PEOPLE IN AID

Promoting good practice
in the management and
support of aid personnel

Policy Guide and Template

Safety & Security

Created May 2003, Revised in June 2008

Table of Contents

Foreword by People In Aid

For aid and development personnel, working environments are often extremely dangerous. Front emergency relief locations have very clear security risks but it has been shown that long-term development programmes are virtually as risky for both international and national staff. That is why "Safety and Security" is so important for the continued protection of all our staff, and why this is such an important issue for those of us involved in management.

People In Aid

Introduction to the Policy Guides

Since its inception, People In Aid has been bringing together agencies working in the aid and development sector, to enhance the impact they make through better management and support of staff and volunteers.

This document is part of a People In Aid initiative, the 'Policy Guidelines', whereby agencies share their knowledge and experience of a particular issue in order to increase the quality of people management generally within the sector. It forms part of a bank of reference material on a range of people management themes. The material is categorised in three levels:

- Resource Sheets – one or two pages of references and sources of information
- Information Notes – slightly more detailed overview of a specific area of interest
- Policy Guidelines – more detailed documents offering guidelines on policy development

For those agencies which have no established policy we hope this document both prompts and assists you. For those agencies which already have a policy, perhaps the document will encourage a re-think in one or two areas, or a complete revision.

The following notes are not intended to give you an 'off the shelf' policy which you can immediately use within your own organisation. They do, however, offer you the thinking and experiences of other agencies in our sector and prompt you to assess how your own organisation, with its unique mission, values and resources, can best respond to your organisational and staff needs in this important policy area.

The People In Aid Code of Good Practice suggests that human resource policies benefit the organisation most when staff have been involved in their creation and are briefed on their use. In addition, effective policies require managers to implement them and monitor their effects.

We hope to be continually updating our policy guide documents. This relies on new knowledge and experience being relayed to us by you. Please e-mail us on info@peopleinaid.org with your contributions and comments.

Acknowledgements

This document has benefited from the policies, suggestions or thinking of Care International, HelpAge International ICRC, IMC InterAction, InterHealth Oxfam Australia, Oxfam GB, RedR, Save the Children UK, Tearfund, The United Nations, VENRO, World Vision International and a variety of expert individuals from the NGO community. People In Aid would like to thank them for their input.

Safety & Security: Introduction

Safety and Security are the responsibilities of all. Managers and staff must be equally committed to the process to ensure success. Personal safety, organisational security, and ultimately the safety of the communities we serve, will only be attained where all parties join together in maintaining safe working conditions. Furthermore, our capacity to work with communities we serve, and increasingly to obtain funding from donors, is considerably weakened by poor attention to the issue of security and safety of our staff.

The focus of this document is on violence and insecurity perpetuated deliberately or consequentially on humanitarian aid and development workers. A lack of security can impact health, and accidents can compromise personal security. Prevention of accidents, and health and safety are also important and are the topic of separate People In Aid publications.

People In Aid believes that consideration of security issues and forward planning to mitigate risks and anticipate response to a range of scenarios will lead to safer and more secure working environments for humanitarian workers the world over.

This guide attempts to highlight current good practice in this field. Managers and individuals are, however, strongly advised to constantly review individual and organisational aspects of safety and security as the body of expertise continues to grow. The organisations and resources listed at the end of this paper will provide access to a range of readily available practices and analysis.

The safety and security of humanitarian aid staff is an essential component of the People In Aid *Code of Good Practice in the Management and Support of Aid Personnel.* (See below) The working environments for all humanitarian staff, whether in front line emergency relief or in long-term development programmes, have become more dangerous than ever in the past few years. Historically, personnel were afforded some protection by the nature of their employment. Increasingly, however, humanitarian workers are more and more likely to be the targets of intentional violence and aggression. Employing organisations must ensure that all staff, in all of the varied types of programme, are appropriately protected as much as possible. This requires significant planning on the part of managers, with the recognition that improving security for staff will increase field project costs.

However, humanitarian work is all about people. In the end the only resource humanitarian organisations have to offer the world is highly skilled individuals willing to venture into some of the most inhospitable environments possible. Maintaining the safety and security of staff is paramount. Cost must be considered, but immediate financial concerns should never be permitted to override the primary objective of ensuring the right staff are able to deliver the best services in the most challenging environments.

Security: the reality of the world around us

A persistent myth abroad in humanitarian aid circles is that most injury and death results from disease and accident. In fact during the period 1985 – 1998, 68% of the fatalities studied were the result of intentional violence against members of aid

organisations[1], and these figures are rising. Car accidents, long the major focus of management, constituted 17% of deaths with non-intentional injury accounting for barely 7%.[2] Of even more concern are the indications that between one half and two thirds of all deaths occur amongst national staff. According to the UN, at least 27 aid workers were killed by violence in 2001. The year before it was at least 48 (article: Staying safe….when it isn't, Aid Workers Network). Given that most agencies have tended to focus on security provisions for international staff this figure, if accurate, is highly disturbing.

Assessment reviews carried out in recent years by major aid organisations such as the ICRC, Care, Oxfam, World Vision and the United Nations have clearly shown that previous security provisions, where they existed at all, are not adequate in the present increasingly insecure environment. In response many of the large NGO's have commenced security training programmes and are in the process of creating internal policies and practices relating to security preparedness. The United Nations has, following a comprehensive review report in 2000, substantially improved its staff security provisions although member states have not fully funded all the recommendations of the Secretary General.[3] The United Nations security division, UNSECOORD, has in recent years expanded and modified its field role. Nearly 100 Field Security Officers (FSO) have been recruited to provide coordination and assistance at field level where required. As a function of its size UNSECOORD can keep FSOs up to date on changing security conditions and hence assist local NGO's to maintain security awareness.

Security training courses and programmes are now more widely available in response to these concerns. The UK group RedR has a distinguished record in provision of tailor-made training programmes both in field locations and at base locations in the UK and Europe. RedR has made its learning materials freely available to the international NGO community and they can be viewed at their web site.[4] The UN and some of the major agencies (for example, ICRC, World Vision, and Care) have created in-house security preparedness programmes for their own staff. Some of these programmes also make available limited places for other aid workers on payment of a fee. (More information on safety and security training providers can be found in the People In Aid Training Resources Sheet, 2007 www.peopleinaid.org/pool/files/publications/training-providers-resource-sheet-final.pdf).

However, even the agencies providing security training programmes often target international staff more heavily leaving the vast majority of staff with limited access to professional security preparedness. Staff employed by small to mid level NGOs, and many national or local staff, often remain without access to intentional security preparedness.

One of the most significant findings from recent research studies resulted from an examination of the risks associated with apparently different groups of workers. It is commonly believed that emergency relief work, especially in war zones, is inherently more dangerous than traditional development work. But an examination of both environments demonstrates that the risks are virtually identical, with the development environments appearing to have more potential for violence and injury than war

[1] Brabant, Koenraad van, *Operational Security Management in Violent Environments – A Field Manual for Aid Agencies,* Humanitarian Practice Network (HPN), Overseas Development Institute, London 2000.
[2] VENRO, *Minimum Standards regarding Staff Safety & Security*, Bonn, 2002
[3] United Nations, *Report of the Secretary General on the Safety and Security of United Nations Personnel*, October 2000.
[4] www.redr.org

zones. Certainly field worker perspectives of danger in both environments are similar. The other division applied to international aid work, between international and national staff, shows a similar pattern. National staff are no safer in any environment than international staff. It may be, in fact, that national staff are consistently at higher risk of danger than their international partners.[5]

These findings lead to the obvious (and potentially dangerously simplistic) conclusion that humanitarian work, no matter where it is performed or who performs it, is inherently risky, and growing more risky every year.

While there may be grounds to dispute some of the statistics generated by research studies this approach is, in the end, unhelpful. The death or injury of any humanitarian worker by an intentional act of violence is unacceptable. Whether violence against personnel causes only 40% of injuries instead of the 70% claimed in some studies is immaterial. Where staff are working in potentially dangerous environments it is incumbent on managers to ensure they are fully aware of the risks and have the necessary skills and knowledge to minimise those risks.

Security Preparedness contains three interdependent aspects.

- Organisational commitment
- Individual commitment
- Risk assessment

Organisational Commitment

Organisations seeking to improve security for staff will need to balance these three components, ensuring adequate focus on all. Management must demonstrate organisational willingness to examine security risks and to provide adequate resources for staff to become safe and secure. This will require planning and financial expenditure. Senior staff will need to demonstrate personal security behaviour in order to model risk-reducing practices.

Individual Commitment

Individual staff need to alter their own personal behaviours and practices to maximise the safety of themselves and others. Staff should not rely totally on the organisation to provide security. At the ground level good security will be dependent on individual behaviour in the context of organisational assistance.

Risk Assessment

*"Risk is a product of threats and vulnerability (*Risk = Threat x Vulnerability). *A structured risk assessment will help to identify the likely threats and the degree of vulnerability to them. "* (Oxfam Security Policy, 2004)

Risk assessment is both organisational and individual and is the core component of any security preparation. Knowing that both national and international staff are killed at about the same rate in humanitarian work does not constitute adequate risk assessment. The reasons for each death differ and in that difference will be indicators as to what might more effectively protect both types of staff in future. The fact that apparently the risks associated with development environments are similar to those found in emergency relief operations tells us little about the causes of those risks. Assessment, therefore, needs to become an integral and essential component

[5] World Vision International, *World Vision Security Manual,* Geneva 1999.

of every programme design, every programme proposal, and every programme review. Assessment also needs to become an integral part of every aid workers assignment preparation and daily activity. Managers need to build risk assessment into every decision-making level of organisational practice. Decisions as to what types of programmes, what countries to work in, what funding sources to approach, all need to include aspects of risk assessment.

Ultimately, of course, security preparation will impact the ability of the organisation itself to survive in hostile or challenging places. Security, on this level, is less about guns and bombs than it is about organisational competition for funds and skilled personnel, and about public accountability and credibility. Organisations that are unable to provide adequate safety precautions for staff will increasingly be shunned by potential employees, by donors and eventually by the communities they are seeking to assist.

Link to People In Aid Code Principles and Indicators

The People In Aid Code of Good Practice devotes one of its seven principles to health, safety and security. When the Code was first formulated it was explicit that the end product was 'staff security and well-being'. The six principles which preceded it all enabled the agency to assure itself that staff were being looked after, in the broadest sense. Strategy, planning, budgeting, briefing, training, consultation and more all contributed to staff security and well-being. That in turn is reflected in staff retention rates and quality of aid delivery.

People In Aid Code of Good Practice:
Principle 7 Health, Safety and Security

The security, good health and safety of our staff are a prime responsibility of our organisation.
We recognise that the work of relief and development agencies often places great demands on staff in conditions of complexity and risk. We have a duty of care to ensure the physical and emotional well-being of our staff before, during and on completion of their period of work with us.
Indicators:

1. Written policies are available to staff on security, individual health, care and support, health and safety.
2. Programme plans include written assessment of security, travel and health risks specific to the country or region, reviewed at appropriate intervals.
3. Before an international assignment all staff receive health clearance. In addition they and accompanying dependents receive verbal and written briefing on all risks relevant to the role to be undertaken, including insurance. Agency obligations and individual responsibilities in relation to possible risks are clearly communicated to staff. Briefings are updated when new equipment, procedures or risks are identified.
4. Security plans, with evacuation procedures, are reviewed regularly.
5. Records are maintained of work-related injuries, sickness, accidents and fatalities, and are monitored to help assess and reduce future risk to staff.
6. Work plans do not require more hours work than are set out in individual contracts. Time off and leave periods, based on written policies, are mandatory.
7. All staff have a debriefing or exit interview at the end of any contract or assignment. Health checks, personal counselling and careers advice are available. Managers are trained to ensure these services are provided.
8. In the case of staff on emergency rosters, managers should ensure that health clearance, immunisations and procedures for obtaining the correct prophylaxes and other essential supplies are arranged well in advance.

Definition of Safety and Security

Security can only be defined in relative terms. Security is context specific. Security in a particular location can be assessed through a process of risk assessment. This involves being aware of all potential and real risks and developing a system to track changes over time and introduce interventions to mitigate risk as far as possible and practicable. Security assessment is dynamic and ongoing and must become a regular part of daily field life.

The nature of NGO work means that staff and organisations will be located in environments where relative security risks are higher than in other contexts. However, recent changes in geopolitical realities mean that certain security risks are now found in locations previously thought relatively safe. Headquarter locations or regional management centres located in previously "safe" locations may now have a higher degree of risk than ten years ago.

The purpose of risk assessment is to keep the staff and the organisation safe. It is therefore most useful to talk about security in the context of safety.

Operational definition of security:

NGO security is achieved when all staff are safe, and perceive themselves as being safe, relative to an assessment of the risks to staff and the organisation in a particular location.

In addition to this definition one must also add organisational security. This is not just the protection of organisational assets such as vehicles and buildings but the organisation's existence and reputation, which relates to how it is perceived, what relationships (real or presumed) the organisation has with other entities, its perceived integrity, etc.

Organisational definition of security:

NGO security is achieved when organisational assets are safe and when the organisations name and reputation are maintained with a high degree of integrity.

This latter point is complex and challenging, but of vital importance with regard to the safety of NGO staff. In an increasingly polarised world the functional, political, religious and ethical relationships that an NGO maintains will have a significant impact on the safety of staff and assets. Ultimately this will impact the existence of the NGO itself.

This document does not attempt to address the issue of NGO's working alongside the military, accepting government funds, or being partnered with religious or political groups. There has been much written recently on these topics. However, in making a full and accurate assessment of the relative safety of staff and assets in any field location it is essential to consider these broader aspects of organisational existence. While it is often tempting for field staff to brush off headquarters policy-making activities as being of little practical impact locally, it is no longer possible to compartmentalise NGO work in this fashion.

The creation of an overarching security policy must remain the responsibility of headquarters, but implementation in a manner that is meaningful for the context will obviously be conducted by field based management through country or location specific security plans and evacuation plans. Organisations should determine the key factors that make up a comprehensive security policy and design a series of standard operating procedures (SOPs) for field operations. For example, every security plan must contain an evacuation plan. This plan must be written down, available to all staff, and regularly reviewed to take account of changing circumstances. However, the precise details of the evacuation plan will differ from country to country and will be designed by local management in consultation with local resources and HQ personnel.

This separation of responsibility is essential because it lays out the framework of the agreement between HQ and field personnel on the provision of services (by the organisation) and the expectations on field staff in order to maintain security. There are, therefore, a series of organisational pre-requisites that must be completed before a field security plan can be designed and implemented.

A full and proper security risk assessment will begin with the wider organisational reality and then consider how that reality impacts staff and asset safety at a field location.

Whilst a robust security policy is considered to be the key tool for managing staff security, it must be remembered that security management is more than just a piece of paper. The existence of a document does not guarantee staff security; it is only valuable to the extent that activities are managed in accordance with it and it forms part of a comprehensive security management system. Which is fuly integrated into wider programme management.

The core elements of a Security Policy

The two essential elements of a successful security policy are
1. The organisational commitment to properly maintain staff safety and security
2. A series of concrete standard operating procedures for use at field level.

In Section 3, we expand upon each of the bullets that follow.

Organisational Pre-requisites/commitment

- A value statement relating to the safety and security of personnel
- A statement defining safety and security
- An organisational location for security preparedness and coordination. E.g. A Security Officer
- A Crisis Management strategy
- Incident analysis and evaluation component
- A budget allocated to security training and implementation
- A statement defining organisational relationship with local and international legal provisions
- A statement regarding relationship with armed guards or military units
- A statement clearly outlining the organisations policy on kidnapping for ransom
- Provision of health and other insurance cover for personnel

Key components of a security policy

- Statement as to who is responsible for designing and modifying the policy
- Process of evaluation of policy. Who reviews it and how often?
- A process of risk assessment incorporated at all levels
- Choice of a Security Strategy. Who chooses and may the strategy be changed?
    - Acceptance
    - Protection
    - Deterrence
- Crisis Management Team
- Stress and Trauma Management
- Coverage by the policy. Does this include all staff as well as dependents?
- Statement on individual responsibility for staff to reduce exposure to risk
- Media relations
- Training processes for all personnel covered by the policy
- Evacuation plan for staff from high-risk environments
- Contingency plans for other emergencies
    - Medical emergencies
    - Kidnapping
    - Natural disasters
- Standard operating procedures
    - Money
    - Communications
    - Vehicles
    - Mines
    - Organisational assets
    - Data and document storage
    - Incident reporting
    - Site selection
    - Visitor security

The UNHCR insists that each country should develop and maintain a five-phase security plan under the umbrella of the organisation-wide security policy. In addition to this, separate evacuation and movement control plans should be created and maintained.

Phase 1 – precautionary
Phase 2 – restricted movement
Phase 3 – relocation (concentration of all international staff and relocation of non-essential staff either inside or outside the country)
Phase 4 – programme suspension (involves relocation of all staff and programme activity outside the country. Some key field staff may remain)
Phase 5 – evacuation of all international staff using pre-prepared evacuation plan

UNHCR Handbook for Emergencies www.unhcr.org/publ/PUBL/3bb2fa26b.pdf section 23, page 237

Action Plan for preparing a Security Policy

The process of creating a policy requires commitment from all levels of an organisation and sound relationships with other NGOs and specialist agencies. The process must be led by senior management and affirmed by the organisational governance structure. (e.g. Board of Directors and/or trustees). The process should be internally consultative and externally advised to ensure the objectives are met.

The use of a checklist of questions can usefully support the design and implementation of a good practice security policy. The sections below offers such a checklist for creating a security policy from scratch:

Foundations of the policy

- Does the organisation have a value statement relating to safety and security of people?
- Is there a clear operational link between this value statement and security related standard operating procedures at a field level?
- What is the organisational definition of Safety and Security? A policy should always begin with such a definition
- How does the policy include a global assessment of risks to NGO's?
- How does a global assessment of risks to your NGO influence the policy?
- Does the policy development process allow for dynamic change following frequent reviews of changing global influences?
- Does the policy allow for local interpretations based on wider global assessments?
- Is the policy flexible enough to allow local realities to be addressed?
- What are the lines of authority and decision making? A clear statement as to authority and responsibility must be included. This is especially important during emergencies where HQ staff sometimes find themselves in disagreement with field managers

Design and implementation of the policy

- Who is responsible for creating a security policy? Does this responsibility rest with a person or a position?
- Does the person who designs the policy also implement it? Who has the authority to enforce the policy?
- Is authority delegated or centralised?
- Is the policy negotiable?
- Is it able to be suspended?
- Do field managers, or other managers, have the ability to bypass the policy?
- Who holds the senior management accountable?
- Is there a specialist security management function in the organisation?
- Where do funds for this position come from?
- Are there adequate resources for the role?

Coverage under the policy

- Who is covered under this policy?
- Are local staff covered?
- Are family members of expatriate and local staff covered?
- What about local volunteers, contract staff from other NGO's, local government associates?
- Are staff working at headquarters or regional locations covered under this policy?
- Are family members living in headquarters locations covered?
- Does the policy adequately and clearly delineate individual versus organisational responsibility for maintaining security?
- What responsibilities are individual staff members expected to take on?
- Where does organisational responsibility end and individual begin?

Extent of the policy

- Does the policy cover people only or does it include material and financial assets?
- What are the organisational priorities? People first? Money first? Who decides?
- How much authority does a local manager have according to policy to make decisions over these priorities in a high risk event?
- Does the policy cover organisational marketing?
- Does the policy cover how the organisation is promoted in donor environments?
- Would inter-agency or government relationships increase or reduce security risks?

Policy as it relates to external groups

- Does the policy address armed security provision? Security provided by military? Private security organisations?
- How does the organisation address relationships with local laws and local customs?
- Does the policy provide opportunity for local managers to vary practice because of local laws, customs or practicalities?

Nature of the policy

- Is the policy advice or requirement?
- Is the policy practical or conceptual?
- Are managers encouraged to reflect on security and safety or are they required to implement clear practical activities?
- Does the policy include audit and evaluation processes?
- How often does audit occur?
- Who will perform the audit? Local managers? Headquarters staff? External consultants?

Policy as it relates to rights and responsibilities

- Does the policy outline rights that staff (and family members) have to decline to enter high risk environments without impacting employment?

- Does the policy allow staff (and family members) to leave locations where their personal assessment is that safety is being compromised?
- Is the individual or the organisation responsible for any costs incurred in acting on these rights?
- Are staff required to behave in ways that will not increase the risk to safety and security? What are those behaviours?
- What are the disciplinary outcomes of failing to adhere to organisational requirements relating to security and safety?
- What is the organisation's responsibility to assist staff and family members who are impacted by increased risk or exposure to threat?
- In cases of kidnapping, assault, sexual attack, arrest, what commitments has the organisation made to staff and family members?
- Has the organisation made provisions for full medical and psycho-social support?

Policy as it relates to preparedness

- Does the organisation have a commitment to develop competencies in safety and security?
- What does the policy state about ensuring ongoing risk assessments?
- Is there a process of security planning and crisis preparedness?
- Does the policy provide insurance cover for staff and family members? Is this coverage available to locally hired staff?
- Is there an established crisis management process or structure? What level of authority does this structure have?
- Does the policy include development of evacuation plans? Is it required that every field location has a full evacuation plan? Does this plan cover all staff, or only expatriate staff? What provisions are made for local staff?
- Does the organisation analyse incidents in order to improve overall safety and security?

Policy as it relates to training

- Does the policy cover the organisation's commitment to provide ongoing personal security training?
- How is such training to be funded?
- Is this training available to all staff? Locally hired staff? Family members?
- Will the training also cover issues of management of security and safety?
- How will managers be equipped to ensure field locations are safe and secure?
- What expectations does the organisation have of individuals who have been trained?

Policy implementation

The way in which you implement and publicise your policy will depend on the culture and communication norms of your organisation. We have therefore not attempted to offer a "one size fits all" good practice implementation guide, suffice to say that clear communication and the opportunity to ask questions or involve staff in a discussion around the subject of Safety & Security both during the policy development stage and at the point of implementation is key to fostering understanding and helping colleagues see the benefits of its application within their operational context. Equally, appropriate, targeted training and on-going support and awareness in safety and security will be critical.

Further Resources

A number of the resources listed below can be accessed via the People In Aid online resources www.peopleinaid.org

Brabant, Koenraad van, *Operational Security Management in Violent Environments – A Field Manual for Aid Agencies,* Humanitarian Practice Network (HPN), Overseas Development Institute, London 2000.

Brabant, Koenraad van, *Mainstreaming Safety and Security Management in Aid Agencies.* Overseas Development Institute / Humanitarian Policy Group Briefing Number 2, March 2001. (www.odi.org.uk/hpg/papers/ hpgbrief2.pdf)

Brabant, Koenraad van, *Security Training: where are we now?* In: Forced Migration Review 4, April 1999.(www.fmreview.org/FMRpdfs/FMR04/fmr402.pdf)

Luis Enrique Eguren, *Beyond security planning; towards a model of security management*, 2002, http://www.jha.ac/articles/a060.pdf

Care International, *Safety & Security Handbook.*

ECHO, Review of: "Standards and practices for the security of humanitarian personnel and advocacy for humanitarian space", September 2004.

InterAction, *The Security of National Staff: Toward Good Practices*, July 2001. http://www.interaction.org/files.cgi/531_sec_nationals_staff_final_doc.doc

Interaction, The security of national staff: essential steps 2002, http://www.interaction.org/disaster/securitysteps.html

International Committee of the Red Cross (ICRC), *Staying Alive. Safety and Security Guidelines for Humanitarian Volunteers in Conflict Areas,* Geneva 1999.

International Federation of the Red Cross and Red Crescent Societies (IFRC), *Security Guidelines.*

InterAction, *InterAction Security Planning Guidelines.*

International Rescue Committee, *Security Management Plan Workbook*, October 2000.

People In Aid, *Prevening Accidents – Guidelines for the Aid Sector*, 2003. http://www.peopleinaid.org/resources/publications.aspx

People In Aid, *Preventing HIV/AIDS – Guidelines for the Aid Sector*, 2003. http://www.peopleinaid.org/resources/publications.aspx

People In Aid, *Health and Safety in Aid Agencies*, 2002. http://www.peopleinaid.org/resources/publications.aspx

Aid Workers Network, Staying safe…..when it isn't http://www.aidworkers.net/?q=node/255

UNHCR Handbook for Emergencies, 2nd edition http://www.unhcr.org/publ/PUBL/3bb2fa26b.pdf

United Nations, *Report of the Secretary General on the Safety and Security of United Nations Personnel*, October 2000.
(http://www.reliefweb.int/library/documents/SG_Report_A_55_494.htm)

United Nations, *Report of the Secretary General on the Safety and Security of Humanitarian Personnel and Protection of United Nations Personnel,* August 2002.

United Nations Security Coordinator, *Guidelines for UN/NGO/INGO Security Collaboration,* February 2002.

VENRO, *Minimum Standards regarding Staff Safety & Security*, Bonn, 2002.

World Vision International, *World Vision Security Manual,* Geneva 1999.

Internet Resources

Bioforce security training programme: www.bioforce.asso.fr

Centre for Safety and Development www.centreforsafety.org

CINFO training programme on security and stress, preparing for an assignment abroad: www.cinfo.ch

The Overseas Development Institute's Humanitarian Practice Network: www.odihpn.org.uk

RedR training programme on security, staff and project management in humanitarian assignments: www.redr.org

Reliefweb has web pages on training programmes and staff safety
www.reliefweb.int/ocha_ol/civilians/security personnel/index.html
www.reliefweb.int/training

This list is not exhaustive and will be added to over time. Please contact People In Aid to contribute any useful materials to this list.

Visit the online People In Aid member resource site for examples of current INGO safety and security policies. **The People In Aid Policy Bank:**
http://www.peopleinaid.org/resources/policybank.aspx

Checklists for Health and Safety can be dowloaded for free
http://www.peopleinaid.org/resources/publications.aspx

Related **Information Notes** can be found on
http://www.peopleinaid.org/pool/files/publications/enhancing-staff-security-inote-final.pdf
http://www.peopleinaid.org/pool/files/publications/staff-vulnerabilities-&-security.pdf

The example policy documents in the following appendices draw on the experiences of all the contributing organisations and in particular the policies of Oxfam GB and Oxfam Australia for which People In Aid wishes to thank these organisations.

Appendix 1: Sample safety and security policy

Relief Aid* – Safety and Security policy

Date of Policy Issue:
Issue Number:
Date of Policy Review:

Relief Aid Mission and Vision Statement
Relief Aid works in the poorest countries of the world to provide emergency healthcare and sanitation to those most at risk and to educate local people in the necessary skills to maintain these services to themselves in the future.

Introduction
Relief Aid recognises that humanitarian work is often performed in extremely unstable and potentially dangerous environments and has therefore created this safety and security statement with a view to maintaining the safest possible working conditions.

Relief Aid subscribes to the Principles of the People In Aid Code of Good Practice and believes that staff comprise the most important resource for Relief Aid and the communities we serve. Effective safety and security policies and procedures are designed to ensure that the work of Relief Aid can continue even in challenging environments.

Relief Aid believes that safety and security exist when staff are enabled to pursue their tasks without undue risk to health or life.

Coverage of this policy
This policy covers all staff employed by Relief Aid including international and local staff and their dependents, independent contractors and official non-employee visitors.

Authority and responsibility for Safety and Security

Individual: Staff members at all levels have the authority and responsibility to improve safety and security procedures wherever these are inadequate. In order to ensure that the security guidelines are successful there must be clear delimitation of responsibility at every level of the organisation. All staff should comply with the Relief Aid Code of conduct and should not behave in any way that could present a risk to themselves, others or the organisation. Failure to follow security guidelines and procedures may be treated as a disciplinary matter.

Irrespective of the organisation's judgement of risks in a particular situation, any staff member may decline to work in an insecure area, and may withdraw, having first informed their manager. If the risks are constant, continuation of employment will be reviewed, in line with organisational procedure.

* Fictitious agency

Managers: All managers are responsible for the security of the staff they manage, and are, in turn, under the responsibility of their line manager. This responsibility follows the line management structure with ultimate responsibility resting with the board of trustees. The manager is responsible for managing staff security, including: delegating security management tasks; ensuring an appropriate security management system and plan is developed; inducting/briefing all new staff and visitors on the security situation and security measures. Security management is demanding and adequate time must be allocated to it.

Organisation: The Office of Security Management has overall responsibility for safety and security. Policy and Standard Operating Procedures will be determined through a consultative process between field representatives and senior management. The Security Manager will determine the extent and nature of the overall policy. Field Managers have authority and responsibility to design and implement operating procedures deemed appropriate to specific environments. In addition to reviewing and monitoring this policy the Office of Security Management will provide guidance and assistance to field based managers who are charged with developing local safety and security plans on specific issues that are pertinent to that context.

Risk Rating System
All Programme Offices are rated according to the assessed level of risk. The risk rating categories will be made available to all Programme Managers. Programme Security Plans will be designed in the context of the assigned risk rating for that location. Security Plans will be flexible enough to cope with changes in risk ratings from time to time.

Budget
Funding for security and safety will come from a variety of sources. The general funds account will meet all costs associated with the Office of Security Management. All training costs will also be met from this budget. Programme Offices will be expected to share costs where possible. Project proposals will include line item requests for some costs associated with safety and security. Security Management will provide training for enhancing access to donor funding for this purpose.

Security Management Plan
Each Programme Office will have a written security management plan. This plan will comprise all the key elements of safety and security listed below. The security plan will be approved by the Security Manager and will be reviewed on an annual basis, or more frequently as the context warrants.

The security plan will be designed using both local and international sources being sure to make maximum use of local knowledge and expertise.

Should the country situation change according to the Security Rating Criteria Programme Managers will consult with the Security Manager to update the operational components as required.

Training
All staff will have access to personal security training. This training will be coordinated through the Office of Security Management. Programme Officers will attend District training events and will be expected to ensure field based training occurs for all field staff.

Performance Management
Performance objectives and reviews should include management of security. This can be at the individual level, i.e. displaying awareness of personal security issues the impact of own actions on the security of self, others and agency. It can also be more formal in terms of the safety and security remit of the specific role that is being undertaken.

Insurance Cover
Relief Aid will provide health and evacuation insurance cover for all international staff and dependents. Programme Officers are expected to seek local insurance options for local staff where possible. Where there are no local insurance possibilties Programme Offices should consult with the International Staff Director to discuss other support programmes. Such programmes could include self-funding or matched funding options.

Components of a Field Programme Safety and Security Management Plan
Each Programme Office Security Plan will include the following key points. The Office of Security Management will assist in determining specifics of each section if requested.

- Line of Authority
- Risk Assessment Process
- Security Strategy. (Protection, Deterence or Acceptance?)
- Crisis Management Strategy
- Personal Safety and Security
    - Relationships with local community
    - Moving around the local community
    - Residential arrangements
    - Situational awareness
    - Specific security concerns for women
- Standard Operating Procedures
    - Site selection and security
    - Handling cash
    - Document security
    - Communications
    - Transportation and vehicle maintenance
    - Incident response. Eg, carjacking, robbery, ambush, etc.
    - Incident reporting
    - Landmines and bombs (where appropriate)
    - Evacuation plans
    - Contingency plans
        - Medical emergency
        - Natural disaster
        - Kidnapping
    - Media relations
    - Stress and Trauma Prevention

Reporting incidents
All security incidents must be reported immediately to the line manager, who is required to report serious incidents to their line manager and up the management line to the Office of Security Management. Incident analysis must be undertaken, after the immediate event has been dealt with, to determine why the incident happened and how it could be prevented or managed more effectively in the future.

Serious Security Incidents
Depending on the nature and severity of the incident, the Security Manager may assume ultimate decision making authority for managing the response. In addition, in the most serious cases, the decision may be taken to convene an organisational Incident Management Team to lead co-ordination, decision making and delegation of responsibilities.

Involvement with Arms
Relief Aid staff must not carry or take up arms under any circumstance and must not use or hire armed personnel either directly or indirectly. Arms and armed personnel must not be allowed in Relief Aid premises or vehicles, except if staff are threatened or coerced. Permission to use or hire armed personnel (either directly or indirectly) may only be granted by the Security Manager on a case by case basis.

Involvement with Armed Forces
Relief Aid should only undertake work involving links with armed forces (whether they are national authorities, non-state actors, or international in nature) when it can be done without undermining our identity as an independent humanitarian actor. Guidance must be sought from the Office of Security Management in specific cases of potential involvement, and a decision will be taken by the Security Manager who will consult with the Director where this involves wider implications for the organisation's identity.

Evacuation
Planning and preparation for evacuation is a key part of any security plan. Preparation should also be made for 'hibernation' – when it is safer to stay in a location rather than to attempt to move.

In an evacuation Relief Aid's aim is to return staff to their home base, or place of safety. Notwithstanding legal obligations, we endeavour to undertake, as far as reasonably practicable, to move all staff to a place of safety, if they are at risk directly as a consequence of their work with Relief Aid, their nationality, their ethnic origin or are subject to a particularly serious or targeted threat. All staff should be made aware of their own and Relief Aid's responsibilities in advance.

Staff who are evacuated will, as far as practicable, be offered a formal debrief and counseling if deemed appropriate.

Authorisation to withdraw from an area, to suspend operations or to temporarily close an office for security reasons, can be given by the local manager with immediate effect and is binding on all staff. Senior management may direct a team to withdraw, suspend or close an office and may override a local manager's decision to stay, to continue the programme or for an office to remain open, but cannot override a local manager's decision to leave, suspend or temporarily close. The instruction from management will define the specific programme, office, location or staff that the ruling refers to. Relief Aid staff have no right to remain in a location, if they have been directed to withdraw by management.

Authorisation to return to an area after evacuation or suspension can only be given by senior management. A systematic security review must be undertaken by the relevant manager and a written report, including recommendations, submitted by the Office of Security Management for decision-making. The systematic security review should re-consider and revise the existing context and risk analysis and the appropriateness of security strategies and security management plans. Particular emphasis should be placed on how the situation may have changed and what measures should be taken to reflect these changes.

Medical Emergencies
In all locations where Relief Aid staff work, the manager must formulate a Staff Health Protocol, which includes a procedure for medical emergencies.

I have received RELIEF AID's Safety & Security Policy which I have read and understood.

NAME: ----------

SIGNED: ----------

DATE: ----------

Please return this page to Human Resources

ENDS……

Appendix 2: Example Field Office Security Guidelines

Security Ratings

Security level	Actions necessary	Authorisation level	Reporting required
Level 1 **Normal operation** Where: • No specific threats are identified	• Normal procedures apply • Staff should be informed and trained in the program security guidelines • Provisions should be made to ensure security guidelines can be adequately implemented.	Program Manager or Field Rep	Minimum fortnightly
Level 2 **Precautionary** Where: • There is an established threat to security, or information is received on new threats or specific incidents • Forthcoming events are likely to increase tension and likelihood of incidents • Security monitoring indicates a general rise in tension or increase in number or severity of incidents • But none of these, nor a combination of these suggest that measures greater than precautionary ones are necessary. For instance that a rapid deterioration is unlikely	1. One person is appointed to monitor and log security information each day and before each journey (use green, yellow and red codings for routes and locations – see below) 2. Identify what belongings, including documents need to be taken in the event of an evacuation 3. Identify possible areas to assemble staff in the event of any evacuation 4. Identify who may need to be evacuated 5. Keep updated list of staff and visitors 6. Check the validity of identity cards and passports 7. Identify possible evacuation routes and check these for feasibility under emergency/conflict conditions 8. Check supplies of the following items ▪ Food and water ▪ Fuel for vehicle ▪ Torches, batteries, candles and matches ▪ First aid kit ▪ Extra cash 9. ensure adequate communications equipment is available and correctly used for road travel 10. ensure all staff and visitors are aware of potential risks and evacuation procedures	Program Manager or Field Rep	Minimum weekly to Program Coordinator

Level 3 **Restricted movement and evaluation of non-essential staff** Where: • The level of tension of number and severity of incidents is such that normal operating procedures are no longer appropriate • The situation deteriorates at a speed which suggests that program suspension or evacuation will soon be necessary	Continue program work, but 1. Do not travel unless necessary 2. Non-essential staff and dependants should leave and non-essential visits should be cancelled 3. Back-up important files 4. Carry personal documents and a small bag of personal belongings in case of evacuation without passing by the house/office 5. Identify any equipment to be evacuated 6. Make an inventory of equipment and assets/check it is up to date 7. Ensure vehicles are ready to leave – use a checklist to make sure nothing is forgotten 8. Discuss possible evacuation with partners and communities as appropriate and make arrangements for support in the event of a full evacuation	Regional Manager	Minimum twice weekly to Division Director
Level 4 **Hibernation** Where: • The level of violence, either generalised or targeted at the agency or agencies is such that it is no longer safe to carry out program activities or to move outside the house or office • The situation is such that imminent full evacuation is likely • The situation is such that evacuation has been agreed but it is not safe to move out of the house or office	1. Retreat to safest location; homes, office or , if necessary, with an other NGO 2. Inform head office on a new location and contact details 3. Ensure access to 15 days of food and water per person 4. Ensure access to communications equipment 5. Ensure instructions and training in sue of radios (if used), is current 6. Prepare for Level 5 Evacuation procedures	Division Director	Minimum daily to Executive Director
Level 5 **Evacuation** Where: • It is no longer for staff to remain in the area or country, or where the risks outweigh the value of remaining • Recent and anticipated incidents suggest that little or no usefully activity will be possible in the foreseeable future because of security constraints	1. Notify other agencies, coordinating bodies and local authorities as appropriate, that you are leaving 2. Coordinate evacuation with others if necessary 3. Pay salaries to staff remaining, with payment in advance as appropriate. Ensure roles and responsibilities for staff remaining are clearly understood and establish a means to stay in touch for the period of evacuation 4. Prepare office/house for possibility of looting 5. Move evacuating staff to assembly point for evacuation 6. Proceed with the safest mode of travel	Executive Director	Minim 2-3 times daily or hourly