SAFETY AND SECURITY GUIDELINES

INCLUDING CRITICAL INCIDENT AND CRISIS MANAGEMENT AND PREVENTION

18 May 2015

Produced by Global Connections in association with Steve Penny, Consultant.
CONTENTS

1. Introduction
2. Definitions
3. Safety and Security
4. Selection & appointment, induction & arrival and ongoing supervision
5. Being Prepared
6. Critical Incident Response
7. Crisis Response
8. Abduction

Appendix 1: Decision-making flowchart
Appendix 2: Critical Incident Report Form
Appendix 3: Security Incident Report Form
Appendix 4: Logbook
Appendix 5: Resources and contacts
1. INTRODUCTION

These guidelines are designed to help organisations take safety and security issues seriously. They give practical advice on preventing critical incidents from happening and crises developing, as well as knowing how to manage such events if they do occur. They have been written to assist any UK based agency or UK church sending staff or volunteers overseas. The principles should be applied to all types of staff including mission partners, volunteers working overseas, national staff and UK staff visiting field locations. Agencies and churches should also apply them in all contexts, both long and short term, although some different procedures might be needed in each context.

The safety and security of mission partners and their families is vitally important. However no area of the world or working situation is completely risk-free. Accidents, safety concerns and security incidents are a reality. This is especially true when sending staff to remote or insecure areas.

While we can never eliminate all risk, we can seek to minimise it. Developing clear security guidelines and preparing for responding to critical incidents or crisis situations is an essential first step in dealing with events. Preparation can reduce the risk of an incident occurring, or diminish its impact.

At the same time, we need to acknowledge that the love of Christ calls us to work in places where safety and security are difficult to guarantee. Many Christians living in comfort and prosperity need to hear again the call of Christ to be willing to suffer for him. The Lausanne Commitment (Section IIC2) has some helpful insights into this issue. However as organisations we have a clear “duty for care” to minimise risk and deal with crises effectively. There can be no excuse for poor security policies or lack of clear crisis management procedures.

It is impractical to provide “off the shelf” policies and procedures that fit all locations, circumstances and the needs of all groups. The contents of this document are intended as general guidelines only and have been developed to help agencies and churches think through and develop their own policies and procedures as part of their own comprehensive safety and security risk management system.

It should be noted that the use of the term “staff” throughout this document is a generic word, which is used to include all categories of people and their families working or visiting overseas, including volunteers and those who are self-supported.

Global Connections has produced these guidelines in consultation with its members and other experts.


1 From The Cape Town Commitment - A Confession of Faith and a Call to Action © 2011 The Lausanne Movement, found at www.lausanne.org/en/documents/ctcommitment.html
2. DEFINITIONS

The following definitions are taken from the EISF briefing Paper on Crisis Management of Critical Incidents. These guidelines use these concepts throughout.

A critical incident is an event (or series of events) that seriously threatens the welfare of personnel, potentially resulting in death, life-threatening injury or illness. Most critical incidents – although they may have potentially severe impacts on individual staff and programmes – do not have wider implications for the organisation as a whole and can therefore be managed by regular management structures, with additional support from headquarters if required.

A crisis is an event that significantly disrupts normal operations, has caused or is likely to cause severe distress or has severe consequences for individual staff or organisations. It requires out of the ordinary measures to restore order and normality, thus demanding immediate action from senior management. Crises can come in various forms, and include events threatening an organisation's reputation, image, programmes, assets, financial stability or the safety and security of its staff. In this last case, a crisis may be precipitated by a critical incident involving one or more staff members.

A critical incident (or series of such critical incidents) becomes a crisis when its nature, severity or broader consequences for an organisation warrant a response beyond the capacity of routine programme management mechanisms, requiring leadership and coordination from senior management level.

Critical incidents that frequently constitute crises include but are not limited to:
- Abduction, kidnap or hostage-taking
- Murder or death in suspicious circumstances
- Incidents causing multiple casualties and requiring urgent response (medical, road traffic accident, operational, psycho-social)
- Arrest or detention
- Other security situations or events causing a high degree of threat to staff
- Complicated or large-scale evacuation, or medical evacuation (“medevac”)

When such incidents occur, special structures and policies may be activated to supplement regular management capacities.

An Incident Management Team (IMT) manages a critical incident at country level. IMTs may be formed in cases of incidents not constituting crises, where they will operate under regular management structures. In the case of a critical incident constituting a crisis, this team needs to work under the direction of the Crisis Management Team.

A Crisis Management Team (CMT) manages a crisis situation at headquarter (or regional) level. A CMT is activated when a critical incident or any other situation is determined to be a crisis by senior management. The composition and role of a CMT differs according to the type of crisis.

A Crisis Management Plan describes mechanisms, responsibilities and protocols to be activated by an organisation in the event of a crisis.

3. SAFETY AND SECURITY

Prevention is always better than cure. It is vital that organisations both plan and manage the safety and security of staff thoroughly.

Safety and security management is a huge subject and it is important to take many areas into consideration such as:-

- **Risk analysis**: Ensuring that all locations undertake a risk analysis for both safety and security.
- **Briefing and training**: Ensuring staff are well informed before and during their travel or assignment about the possible risks and that essential training is given especially for high risk locations and first aid.
- **Travel**: Ensuring travel is managed in a safe way. In particular ensuring no go areas and curfews are identified and communicated widely. Ensuring travel is monitored and tracked appropriately. This includes keeping vehicles in good conditions, ensuring all drivers handle their vehicles safely as a high proportion of deaths are due to vehicle accidents.
- **Administration**: Ensuring people are aware of what documents to carry, including identity, and insurance information. Ensuring careful administration of money, information and valuable items. Ensuring personnel are registered with appropriate authorities.
- **Communications**: Gathering information on landline and mobile usage. Where radio use is essential, having clear radio procedures and keeping communications equipment in good condition. Developing and communicating clear policies on use of social media.
- **Property**: Ensuring buildings are secure and recruiting and managing guards appropriately. Keeping fire risk to a minimum and ensuring buildings have clear fire safety procedures and maintained fire equipment.
- **Health and medical**: Ensuring health and hygiene of staff is taken seriously as in many cases health risks are a greater threat to life than security risks.

One of the best ways of preventing security problems, especially in areas of insecurity, is to have good relationships with local staff, other missions and NGOs, UN bodies, local communities and local government officials. This also involves many things, including:-

- Spending time building good relationships with a variety of different organisations and individuals
- Ensuring staff are registered with local authorities appropriately
- Coordinating with local security forces (if this does not compromise an organisation’s integrity) and other organisations

Consequently it is important for an organisation to have clear policies on safety and security matters. In particular, good safety and security management requires organisations to have both a Safety and Security Policy which links into a Crisis Management Plan and a safety and security plan specific to each location where staff are based.

**A Safety and Security Policy** is a statement of intent that demonstrates a responsibility and commitment to all staff, including international staff, national staff and volunteers. It helps to create the safest and most positive environment for staff and to show that the organisation is taking its responsibilities seriously.

In addition to overall safety and security matters, it is also important to develop an organisation’s preparedness and ability to respond to and **manage critical incidents and**
crises. Whilst every incident is unique and will require a tailored response, it is paramount that essential capacities are in place before an incident occurs, to enable an organisation to adequately manage the situation in real-time.

1. All organisations should have a Safety and Security Policy regardless of whether or not they work in a high-risk area, as situations can happen unexpectedly.

2. The policy should be clearly written and should be easily understandable. Policies and procedures should be written with a holistic approach in mind across all departments. It should be integrated with all other HR and member care policies and be an integral part of an organisation’s risk management analysis. The policy should be reviewed on a regular basis, preferably every year.

3. One of the aims of the policy should be to identify clear management structures so that everybody knows who should be informed and involved so that the best standards of care can be offered.

4. The policy should guide an organisation’s procedures to ensure the safety and security of staff. It should include everything that needs to be in place to activate critical incident and crisis responses. The policy should include areas such as:-
   - Assessing risks in the location of work and deciding on acceptable levels of risk
   - Training, briefing and equipping staff
   - Security and safety while travelling
   - Strategies for security including managing the organisation’s image
   - Reporting and managing critical incidents and crises

5. The policy should be given to all staff and volunteers who work in or visit overseas locations. It should be an integral part of the staff handbook, orientation and training programme.

6. The policy should clearly outline the level of responsibility for all categories of staff: contracted staff, seconded staff, volunteers, consultants, staff of partner organisations, national and international staff (these are determined by the relevant contractual and labour law frameworks, which vary by country). In addition, organisations should be explicit about whether and to what extent they will accept security responsibility (including crisis response) for individuals for whom they have no legal responsibility but may have a moral duty of care. These responsibilities should be communicated to relevant staff and partners, to curb unrealistic expectations and potential liability issues.

7. In situations where a staff member is seconded to a local partner, the local partner should also be encouraged to develop safety and security policies and procedures, which includes critical incident and crisis management.

8. Clear procedures based on the overall policy should be developed and then adapted as appropriate for each overseas location.
4. SELECTION & APPOINTMENT, INDUCTION & ARRIVAL AND ONGOING SUPERVISION

Taking potential crisis situations into account during selection, induction and supervision is important in all settings. However, in high-risk situations where there are serious external risks, it is especially important.

As a result each agency or church should take regard of the following:

Procedures relating to selection and appointment
- All potential staff working overseas should be informed of any possible risks associated with a placement at the start of any recruitment, appointment or re-deployment process.
- The application process should ensure basic health and psychological screening of applicants.
- Criteria relating to a person’s suitability for being appointed to work in a high-risk area should be clearly set out in the selection process and during the interview process applicants should be asked about previous high-risk areas and crisis situations in which they have been involved as appropriate.

Procedures relating to orientation, induction and arrival
If staff are properly trained and managed, they are much more likely to react well to any incidents that might happen. All staff should be familiar with policies and procedures and be confident in their own abilities and those of their colleagues to act responsibly and decisively when necessary.
- The Safety and Security Policy, including managing critical incidents and crises, should be integrated into the staff handbook or appropriate document and all personnel should be required to acknowledge in writing that they have received and understood it.
- Orientation should be provided for all categories of staff relating to safety and security including critical incident and crisis management.
- Safety and security must be the responsibility of all staff and they must be equally committed to the process to ensure success.
- All staff should know how to behave appropriately in the culture and security context relevant to their placement.
- All staff should undertake security and safety training prior to departure including travel and personal security elements.
- Staff working or visiting high-risk areas should be provided with additional appropriate specialist training.
- Appropriate equipment should be made available such as first aid kits.
- Induction relating to specific situations should be provided on site on arrival.
- Relationships with Embassies should be established. All staff members and families should be registered with the Embassy. The organisation and its staff should be familiar with the Foreign and Commonwealth (FCO) travel advice relating to the country www.gov.uk/foreign-travel-advice.
- Additional advice should also be sought from local Christian leaders, other agencies and international bodies. Appropriate use should be made of any UN traffic light system for entering restricted areas.
- A risk assessment should be carried out for each location before the placement of any personnel.
Procedures relating to ongoing supervision

- Staff working in a high risk or stressful situation should have regular periods of rest and refreshment away from their work place. This should be in addition to normal holiday entitlement. The organisation should check regularly that staff stress levels do not rise too high.
- Reporting mechanisms should be in place for work-related injuries, sickness, accidents and fatalities, and should be monitored to help assess and reduce future risk to staff.
5. BEING PREPARED

It is easy to assume that everyone knows what is appropriate in a situation of a critical incident, crisis or potential crisis. This is rarely the case and there is often an absence of specific expectations. Clear guidance needs to be given to staff on many issues.

The following is the basis of a check-list:

Organisational actions
- Agencies should ensure that all staff can access the policy and procedures swiftly, that they can be implemented reliably, and everyone understands their role and responsibilities and those of others
- All staff should be updated regularly on security, travel and health risks together with evacuation procedures for the specific country or region
- Agency/church obligations and individual responsibilities in relation to possible risks should be clearly communicated to staff
- Risk assessments should be regularly evaluated and updated
- Agencies should provide adequate health and evacuation insurance cover which includes health, medevac, disability, and life cover. When working or travelling to areas where kidnapping is a risk then special contingency insurance should be arranged to cover for the deployment of specialised security advisers. Local insurance options for local staff should also be sought
- Abduction profile questions should be asked of all staff, and answers should be stored in a safe place
- Agencies/churches should establish access to funds that will be adequate for emergencies for all staff members. In the case of married couples, both partners should be able to access the funds in the event of an emergency
- If national elections are due in a country where staff are working, discussion should be had with staff in advance those elections regarding additional security risk and potential changes to the evacuation procedure

Staff member actions
Each staff member should:
- give priority to attending briefings and reading information about security, travel and health risks together
- be familiar with the evacuation procedures for their specific country
- appoint a current power of attorney for every adult family member
- have an up to date will and its location should be known by their power of attorney
- notify their organisation about the details of whom to contact in an emergency
- notify their organisation of their wishes in the event of a death overseas, including guardianship of children
6. CRITICAL INCIDENT RESPONSE

A critical incident (CI) which can be managed by regular management structures, with additional support from headquarters if required. (See definition in section 2)

An Incident Management Team (IMT) manages a critical incident at country level where they will operate under regular management structures.

Not all critical incidents require a formal crisis response. At country level, critical incident preparedness needs to be part of the country security management plan. When a critical incident is determined to constitute a crisis due to its wider nature, headquarters level response will be activated (see Section 7).

Composition of an Incident Management Team (IMT) is case-specific, but members are usually drawn from existing coordination or leadership teams. Depending on the scale, severity and complexity of an incident, as well as management capacity at field level, IMTs may opt to deploy additional staff to support or coordinate. The potential psychosocial impact exerted on team members by incidents should also be taken into account when assessing field incident management capacity.

Common tasks undertaken by an IMT include:

- Temporary suspension of activities
- Evacuation of staff, including medical evacuation
- Repatriation of anyone who has died
- Liaison with local and national authorities, embassies, aid agencies, and other relevant actors
- Support to families locally or national staff victims
- Monitoring and management of local media
- Support to affected project and mission staff (including psycho-social support)
- Immediate revision of risk analysis in light of the incident
- Liaison with the home office(s) of the person/people affected and/or international office

- Appoint a Critical Incident and Crisis Management Coordinator who has overall responsibility for developing, completing and implementing its Critical Incident and Crisis Management and Prevention policies. In each location, a local Critical incident and Crisis Management Officer should be appointed as far as possible

- The Critical Incident and Crisis Management Coordinator should keep knowledge, policies, procedures and best practice requirements up to date and ensure local Critical Incident and Crisis Management Officers are adequately trained.

- Agree about and ensure that there is clarity on whom to contact overseas and in the home country.

- Regularly review security procedures at staff meetings and ensure all changes in the security situation are communicated to all staff.
7. CRISIS RESPONSE

A crisis is an event that significantly disrupts normal operations, has caused or is likely to cause severe distress or has severe consequences for individual staff or organisations. It requires out of the ordinary measures to restore order and normality, thus demanding immediate action from senior management. (See definition in section 2)

It is important to develop clear plans for how to deal with a crisis, including the constitution and formation of a crisis management team. This plan should not be static and requires regular review, ongoing training and professional support.

Crisis Management Plan
The Crisis Management Plan should be designed to create, maintain and develop organisational ability to respond to and manage a crisis in an adequate manner. For a timely and appropriate response the plans should be regularly updated, reviewed and simulated. They should include:

- Definitions and types of crises
- Notification and reporting procedures
- Clear and effective decision-making structures
- Roles and responsibilities for the key members of staff
- Protocols and formats for each possible situation

Professional management for such critical situations needs to follow a number of key elements listed below.

Crisis Management Team (CMT)
A CMT manages a crisis situation at headquarter (or regional) level. A CMT is activated when a critical incident or any other situation is determined to be a crisis by senior management (see Appendix 1 - Decision Making Flowchart). The composition and role of a CMT may differ according to the type of crisis and it should be as small as possible while including as many areas of expertise as necessary for fast decision-making and information flows, and efficient information management.

The responsibilities and the level of authority that the CMT holds should be clearly defined in the crisis management plans without restricting the liberty to fast decision-making if the situation requires it.

Key responsibilities of CMTs include:

- Strategic decision making
- Ensuring that staff safety and security are assessed and managed
- Management of the organisation’s legal, reputational, financial and other risks
- Defining and implementing a crisis response strategy with clear reporting structures to senior management
- Authority to ensure implementation of defined strategy, including staffing and directing the IMT
- Defining and implementing a media strategy
- Managing family support and liaison
- Managing the internal information policy
- Consulting with all relevant internal and external stakeholders
- Managing crisis information including collation, analysis, distribution and storage
- Defining the moment that the crisis ends
- Dismantling the CMT and handing over to regular management structures
As CMT members are pre-defined they should all receive relevant training and also have a shadow/ replacement available for operating rotation systems for long-term crisis situations.

The composition of a CMT may vary depending on the type of crisis, but it should always include:

- CMT leader: In charge of crisis management and accountable to senior management
- Operations Manager – someone who understands the field operations
- Human Resources: HR issues, family liaison and support
- Media and Communications: Implementation of media strategy
- Assistant: Minute taking, logbook keeping and other tasks

**Communications and Reporting**

It is important to have clear communications procedures in the event of a crisis situation. There should be a specific person in the CMT responsible for the overall communications. There needs to be an understanding of what is public and what is private. The following are examples of some of the communications areas that should be covered:

- the family and home churches
- authorities, locally at Embassy level and in own countries
- media in all locations
- other agencies in all locations
- local partner

**Post-Crisis Follow-Up**

All crises require some degree of follow-up including the following:

- Aftercare including counselling of staff and their families, practical support, and administrative follow-up
- Debrief and evaluation including analysis of the incident and review of the quality of the crisis management
- Information management of documents and electronic data relating to the crisis
- Operational implications such as a review of the risk analysis
- Feedback and ongoing liaison with external stakeholders including expressions of gratitude for any support given
- Aftercare of the crisis management team itself and all those involved


8. ABDUCTION

Abductions have risen sharply in particular contexts in the past decade. Abduction is a "unique form of critical incident", characterised by its ongoing, "live" nature, often extended duration, the pressure of decision-making and uncertainty. It will always need to be managed in as a crisis due to its potential effect on an organisation.

Though the essential pillars of effective critical incident and crisis management response mechanisms apply, abduction's idiosyncrasies demand a more tailored response, under the umbrella of broader critical incident and crisis management plans and professional security advice.

Motives for abduction vary widely according to the country or the nature of the groups involved. However, while each case is unique, often a pattern can be observed. Based on this, there is a set of characteristics that tend to repeat, such as the long duration combined with a need for a fast and effective response, the impact of decision-making, confidentiality management and the large number of stakeholders that are involved.

First Response
Apart from the principles of critical incident response the following steps can be followed during the first phase of a known or suspected abduction:

- Establish the facts and complete the critical incident report form
- Start an incident log and form the IMT
- Account for all staff and assess risks
- Allocate dedicated phone numbers for communications between the key actors
- Prepare potential recipients for receiving the first call(s) from the kidnapper(s) in case contact is established by phone
- Identify and prepare the person who will be the Communicator
- Consider abduction scenarios
- Contain and control the spread of news about the incident
- Conduct stakeholder analysis
- Arrange for external abduction management support capacity as required

Abduction management
Putting together a plan for such an incident is difficult as strategies that have proved successful in one case or context are not necessarily suitable for another. Every strategy will be based on certain assumptions and bear certain risks and depending on the dynamics of the situation there are a few basic elements that apply to most abduction cases:

- Staff rotation – a rotation plan for the first days of the incident for the staff who will be supporting the crisis response.
- Stakeholder management – select one key channel of communication to reach the involved stakeholders.
- Mediators – third parties who can assist or get involved in the resolution of the case.
- National staff – if chosen to get involved, they can be key in maintaining links to local communities, networking or acting as Communicators with kidnappers.
- Information security and confidentiality – although difficult to control, it is imperative to guarantee maximum confidentiality regarding the situation.

Flowcharts must be tailored to an organisation’s management structure. The model below is therefore simplified, reflecting only major steps in the initial decision-making process.

1. Field reports critical incident to HQ (describe reporting chain in the field)

2. HQ (describe who receives incident report, whom the recipient must inform, and who decides whether incident constitutes a crisis).

3. Decision on whether to activate the Crisis Management mechanism.

**YES**
Activate:
- CMT
- IMT
- Relevant Protocol
- Logbook

**NO**
Regular line management retains responsibility for incident management.
Activate:
- Relevant protocol

Consider activating (incident-dependent):
- IMT
- Additional CI management support
- Logbook

CRITICAL INCIDENT REPORT FORM

<table>
<thead>
<tr>
<th>Reported by</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Country/Project</td>
<td></td>
</tr>
<tr>
<td>Date of report</td>
<td></td>
</tr>
<tr>
<td>Date and time of incident</td>
<td></td>
</tr>
<tr>
<td>Exact location of incident</td>
<td></td>
</tr>
<tr>
<td>Incident description</td>
<td></td>
</tr>
<tr>
<td>(include details of who is affected, what has happened and what has been done so far)</td>
<td></td>
</tr>
<tr>
<td>Current location of affected personnel</td>
<td></td>
</tr>
<tr>
<td>Identity of deceased personnel</td>
<td>1</td>
</tr>
<tr>
<td>Name:</td>
<td></td>
</tr>
<tr>
<td>Nationality:</td>
<td></td>
</tr>
<tr>
<td>Gender:</td>
<td></td>
</tr>
<tr>
<td>Identity of injured personnel</td>
<td>1</td>
</tr>
<tr>
<td>Name:</td>
<td></td>
</tr>
<tr>
<td>Nationality:</td>
<td></td>
</tr>
<tr>
<td>Gender:</td>
<td></td>
</tr>
<tr>
<td>Medical condition:</td>
<td></td>
</tr>
<tr>
<td>Other staff in project location</td>
<td></td>
</tr>
<tr>
<td>What action has been taken/in process?</td>
<td></td>
</tr>
<tr>
<td>What steps need to be taken?</td>
<td></td>
</tr>
<tr>
<td>Contact details of key staff</td>
<td></td>
</tr>
</tbody>
</table>
SECURITY INCIDENT REPORT FORM

Please use this form accurately but imaginatively if it does not exactly fit the incident you need to describe. Complete it as soon as possible after the incident and send to your Manager.

1. Country
2. Location
3. Name of person completing form
4. Name of person/s involved in incident
   Confidentiality: Do not enter the name here if the incident relates to sexual assault or rape
5. Date of incident
6. Today’s date
7. Nature of injuries / deaths, if any:
   - Staff
   - Partners/other NGO staff
   - Others
8. Type of incident (delete those not appropriate)
   - Kidnap, Abduction
   - Detention, Arrest
   - Robbery, Ambush, Theft, Looting
   - Personal Assault
   - Sexual Assault
   - Threats, Harassment
   - Carjacking
   - Difficult encounter with military forces
   - Conflict (cross-fire, sniping, shelling, aerial bombardment, etc).
   - Landmines, UXO
   - Other

Incident description:

Describe briefly what happened, where, when, who was involved, the impact on them and all immediate actions taken.

Did the incident involve weapons?

Was property taken or lost? If so, what?
**Background:**

Do you know who the perpetrators were? *(If appropriate)*

Was this incident targeted at you or your agency? *(In the case of a report about an incident happening to another agency, was it targeted at them?)*

Do you recall any indicators prior to the incident?

Who did you report the incident to locally? *(eg authorities, other agencies and communities)*

**Lessons learned and recommendations for remedial action:**

Do your security guidelines cover this type of incident? Were the guidelines followed? Do the guidelines need to be revised?

Please suggest other aspects of the security management system that need to be updated or revised.

Please suggest specific measures that may help avoid this type of incident in the future.

Please request follow-up actions to be taken locally.

## LOGBOOK

Sample Format

<table>
<thead>
<tr>
<th>No</th>
<th>Date</th>
<th>Time</th>
<th>Event (Meeting, Phone, etc.)</th>
<th>Participants</th>
<th>Content</th>
<th>Decisions</th>
</tr>
</thead>
</table>

RESOURCES AND CONTACTS

1. RESOURCE AGENCIES

EUROPEAN INTERAGENCY SECURITY FORUM (EISF)
EISF is an independent network of Security Focal Points who represent European-based humanitarian NGOs operating internationally. EISF is committed to improving the safety and security of relief operations and staff, by strengthening risk management in a way that allows greater access to and impact for crisis-affected populations. [www.eisf.eu](http://www.eisf.eu)

INTERHEALTH
Interhealth is an international health charity preparing, sustaining and supporting the health and wellbeing of individuals working around the world.

UK: Interhealth Worldwide, International Health Centre, 63 – 67 Newington Causeway, London, SE1 6BD Telephone number: +44 (0) 20 7902 900
[www.interhealthworldwide.org](http://www.interhealthworldwide.org)

Kenya: InterHealth Worldwide
International Health Centre, 331 Masanduku Lane
Nairobi, Kenya
P.O. BOX 19595 CODE 00202 KNH
Nairobi, Kenya
Email: info-kenya@interhealthworldwide.org
Tel: +254 (0) 714763560 / +254 (0) 203861023

SAFER EDGE
Safer Edge was formed in 2003 with the aim of “supplying specialist security and safety advice and training to the humanitarian and development sector.” Safer Edge works on the principle of Inclusive Security – using a combination of approaches to ensure the safety and security of everyone operating in difficult environments whilst still enabling programmes and operations to work as effectively as possible. They provide consultancy services and organise security and crisis management related training courses – see their website: [www.saferedge.com](http://www.saferedge.com)
Steve McCann 07793 821 476 - [steve.mccann@saferedge.com](mailto:steve.mccann@saferedge.com)
Brennan Dwyer 07828 704978 – [brennan.dwyer@saferedge.com](mailto:brennan.dwyer@saferedge.com)

REDR
RedR UK trains humanitarian NGO workers and provides recruitment, technical and membership services to aid workers worldwide. In particular RedR has been organising security training courses and providing security consultancy in the UK and around the world since 1995. See training courses [www.redr.org.uk/en/Training-and-more](http://www.redr.org.uk/en/Training-and-more).

HOSTAGE UK
Hostage UK is an independent charity that supports hostages and their families both during and after a kidnap. Look up the family guides on a number of subjects: [www.hostageuk.org](http://www.hostageuk.org)
2. ONLINE SECURITY AND SAFETY TRAINING

Disaster Ready
Disaster Ready is a free, easy to use online training resource designed to help prepare aid workers for the demands they face in the field. Created by experts in humanitarian assistance and staff development, this initiative is a collaborative, non-profit effort supported by prominent aid agencies and the Cornerstone on Demand Foundation. Travel and security online training - [www.disasterready.org/courses/staff-safety](http://www.disasterready.org/courses/staff-safety)

IFRC
The International Federation of the Red Cross and Red Crescent Societies (IFRC) has made available to the public its [online security training](#). Once into the website then type in to select “Stay Safe Personal Security” The course takes 3 hours and on completion of a final test a certificate is available for print.

There is also a [short video](#) of how to register for online training:

UNDSS
UN Department of Safety and Security (UNDSS) Online Security training; information and training on physical safety and first aid in remote locations – [www.dss.un.org/dssweb](http://www.dss.un.org/dssweb)

3. RESOURCES

ODI Security Management in Violent Environments
The [ODI Good Practice Review](#) 8 Operational Security Management in Violent Environments is one of the most widely used and respected security manual for most INGOs and increasingly for mission agencies. It was written in 2000 and updated in 2010.

EISF Comprehensive Guidelines
A huge library of guidelines, policies, procedures, sample documents and templates relating to security are available as free downloads at [www.eisf.eu/resources-library/](http://www.eisf.eu/resources-library/).

Abduction Management, May 2010
Essential and thorough guidance for all aspect of abduction management. [This paper](#) explores the dimensions of effective, proactive abduction and kidnapping response mechanisms. It complements the EISF Briefing Paper *Crisis Management of Critical Incidents*.

Crisis Management of Critical Incidents, April 2010
An essential and thorough [guidance](#) for all aspects of crisis management.

Family First: Liaison and Support during a Crisis 2013
An invaluable [reference document](#) for those responsible for critical incident and crisis management within organisations.

Act Alliance Security Assessment Tool
This [security assessment tool](#) assesses security management and practices in medium and high risk areas. The tool has four parts: a guideline on how to use the assessment tool; a table to score the level of security management and practices per topic/indicator; a checklist with questions for reflection on important security management issues and to
identify areas of improvement; and a checklist to assess the level of security preparedness of the individual worker/traveller.

**ECHO Generic Security Guide for Humanitarian Organisations**
The aim of this guide, commissioned by ECHO, is to help humanitarian NGOs manage their security effectively. It does so by offering tools, guidance and resources allowing agencies to think through their security policy and procedures.

**Interhealth**
A range of resources and training are available from Interhealth, including the following papers found at:

*Trauma Management: Personal Briefing* - a useful resource to share with employees to help them understand their range of emotions is normal and to be expected. It will also help to identify when they might need to seek further help.

*Spotting the signs of stress* – is particularly useful for managers who should be alert in watching for changes in behaviour from staff for example withdrawal, late to work. There is an increased vulnerability to stress reactions for staff members who have experienced previous trauma or current significant life events e.g. bereavement, parenthood, divorce etc.

*Coping with Trauma* – is another useful resource in helping people to understand emotions but also importantly with recommendations of what *not* to do during this time.
4. OTHER AGENCIES AND NETWORKS

Aid Workers Network
Aid Workers Network is a free service set up to enable aid workers to share practical advice and resources with each other. www.aidworkers.net

Crisis Consulting International
For more than 25 years, Crisis Consulting International has been a premier provider of security and crisis management services to the Christian missionary, humanitarian and church sending communities. CCI assists with:

- Risk assessment, site surveys and security assessments
- Policy development and contingency planning
- Training of staff, leaders and crisis management teams
- Management of major events, conferences and disaster response
- Resolution of hostage and kidnapping events, extortion and other threats

Bob Klamser, Crisis Consulting International
9452 Telephone Rd, #223 • Ventura, CA 93004 USA
Phone: +00 (1) 805.642.2549
e-mail: info@CriCon.org
www.cricon.org/

First Rock
First Rock is the only organisation of its kind in the UK, Ireland and Europe catering solely for the missionary community and Faith-based Aid Agencies. It provides realistic training on how to survive in hostile environments. The Director Tim Mercer is a former member of Police Special Operations Branch. He served in the RUC between 1977 and 1993. Since leaving he has worked and operated in 50 countries, most of which would be considered hostile. He is employed by the BBC and ITN as a High Risk Trainer, Backwatcher and Security Advisor to prepare their staff to go overseas.

Email: tmercersec@aol.com
www.firstrock.eu/
+44 (0) 7809 689987

Phil Harper - QPM FCMI
International hostage negotiator and crisis management trainer
e-mail: sheep100ph@googlemail.com

Global Connections Member Care
Search for Member Care resources http://www.globalconnections.org.uk/services.

People in Aid
A network of people involved in HR policies with a wide range of resources.
Regent’s Wharf, 8 All Saints Street
LONDON N1 9RL
Tel: 020 7520 2548
Email: info@peopleinaid.org
www.peopleinaid.org