

# Information Note



## Enhancing Staff Security

Contributors:  
Shaun Bickley -  
Security consultant

### Staff Security

The security and safety of personnel is a growing concern for all humanitarian organisations. In the past, agencies believed they would be afforded a degree of protection simply because of who they were and the humanitarian assistance they provided. Today, however, there are huge challenges to these traditional assumptions. Agencies operating in Iraq and Afghanistan now find themselves the target of attacks, having lost the tacit protection necessary for them to operate safely.

Away from the difficulties of Iraq and Afghanistan, agencies are experiencing unprecedented levels of violence directed at their staff. The list is alarming: murder, rape, kidnapping, mock execution, armed robbery, car jacking, assault, improper detention by authorities, and threats and harassment have all become almost daily events in some contexts. Clearly, this level of insecurity dictates the response an agency can provide. In some cases, lack of security results in the suspension of programmes. In others, relief operations continue, but at considerable risk to those involved.

While these disturbing trends pose great difficulties for all organisations, the increased levels of risk faced by some agencies is often the result of their own action or even inaction. Many of these dangers can be avoided or, at the very least, significantly reduced.

A key development in recent years has been the progress made on identifying fundamental principles for staff safety and security. This has led to developing good practice for the management of security. Essentially, however, security management is just good programme management. The type of programme an agency undertakes, and how this is implemented, will both affect and be affected by the agency's security. For security to be truly effective it must be fully integrated into programme design and management and not be viewed as a separate issue. As part of its wider duty of care to staff, an agency must ensure that all staff are aware of and prepared for the risks that exist, and that policies, procedures and practices ensure that these risks are reduced.

### From Principles to Practice

Enhancing staff security involves various management approaches which must be mainstreamed across all levels, from the organisation, to the field, through to the individual staff member. Agencies must ensure that the following security management instruments are in place.

### At the Organisational Level...

- ♦ **Commitment** – agencies must demonstrate a proactive willingness to engage in security issues, by carefully examining the security risks and committing adequate financial and human resources to improving the security of their staff.

- ◆ **Security management team** – agencies should establish a security management team or working group to oversee improvements in security management. Ideally this team should include senior management from different departments within the organisation, for example operations/programmes, human resources and communications, to integrate security management into wider programme management.
- ◆ **Internal discussion fora** – different fora must be established within the organisation where security issues can be raised and adequately discussed. Regular security meetings with senior management should be scheduled to ensure discussion of pertinent security issues and clarify organisational positions on complex issues that relate to security management.
- ◆ **Roles, responsibilities and decision making** – agencies must ensure that the roles and responsibilities of senior staff in managing security are clearly defined and understood. Clear lines of communication from the field through to senior management must be in place, clarifying who is responsible for taking what decisions and, vitally, at what point this decision should be referred to a more senior level.
- ◆ **Organisational security policy** – clear benchmarks and boundaries must be established to support staff in making operational decisions and developing local security policies. In order that these policies and positions are consistent in their application from country to country, agencies must also develop a clear organisational security policy.
- ◆ **Crisis management plan** – preparedness is vital to the successful management of any crisis situation, especially where a coordinated and effective response from many different departments is required.

Agencies must develop a crisis management plan identifying a crisis management team, removed from the immediacy of the environment, which can support, coordinate and analyse the response to a crisis. The roles and functions of the crisis management team must also be clearly defined.

- ◆ **Recruitment, induction and briefings** – it is essential that security issues are introduced to new staff early in the recruitment process. Agencies must ensure that security considerations are made clear in job descriptions. New staff should be informed of the security risks before they accept the post to allow them to ask pertinent questions. On accepting a position, all staff should undergo a thorough induction process in which security is a key element. This briefing must cover all security risks, the organisation's approach to security, measures currently in place to mitigate the risks, the agencies obligations and individual responsibilities.

## At the Field Level...

- ◆ **Roles and responsibilities** – in the field, agencies must ensure that all team members clearly understand their given roles, responsibilities and obligations in relation to security. These clarifications must be made in advance of a situation occurring, in order to ensure a quick and effective response. All staff must be made clear on their individual and team responsibilities, the decision-making process, and how decisions are taken in the event of staff absence or breakdown in communication.
- ◆ **Risk assessment** – agencies must ensure that a thorough assessment is conducted of the risks that exist in the field. A risk assessment should consider what threats exist and how prevalent they may be, both now and in the future. It must also consider to what degree staff, the agency, or

humanitarian agencies in general are vulnerable to these threats. This formal process is essential if agencies are to make more informed decisions about which security measures to adopt. Risk assessments must not be one-off events: continuous monitoring of the surroundings and re-evaluation of possible risks will ensure that agencies have appropriate security measures in place at all times. Agencies must also judge the level of risk to staff they are willing to accept. It is important to ensure that the level of risk the agency considers to be acceptable is compatible with the feelings of individual staff.

- ◆ **Local security guidelines** – agencies must ensure that local security policies and guidelines are developed in the field. These will help staff prevent or mitigate security incidents in a manner that is appropriate for the agency in that particular context. Local security guidelines are key operational documents which should contain context-specific policy and procedures, and any information required to implement them. These guidelines should clearly outline standard operating procedures (SOPs) which, if followed, will help to prevent or minimise insecurity. SOPs should address issues such as: personal security and staff safety; site security; vehicles, movement and travel; communication; financial management; security levels and indicators; and reporting incidents. Local security guidelines must be accessible to all staff, and should be translated into local languages where necessary. It is vital that these guidelines are continually reviewed to reflect any changes in the security situation.
- ◆ **Contingency plans** – unfortunately, even with procedures and guidelines in place, there is no guarantee that security incidents will not occur. In the event of an incident, staff must be prepared to react appropriately to ensure that the impact is minimised. Agencies must ensure that contingency

plans are developed in the field incorporating pre-established procedures and guidance which will assist staff in responding effectively to an incident. Specific contingency plans should be established where there is a risk of a serious incident, for example evacuating or relocating staff; medical emergencies; armed robberies; death threats; and staff disappearance, abduction, kidnapping or hostage-taking.

- ◆ **Incident reporting and analysis** – awareness and understanding of security incidents which arise in the working environment is essential for the overall protection of staff. Agencies need to ensure that a well-maintained system is established for timely reporting and analysis of incidents that affect the agency, or other agencies in the area. This is vital in assisting field teams in identifying, analysing and reacting to changes in the security situation.
- ◆ **Inter-agency collaboration and information sharing** – agencies have an obligation to collaborate and share information on security. Details of specific incidents and information on developments in the wider security environment must be shared with other agencies to allow them to make judgements on changing security situations. Not all agencies will accept the same level of risk; each agency will interpret and react to a security situation in different ways. Agencies should actively engage in a range of information exchange mechanisms that exist in the field, including informal networks, regular inter-agency security briefings or meetings, or through centralised security information systems such as the Humanitarian Information Centre (HIC) or the NGO security officer forum, if present.

## At the Individual Level...

- ◆ **Individual responsibility** – agencies must clarify what they expect of individual staff

members in terms of security. All staff have a responsibility not only for their own personal security, but for the security of their colleagues and other agencies' personnel. Staff must be able to develop an awareness of their own personal security responsibilities, together with an understanding of how their actions or inaction in a particular environment can jeopardise their safety and that of their colleagues.

- ◆ **Personal conduct and behaviour** – agencies must ensure that staff are aware of the impact their personal conduct and behaviour may have. How staff act, dress and interact with others will influence how they are perceived as individuals, as well as having an impact on the image and reputation of the organisation and its capacity to operate. Agencies must provide clear guidance to staff on the conduct which is expected of them, and raise awareness of behaviour and attitudes that might offend or provoke aggression, exposing them and their colleagues to unnecessary risks.

## Developing Greater Awareness...

- ◆ **Training and staff development** – security training, continuous guidance and support are fundamental elements in improving the security awareness and management capacity of staff. Agencies must ensure that staff have access to security training, either through the development of in-house training or by facilitating access to the increasing range of external training opportunities. Several organisations, including RedR and Bioforce, are providing security training. RedR's security training programme is aimed at individual personal security and the more senior security management level. These training courses are available in the field, regionally and also in Europe and the United States.

## Useful resources

### Publications

Bickley, S (2003) *Safety First: A field security handbook for NGO staff*, London, Save the Children

Kreidler, C (2003) *Minimum Standards regarding Staff Security in Humanitarian Aid*, Bonn, VENRO

Van Brabant, K (2000) *Operational Security Management in Violent Environments*, Good Practice Review 8, London, Overseas Development Institute

Van Brabant, K (2001) *Mainstreaming the Organisational Management of Safety and Security: A review of aid agency principles and a guide for management*, London, Overseas Development Institute

### Web Links

Aid Workers Net – Safety and Security

[www.aidworkers.net/security/index.htm](http://www.aidworkers.net/security/index.htm)

Reuters AlertNet – Security

[www.alertnet.org/thefacts/reliefresources/sections/SECURITY.htm](http://www.alertnet.org/thefacts/reliefresources/sections/SECURITY.htm)

### NGO Security Training

RedR security training programme

[www.redr.org](http://www.redr.org)

Bioforce Security training programme

[www.bioforce.assoc.fr](http://www.bioforce.assoc.fr)

# Information Note



## Staff Vulnerabilities

**Contributor:**  
**Corinna Kriedler -**  
**Security consultant**

### Age/previous work experience

- Younger people tend to take more risks, and especially young men
- Older, more experienced staff tend to be able to weigh the risks better, but also tend to become complacent about risk
- Nationally recruited staff – young national staff tend to be much more at risk, from attack by armed groups, or by perception of association with opposition groups, and also because of a tendency to take risks
- A more experienced person will have a better knowledge of the risks and their potential consequences, but statistics show that more significant is the amount of time the person has spent in that specific assignment

### Gender

- Female staff members are more likely to be the victim of sexual assaults, but are less likely to be taken hostage than men. Women international staff are often not subject to the same cultural norms and rules as nationally recruited women staff, and therefore may benefit from a certain degree of freedom in negotiation and debate, which is not available to other staff

### Nationality

- Staff coming from a country involved in a conflict may not be perceived as neutral. Both current and historical national interactions should be taken into account when recruiting staff, as should the availability of support from the appropriate embassy. The nationality of donors, and expatriate staff is also a significant factor in risk assessment

### Ethnicity

- Especially for nationally recruited staff, ethnicity is a critically important factor, and the ethnic mix of staff teams should be carefully managed. Both the social bonds between people from the same area or group are significant positive and negative

factors, as are the potential differences between people from different areas or groups

### Race

- There are potential problems associated with the race of staff members in being accepted by the local population – for example an African staff member in an Arab country or in the Balkans may find difficulties in being accepted

### Religion

- A staff member with strong religious affiliations should not be sent to a country where religion is a serious source of tension, and the display of religious symbols should not be public. The mission, vision and values of the organisation play an important part in people's perception of its neutrality, as does its choice of local partners

### Status/position

- The job title can be a factor in risk – e.g. human rights monitor, or security manager may influence other people or groups. In addition, the more senior that the job title implies, the more readily accepted the person may be at potential flash-points such as road blocks

### Language and communication skills

Ability to communicate in the international language in a country is a serious risk factor, adding substantially to the risk of an incident being misinterpreted or the level of danger increased through lack of understanding. For nationally recruited staff, the more local languages that are spoken the better will be the level of understanding of interlocutors in meetings, at roadblocks etc.