

APPROVED BY INTERACTION'S BOARD ON JUNE 14, 2006

Suggested Guidance for Implementing InterAction's Minimum Operating Security Standards

This document seeks to assist InterAction members in the incorporation of InterAction's Minimum Operating Security Standards (MOSS) in their respective institutional approaches to security. Recognizing that every organization will have differing needs, the "Suggested Guidance" section for each standard below represents point(s) to consider, rather than requirements, for implementing InterActions' Security Standards. Not every point is necessarily appropriate for every organization or for every situation.

STANDARD 1: ORGANIZATIONAL SECURITY POLICY AND PLANS

InterAction members shall have policies addressing key security issues and formal plans at both field and headquarters levels to address these issues.

SUGGESTED GUIDANCE

1. Establishing appropriate security policies.

Security policies should be reasonable in relationship to the organization's mission, mandate, commitments, and mode of operation which impact on security. They should clearly articulate the expectations the organization has of its employees and the responsibilities the organization assumes on behalf of its employees. Below are some issues that should be considered in developing security policies:

- ☞ Policy defining employees' rights, if any, to withdraw or remain due to security concerns.
- ☞ Definition of a framework for determining acceptable and unacceptable risks to staff, assets, and image of the organization.
- ☞ Guidance on the incorporation of acceptance, protection, and/or deterrence strategies.¹
- ☞ Agency response to employee being taken hostage and to demands for ransom or protection money.
- ☞ Position on offering or accepting gratuities, gifts, or bribes.
- ☞ Security incident reporting requirements.
- ☞ Use of weapons by employees.
- ☞ Use of armed security.
- ☞ Use of alcohol where prohibited.
- ☞ Use of drugs.
- ☞ Speaking with the media.
- ☞ Consequences for violation of security policies.
- ☞ Civil-military relations.
- ☞ Distinctions between policies regarding national and international staff.

2. Establishing appropriate and specific security plans at all levels of the organization.

¹ Van Brabant, K: *Operational Security Management in Violent Environments*, Overseas Development Institute, London, 2000.

Specific security plans should be reasonably related to the organization's mission, mandate, commitments, and mode of operation which impact on security and address the identified vulnerabilities and threats that facing staff.

Consider including the following items, as appropriate, in a headquarters security plans:

- ☉ A crisis management plan that describes the crisis management team and members' responsibilities.
- ☉ List of emergency contacts and the channels to reach them outside business hours.
- ☉ Procedures for contacting and maintaining communications with the next of kin of employees in emergency situations.

The following "Security Planning Guidelines" should be reviewed and considered in developing security plans for particular countries, regions and posts:

InterAction Security Planning Guidelines

Importance of Security Plans

Each agency operating in an area should develop and implement a security plan. A security plan is a single document containing information, standard operating procedures and contingency plans relating to the security of NGO staff and property. The purpose of a plan is to enable staff to act effectively to prevent and mitigate the effects of security problems in a manner appropriate to the agency.

Need for Individualized Security Plans

A security plan is based upon an individual agency's security strategy that reflects its overall approach to security. Each agency is likely to take a different approach based upon the agency mission, mandate (if applicable), principles, policies and programs, as well as on their understanding of the context.

Planning Process

The process of developing, implementing and updating a plan is as important as the plan itself. An individual should be designated responsibility for leading the development of the plan as well as for the periodic review and updating of the plan. Staff expected to implement the plan should be involved its development. This helps to foster consistent implementation through ensuring that (1) the plan is realistic in its assumption about the situation, threats, and staff willingness and ability to implement it, (2) the staff understands all aspects of the plan, and (3) the staff feels ownership of the plan, thereby promoting adherence to the plan. All new staff members should be given a briefing on the situation and threats, a copy of the plan, and any training required to implement the plan.

The plan should be tested and updated at regular intervals and whenever there is a change in the situation or threats faced by the NGO.

Components of a Security Plan

I. Introduction:

- Purpose of the plan
- Identification of the person(s) responsible for security and for leading the development, review and updating of the plan
- Intended users of the plan (which staff, locations, etc. are covered)
- Location of master plan and distribution list

II. Background:

- Articulation of agency mission, mandate (if applicable), principles and policies related to security.
- Summary of the situation (political, economic, historical, military, etc.)
- Threat assessment (indicating most likely types of threats NGOs will face)

III. Standard Operating Procedures:

Outline procedures for daily operations and routines as well as individual responses to incidents. For all procedures include (1) what to do/what not to do, (2) how to do it, as appropriate, (3) who does it/with whom, (4) when it is to be done; frequency and sequence, and (5) where it is to be done.

Site selection and management (offices, residences, etc.)

Movement and transport (vehicles, convoys, etc.)
Telecommunications (regular use and during emergencies)
Post incident actions (reporting, analysis, etc.)

IV. Contingency Plans:

Outline procedures for incidents requiring complex, multi-personnel responses. Include the same information as for standard operating procedures. Include also lines of communication and of authority. Articulate alternative options.

Evacuation
Medical evacuation
Death of staff
Other high risk, foreseeable events

V. Supporting Information:

- Warden system with contact information and instructions to locations
- Cooperating agencies, contact persons and information (phone numbers, radio frequencies, etc.)
- Contact information for government officials, airport, hospital, etc.
- Maps with assembly points, routes, borders
- Emergency supply inventory
- Incident reporting forms

STANDARD 2: RESOURCES TO ADDRESS SECURITY

InterAction members shall make available appropriate resources to meet these minimum operating Security Standards.

SUGGESTED GUIDANCE

Relevant resources that should be considered include, but may not be limited to: personnel, corporate will, funding, information, and material. Resources that may support security plans include: project design, specific line items in grants, inclusion of security expenses in negotiated overhead rates, or an organization's own unrestricted funding. InterAction will help the membership implement MOSS by facilitating sharing of information among its members, publishing security training opportunities, collecting and distributing security training materials, providing the advice of its security coordinator, and referral to specialized experts.

STANDARD 3: HUMAN RESOURCE MANAGEMENT

InterAction members shall implement reasonable hiring policies and personnel procedures to prepare staff to cope with the security issues at their post of assignment, support them during their service, and address post assignment issues.

SUGGESTED GUIDANCE

1. *All staff are provided with an orientation appropriate to the context of the area of assignment prior to, or immediately after, filling their position.*

Specific components of orientations might include, but are not limited to:

- Description of the organization's general mission and mandate as well as of its security policies
- Identification of specific threats individuals may face. Among such threats would be:
 - Potential natural phenomena such as earthquakes and hurricanes.
 - Potential technological accidents (CBRNE).
 - Potential or ongoing political instability, war, or insurgency.
 - Unstable or declining economic situation.
 - Targeted and/or random crime.
 - Potential hostage situations and kidnapping.
 - Existence of landmines, unexploded ordinance, and booby traps.
 - Ongoing or emerging persecution, violence, or harassment based on race, gender, ethnicity, religion, or nationality.
 - Unfamiliar cultural standards, norms, or laws in the country(s) of service.
- A copy of the security plan for the country(s) of service.
- Explanation of employee responsibilities and benefits during evacuation, relocation, hibernation, and suspension of operation.
- Description of operation and usage policy for communications and transport equipment at post.

2. Consider options for obtaining appropriate insurance coverage for staff and provide a general explanation to staff describing what is and is not covered with opportunities for staff to inquire into coverage in greater detail at their request.²

Some elements commonly included in insurance coverage and benefits for staff working in insecure environments are:

- Life, workers' compensation for work-related injuries, and health insurance.
- Medical evacuation.
- War risk supplemental coverage when country(s) of service are excluded from standard insurance company plan(s).

3. InterAction Members shall be guided and informed by the InterAction document, "The Security of National Staff: Essential Steps".

The following steps are recommended by *The Security of National Staff: Essential Steps 2002*:

- Encourage the involvement of national staff in the formulation, review and implementation of security policies and plans.
- Identify threats to national staff and act to reduce their vulnerability to these threats.
- Establish clarity on security procedures and benefits, especially with regard to evacuation and relocation options.
- Integrate national staff security into preparedness, training, and human resource management procedures.

4. Consider incorporating an employee's specific security responsibilities, if any, into their job descriptions or comparable documents,

The following suggestions may be helpful in developing appropriate job descriptions:

- Employees charged with specific security responsibilities have job descriptions with explicit descriptions of security duties.
- General references to security awareness may be appropriate in the job descriptions of other employees.
- Strive to make every effort to anticipate eventual or emergent security threats and vulnerabilities that could warrant additional duties.
- In circumstances where responsibilities are delegated after an employee's job description is established, amend the job description to reflect the new responsibilities.

²At a minimum, if available, insurance coverage should comply with any applicable legal requirements e.g., workers compensation for work related injuries.

5. All employees charged with security responsibilities receive adequate training to fulfill their obligations prior to or immediately after assuming their post.

The security training provided matches the security responsibilities described in the employee's job description and any reasonably anticipated responsibilities that the individual(s) may be expected to assume.

6. Resources permitting, consider providing all staff with the opportunity to receive appropriate post-incident counseling in a manner that promotes confidentiality and cultural sensitivity.

Appropriately trained individuals are available in a reasonable amount of time after a traumatic incident to provide counseling to all staff that require or request it. Where possible, allowances are made for counselors that can carry out this duty in a culturally sensitive and appropriate manner.

STANDARD 4: ACCOUNTABILITY

InterAction members shall incorporate accountability for security into their management systems at both field and headquarters levels.

SUGGESTED GUIDANCE

INTERACTION MEMBERS SHOULD DEVELOP CLEAR LINES OF RESPONSIBILITY FOR STAFF SECURITY AND DELEGATE TO EMPLOYEES CHARGED WITH THOSE RESPONSIBILITIES THE AUTHORITY TO ENSURE COMPLIANCE.

Establishing clear lines of responsibility and authority, as well as systems and structures for implementation of the organization's security policies, plans, and procedures helps ensure that these are observed. The following elements, may contribute to accountability:

- Periodic security briefings and drills which enhance knowledge of lines of responsibility and authority.
- Organizational security reviews include evaluation of effectiveness of management systems and structures as they relate to security (human resources, technology, procurement, etc.).
- Organizational security reviews include evaluations of employee fulfillment of their security responsibilities as individuals and, where appropriate, as supervisors.
- Personnel evaluations include assessments of how well employees comply with the security policies and practices of the organization.
- Violations of security policies and procedures have consequences for the violator (though always consistent with applicable labor laws).

STANDARD 5: SENSE OF COMMUNITY

InterAction members shall work in a collaborative manner with other members of the humanitarian and development community to advance their common security interests.

SUGGESTED GUIDANCE

1. Regular participation in security fora when possible.

The security of the employees of InterAction members is based on the individual organization's own policy and practice, the actions of other humanitarian and development actors, and the perceptions of local communities. Participation in

regular and/or ad-hoc security fora provides opportunities to share mutually useful information, exchange good practices, and consider the larger picture of security in the operating environment.

2. *When appropriate, work with UN coordination structures*

When, in an agency's view it is appropriate, it will take advantage of the Menu of Options endorsed by the UN Inter-Agency Standing Committee enabling NGOs to obtain security assistance available from United Nations security personnel.

3. *Sharing of significant security information with other humanitarian actors when appropriate.*

Information is the foundation of security. Sharing of significant information has many benefits from corroboration and verification to increasing the organization's knowledge base. Examples of useful information that might be shared include: incident reports and analysis, situation reports, threat assessments, and security training. While there is certainly some security information that cannot and will not be shared, members may consider whether significant security information might be shared in a format that is "scrubbed" of identifying information.

4. *Maintain awareness of, and when possible mitigate, any negative impact operations or conduct have on the security of other humanitarian actors.*

It is well known that the operations and / or conduct of one organization can impact the security of other members of the humanitarian community, if not the whole community. While it may never be possible to eliminate all the negative impacts one organization's operations have on others, actively seeking to minimize them will certainly make a difference.