journey stages; and on arrival
- Understanding that all procedures, including the above, depend on the local context and should be adjusted when the context changes
- Vehicle maintenance checks

4.2 Understand the great danger of road traffic accidents and the main methods of avoiding them

4.3 Understand the need to keep a vehicle secure, including:

- Searching the vehicle before use
- Locking all doors while in the vehicle
- Parking face out
- Retaining enough room for manoeuvre when in traffic or enclosed spaces

4.4 Be able to behave appropriately at a checkpoint

4.5 Be able to plan a route

4.6 Be able to use convoy routines

4.7 Be aware of basic tips for security in hotels

5 First Aid

5.1 Be able to carry out basic First Aid appropriate to remote or insecure environments. This includes:

- Resuscitation
- Compose and use First Aid kits
- Trauma
- Burns
- Injuries from blasts, explosions and gunshots
- Fractures
- Improvise stretchers and carriers (only to be covered briefly – 5 minutes?)
- Effects of heat and cold
- Common illnesses and conditions
- Skill assessments

5.2 Practical and realistic exercises are to include procedures suitable for remote or hostile environments, including for blast injuries and gunshot wounds

6 Stress

6.1 Be aware of the danger posed by excessive stress

6.2 Be aware of methods for preventing excessive stress

6.3 Know the common signs of excessive stress

6.4 Know common ways of managing and relieving excessive stress

6.5 Know when and where to seek professional help for stress

7 Context specific risks and threats

7.1 Be aware of the likely threats and risks associated with a particular location, country, or task

7.2 Be aware of how to prevent and react to such threats

7.3 Threats and risks that could be included are:

7.3.1 Landmines and explosives

7.3.2 Sexual violence

7.3.3 Carjacking

7.3.4 Riots

7.4 Know how to use the appropriate equipment associated with preventing and reacting to local threats and risks

Back to TOC

Annex T - Syllabus for a Security Management Course

Users and Usage: For the senior management team and staff who are responsible for developing and/ or implementing the course, the syllabus lists typical topics that are often included.

Preparation: Security Management Course can be conducted in-house, with the ACT Alliance or externally. It can take a half-day and up to five days.

The primary purpose of the course is to prepare and support managers with security responsibilities.

As your organization probably will provide different types security courses, there should be a brief explanation about the courses and who is expected to attend. To supplement and support you with developing and/ or implementing the various courses, you can utilize the posters and DVD providing for the Security Awareness Week (23-27 May 2011).

Before the course, all participants should prepare themselves to use:

- "ACT Staff Safety and Security Principles" (Annex A)
- Their organisation's policies that relate to security (section 2.8)
- The overall Security Plan, paying particular attention to the parts that relate to their specific jobs
- And, at least familiarised themselves with the outline of these Guidelines.

Syllabus: The points below are suggestions that should be modified to suit your organization and location.

- Approaches to security: acceptance, protection, deterrence
- Security-related responsibilities of a field manager
  - Team leadership
  - People-management
  - Security assessments, including understanding the local context, influential actors and threats assessing the implications of political and security developments
  - Analysing the risks and likely benefits of a programme
  - Writing a security plan
  - Giving a security briefing
  - Writing sitreps and incident reports
  - Security coordination through ACT forum, with other ACT members and other agencies (UN, Red Cross, NGO)
  - Common security problems and dilemmas
  - Deciding on and managing an evacuation and/or relocation to a safer area
  - Organising security training for staff
- Winning acceptance among staff, local leaders and people
- Dealing with senior civil leaders, police and/or military commanders
- Handling the media
- Serious incidents: kidnapping, assault, rape, murder etc
- Securing buildings
- Managing communications
- Security aspects of administration:

  - Human resources aspects of security management: recruitment, contracts, briefing, discipline, termination of contracts etc
  - Financial security
  - Security of property, inventory management etc
- Stress: prevention and treatment
- The UN Security Management System

Annex U - Syllabus for a Crisis Management course or exercise

Users and Usage: For the senior management team and staff who are responsible for developing and/ or implementing the course, the syllabus lists typical topics that are often included.

Preparation: Crisis Management Course or Exercise can be conducted in-house, with the ACT Alliance or externally. It can take a half-day and to two days. To supplement and support you with developing and/ or implementing the various courses, you can utilize the posters and DVD providing for the Security Awareness Week (23-27 May 2011).

The primary purpose of the course is to prepare and support managers with security responsibilities with managing a crisis. In other forms, the purpose is to prepare particular staff and teams. The aim is to familiarise them with the procedures and decision-making processes likely to be required if such an incident occurs.

Before the course, the senior management team and staff who are responsible for developing and/ or implementing the course should discuss, in detail, the organizational and contextual issues to be covered. Also, you should create a plan for the various levels of staff so to provide the appropriate degree of information sharing and training.

As part of their preparation, all participants should be ready to use:

- "ACT Staff Safety and Security Principles" (Annex A)
- Their organisation's policies that relate to security (section 2.8)
- The overall Security Plan, paying particular attention to the parts that relate to their specific jobs
- And, at least familiarised themselves with the outline of these Guidelines.

Syllabus: The syllabus below outlines the content of a typical Crisis Management Course or Exercise. These points are suggestions that should be modified to suit your organization and location.

During the course and after the exercise, the following topics should be covered:

- Discussion of the main types of crisis assessed that could occur in the local situation. For example:
  - Kidnap
  - Rape
  - Murder
  - Mass casualties
  - Large scale robbery
  - Natural disaster like earthquake or forest fire
- Discussion of some decision-making dilemmas commonly posed by such crises
- The importance of having a single person in charge of the crisis
- Procedures for a Crisis Management Team for example communication, division of labour
- Discussion about which resources might be needed including relevant documents like staff emergency contact lists, organizational policies, etc
- Informing next of kin, keeping contact with them, providing reassurance and support
- Where to find specialist help, for example in kidnap negotiations
- Dealing with the press

An exercise should be conducted, using a fictional scenario relevant to the local situation. The exercise should pose practical and decision-making problems. It should be followed by a discussion designed to draw out and underline the lessons identified during the exercise.

Back to TOC

Annex V – Field Travel authorisation form

Users and Usage: For travelling staff, you may be asked to fill out this or a similar form. You can also use the form as part of your pre-departure preparations. By reviewing the considerations that need to be addressed when seeking authorisation, you can be better understand your agency's responsibilities for your safety and security.

Managers should note that this form is most relevant when adapted to the local situation and the working practices of the team. In many situations a travel authorisation form may not be necessary or appropriate. It is for the relevant line manager to decide whether it is required as a standard procedure.

For Security Focal Points, below there is a list of considerations that you can integrate into your process for granting travel authorisation.

Names of all people travelling	
Purpose of the journey	
Starting from	
Destination	
Route	
Date of journey	
Estimated time of departure	
Estimated time of arrival	
Any threats assessed to be relevant to this journey	
Precautions to be taken	
Any permissions needed from local authorities or others? Have they been obtained? Any conditions attached?	
Communications:	
Mobile phone? (Give number)	
Satellite phone? (Give number)	
VHF radio? (Give frequency and call sign)	
HF radio? (Give frequency and call sign)	
Give reporting times and locations	
Vehicle type and registration	
Name of driver	
Signature of lead traveller	
Print name	
Date	
Signature of authorising manager	
Print name	
Date	

Security Focal Points should consider the following before granting travel authorisation:

- Terms of Reference for the trip: What should be the benefits of the trip?
- Risk analysis: In addition to the analyzing the risks for a certain location, it is important to analyze your staff's vulnerabilities to these risks. While an experienced staff member may be permitted to travel in a high-risk area if circumstances demand, a more cautious decision should be made for travellers with less experience. Most aspects of security and safety are gender, age and diversity specific; a staff member of a given nationality, age, job title or gender may be more at risk, or run different risks, than others.
- Competence: What is the experience and competence of the traveller to cope effectively with likely security scenarios? Has the traveller had the right level of security training for potential threats they might face?
- Personal factors: The personal and family circumstances of the prospective traveller should be taken into account. Is the traveller willing to undertake the level of risk? The medical fitness of the traveller should also be assessed, including a medical check-up if appropriate. This assessment should include the staff member's general level of tiredness/stress.
- Partners: Have the views of other ACT members and humanitarian partners been taken into account?
- Checklist for Travel: has this been properly completed - are there any outstanding issues?

Back to TOC

Annex W – Risk Assessment Template

Users and Usage: Below is a standard format for assessing risks to be used by Security Focal Points and managers with security responsibilities.

Activity	Threats (Hazards)	Vulnerability				Gross Risk*	Existing measures to mitigate	Further measures required	Net Risk*
		Likelihood		Impact					
		Factors affecting likelihood	Level*	Factors affecting Impact	Level*				

* Different agencies use different ways to define levels and risks. For example, your agency may use “High,” “Medium,” or “Low” while another may opt for a 1-5 scale, whereas a third agency may choose a colour system. Your agency can also follow a system that is based on the security risks categories (section 2.3). In general, your agency should use the system that is easy for it to follow.

Back to TOC

Annex X – Traveller Disclaimer Certificate

Users and Usage: Every ACT agency should have a traveller disclaimer certificate/ form that visitors and other guests travelling in the organization's vehicles should sign. Below is a sample that can be modified accordingly.

Traveller Disclaimer Certificate

- I, (full name)………………………………….. hereby confirm that I am travelling to the following countries/ location under the auspices of the named organisation:

  ……………………………………
  ……………………………………
  ……………………………………
  ……………………………………
  ……………………………………

- For my own safety and/or that of the group**, I agree** during the visit to abide by the security advice from the ACT nominated trip leader (…………………………………………) who should accompany me. ***If I fail to abide by his/her advice, ACT partner is not responsible for anything that happens to me.***
- During the visit **I agree** to keep the organisation's trip leader informed of my movements.
- **I confirm** that I have visited my doctor and have the necessary vaccinations for the named countries/location**: I am fit to travel**. (In confidence to my trip leader, I have also disclosed any relevant information concerning medical conditions; allergies and general health matters that might affect my ability to complete this visit.)

Traveller

Signature……………………………

Name: ………………………………

Date: ………………………………

Nominated Trip Leader

Signature……………………………

Name: ………………………………

Date: ……………………………

Copies to be held by:

- Human Resources
- Security Focal Point
- Organisation sponsoring the visit
- Area Team (if relevant).

Back to TOC

Annex Y - Site Security

Users and Usage: This annex is primarily for Security Focal Points, security managers and managers with overall security responsibilities. The advice and checklists below should be modified and added to according to the realities of each location.

Site security refers to both physical and procedural security measures at each site. Access to a site is controlled through a series of physical and procedural "boundaries," both designed as methods for blocking would-be intruders from gaining access to the site. These boundaries may be:

- Physical, such as walls or fences;
- Physical and psychological, such as hedges or flowerbeds; and/ or
- Procedural, such as security sign-in and out; or any combination of these.

Keep in mind these different boundaries when selecting a site and maintaining the security of your organization's locations.

The ECHO Generic Security Guide provides useful advice on building security in annex 1, using the categories of:

- General location
- Physical security of the building
- Local infrastructure
- Arrangements for receiving visitors
- Identity of the owner

Guidelines on office and accommodation security for staff are in section 3.5.

Site Security Surveys

Each location should undergo periodic security surveys. Each survey should consist of:

- A physical review of the premises
- A review of in-place policy and procedures
- Interviews with the representative and staff

SAMPLE: Site Security Review Checklist

Office:

Date of Review:

Review Item	Notes	Remarks/Action
	Approaches - Do the office buildings have good access to routes and locations that are important for the programme?)	
	How is criminality in the area? Rate of incidence, type of crime..	
	Are there potential evacuation routes? Is the building accessible from many access points, or only one or two? (One or two may be easier to control.)	
	Is it discreetly located, or is it in a high profile location? Which is more beneficial	

Location	to your security in the current situation?	
	Can you overlook the premises, that is, look down at the building from a higher position? Does that matter in the current circumstances?	
	Are access routes to the building free from places for people to conceal themselves? (Keep shrubbery and bushes around residences and offices trimmed low.)	
	Is it close enough to the beneficiary population; other NGOs?	
	Proximity of 0ther NGOs, UN,	
	At what distance are the police or other security forces? How long does it take to reach the nearest police station on foot and by motorised transport?	
	Is the building close to a sensitive location? (E.g. a military or police barracks; a political party office; the house of a prominent politician, etc	
Physical security of the building	Are the walls strong enough to withstand likely threats? Are the windows barred?	
	Are the doors strong? Check locks, hinges, bars. Are the locks of good quality and the keys not easy to duplicate?	
	Is there a perimeter wall? How easy/difficult is it to surmount? Does it have barbed wire? Does it need barbed wire, or would that send the wrong signal to local people?	
	Are its gates strong? Can a guard look through the gate without opening it?	
	Is the roof difficult to access from the outside?	
	Is there a suitable place for a safe?	
	Is there a suitable shelter, in case of armed robbery, attack or fighting in the vicinity? A shelter should preferably be behind thick walls and out of sight of any window. Sometimes a central room or inner corridor is suitable.	
	Is there storage for valuable items?	
	Is there an alarm system; CCTV, or other relevant security equipment?	
	Are there sufficient fire safety measures, such as smoke alarms, fire alarm, primary and secondary escape routes?	

Safety Measures	Is there an emergency evacuation plan for the building? Is it practical? Does it take into account the specific needs and threats connected with gender, ethnic origin, age or other particular attributes that staff may have? When was the last fire drill carried out?	
	Are electrical installations sound and safe?	
	Is there sufficient parking, and will vehicles be secure?	
	Is there sufficient lighting, externally and internally?	
	Is the building close to a dangerous location? (E.g. a fuel store)	
	If fighting were to break out, would the building be potentially exposed to direct fire?	
	Is the building in an area prone to flooding earthquake or other problems? If so, is it protected against these?	
	Are there any health risks in the area? (E.g. sewage or rubbish facilities)	
	Are external electrical, telephone and gas supply boxes locked?	

Name of Reviewer: ___________________________________

Site selection

When choosing a site for a new office, warehouse or other operational workplace, consider:

- The neighbourhood
    - Make sure the site chosen is in a fairly reputable neighbourhood.
    - Avoid choosing a location in a high crime area.
    - Consider the location of the site in relation to passing traffic. High pedestrian traffic is statistically proven to increase vulnerability because it increases opportunity.
    - Consider the proximity to potential targets, such as military installations, embassies, or other high profile buildings.
- Affiliations
    - Consider the predominant people in the area, their ethnicity, religion, class, political affiliations, etc. Especially those in the immediate vicinity around the site.
    - It would not benefit your security to choose a site in an area where ethnicity of the site location conflicts with the ethnicity of the people we are serving.
- Accessibility
    - Make sure there are multiple routes in and out of the site.
    - Choose a site where at least one road surface is paved. (If possible.)
    - Check the width of the roads for vehicle manoeuvrability.
- Services
    - Make sure water is available.

    - Make sure electricity is available.
- Structure
    - Check the overall structural strength of the building.
    - Check to see if there are a sufficient number of windows (at least two) and if the windows are secured by bars.
    - Check the interior for sufficient office space and a reserve room for shelter.
    - Check the susceptibility of the site for hazards to fire, floods, landslides, strong winds, etc.
    - Make sure trees and vegetation do not provide natural hiding places (cover) for would-be intruders.
    - Check to see that visibility around the site is unobstructed.
    - Check the potential for modifications.
- Physical Boundaries
    - Clearly defined perimeters, even if just psychological, play a major role in discouraging intruders.
    - Check for natural boundaries, such as hedges or tree lines that separate the outer perimeter from the roadway or fields.
    - Check to see if inner perimeter boundaries exist. Inner perimeter boundaries may be hedgerows inside the line of trees that skirt the property.
    - At the same time, the “boundaries” and obstacles should not be such that one of your staff members or his/her closest family cannot get out quickly enough to escape danger, or get in quickly enough to seek safety. The balance is not easy to strike but the emphasis should be on getting out quickly.

Physical site requirements

Each location should comply with some basic security requirements. These requirements include:

- Each office/residence location should have an identified interior shelter room.
- Each shelter room should be securable with strong locks, where necessary have a bullet proof door, yet provide enough aeration for those who have to stay there to get the necessary air. It should contain:
    - Flashlights (3) and extra sets of batteries
    - First Aid kit
    - Communication Equipment:
        - Cell phones
        - Radios
        - Satellite telephone
    - Water - one of the 5 gallon office bottles for a dispenser should suffice
    - Food - nutritious food bars work well and do not take up much room per case.
    - Sandbags (If necessary).
- Offices/residences with “barred” windows should have at least one set of bars on hinges to provide an escape route in case of fire.
- Each office/residence/warehouse should have an appropriate number of fire extinguishers.
- Each office/residence with external fuse/breaker boxes should cover or lock the external fuse/breaker boxes.

- Each office/residence/warehouse should have sufficient exterior lighting to illuminate the exterior premises.
- In zones of conflict, offices/residences should have blast film installed on all exposed windows.

Mandatory procedures

Physical boundaries are complemented by procedures. Procedures are designed to establish security-conscious patterns of behaviour. Procedures determine who enters the building; who has access to certain areas; who has access to what and under what circumstances; and when.

Each office with more than five staff members should consider controlling access to the building by posting a guard(s) or by simply having a receptionist in the front lobby to screen people entering the building.

Visitors

Each office should establish and maintain a record keeping system of persons who enter the building. This record system should include:

- The name of the person
- The name of their organization
- The time they arrived and the time they leave
- The name of the person they came to see

All visitors should be accompanied when on the premises. Unaccompanied persons are to be challenged in a low-profile manner. For example, one might ask “May I help you?” or perhaps, “Who are you here to see?” Persons without reasonable explanations as to why they are on the premises should be immediately reported to the organisation’s representative or to security.

- Workmen/Delivery Persons
- Work trucks and delivery trucks should be inspected before they are allowed on the premises.
- All workmen and delivery persons should be supervised at all times when on the premises.
- Work trucks should be inspected prior to leaving the premises at the end of each day.
- Workmen without proper identification and authorization should not be allowed on the premises.
- Each office using conventional keys for the office/residence/warehouse(s) should establish a key control system. The key control system should include:
    - A list of what keys are assigned to whom.
    - A proper lock box for duplicate keys (duplicate keys should be marked with a number code only)
    - The master list of the number codes should be kept by the senior most manager
- Each office should establish daily closing procedures and designate a person(s) who is responsible for checking the premises, the lights, the locks etc., to ensure the office is secure.

Back to TOC

Annex Z – Terms of Reference for security focal points and key contact details of ACT Security Working Group and ACT Alliance management

Users and Usage: The terms of reference is for senior managers who are hiring and managing a Security Focal Point. For SFP's this annex lists key contact details of the ACT Security Working Group and ACT Alliance management.

Kiruja Micheni, Chair of ACT SWG, Corporate Security Manager, Christian Aid
Tel +44(0) 2075232379
Mobile +447788578189
Email: kmicheni@christian-aid.org Skype: caid-kmicheni

Eirik Kirkerud, Programme Officer, Norwegian Church Aid
Tel +47 932 42 481
Email ehk@ nca.no

Sicko Pijpker, Security Coordinator, ICCO
Tel +31 622 034 422
Email Sicko.Pijpker@ICCOenKerkinActie.nl

At ACT Alliance Secretariat:

John Nduna, General Secretary
150 rte de Ferney, 1211 Geneva 2, Switzerland.
Telephone office: 00 41 22 791 6032.
Mobile: 00 41 79 203 6055.
Fax: 0041 22 791 6506
E-mail: jhn@actalliance.org

Box 1: Sample Terms of Reference for ACT Forum Security Focal Points

Background: The "ACT Staff Safety and Security Principles" outlines the key principles of the ACT Alliance approach to staff safety and security. The principles commit the management of each member of the alliance to take responsibility and hold themselves accountable for ensuring the safety and security of its staff. They equally commit each staff person to take personal responsibility for her/his own safety and security. ACT national and regional forums provide a shared platform or space for ACT members to discuss and coordinate issues related to staff safety and security. While some forums have nominated security focal points from within their membership in the past, this practice has been ad hoc and done without systematic guidance. The need to capture learning from experiences to date and to make such a role clearer and better supported

Purpose: To facilitate the strengthening of ACT national and regional forum capacity on security issues, promoting common strategies, actions and responses among ACT members in-country.

Functions: ACT Security focal points will…

Promote the coordination of local security arrangements for ACT Alliance members' in-country via the ACT Forum. When requested,

Work with ACT members' staff responsible for security, where applicable, to review security procedures for all ACT Alliance members and make recommendation for field operations, offices, accommodation, warehouses and the personal security of staff;

Review and make recommendations to improve security as identified;

Assist with the development and implementation of emergency evacuation procedures and plans, and in cooperation with the ACT Forum Coordinator, be responsible for coordinating the implementing of the procedures should this become necessary.

Promote the practice of systematic security briefing of newly arriving staff and visitors among all ACT organisations

Promote the sharing of up to date and appropriate security information at the forum level, ensuring that it is also communicated to field staff.

Promote the inclusion of essential security costs in ACT appeals.

Liaise regularly with the global ACT Security Working Group chair.

Be well briefed on all security developments within the programme area, and provide regular security analysis and in-house briefings for the ACT Forum

Encourage all forum members and their partners to remain updated on changes to the security situation

Promote the development and implementation of common security strategies, actions and responses among ACT members giving due regard to the local security environment

Promote the principles and positions of ACT among ACT members in-country, as expressed in the following documents: "ACT Staff Safety and Security Principles" (2010); ACT Staff Safety and Security Guidelines (2011); SCHR Position Paper on Humanitarian-Military Relations (2010)

Encourage ACT forums to have strong link with external security forums such as those of the UN or NGO networks