

# Guidebook on ‘NGO Standards for Safety and Security’

Version 1.0 – April 2018

Japan NGO Initiative for Safety and Security (JaNISS)

## Contents

<b>Guidebook on ‘NGO Standards for Safety and Security’</b> .....	1
Version 1.0 – April 2018.....	1
About JaNISS .....	2
Acknowledgement .....	2
Disclaimer.....	2
Abbreviations.....	3
Aims of this Guidebook and How to Use It.....	4
1. Aims of this Guidebook .....	4
2. What this Guidebook covers .....	5
3. What this Guidebook does not cover.....	5
4. Structure of This Guidebook .....	6
5. Labelling of Information .....	6
6. How to Use This Guidebook.....	6
Background .....	8
1. Professionalization of Security Management in Humanitarian and Development Field ..8	
2. A Brief History of Changes in the Security Environment .....	9
3. Safety & Security is an Enabler for Programmes .....	9
Standard 1: Commitment to Safety and Security .....	11
Standard 2: Organizational Safety and Security Policies and Plans.....	16
2.1. Safety and Security Policies .....	16
Reference 2-I: Sample Outline of Safety and Security Policies.....	23
2.2. Security Plan at Headquarters .....	24
Reference 2-II: Sample Outline of a Security Plan for Headquarters .....	27
2.3. Security Plan in the Field.....	28
Reference 2-III: Sample Outline of a Security Plan for Field Posts .....	36
Standard 3: Resources .....	37
Reference 3-I: Support Program for External Security Training .....	39
Reference 3-II. Security Expenses that Can Be Included in Budget Supported by Japanese Donors.....	40
Standard 4: Human Resources Management.....	43
Standard 5: Accountability.....	47
Reference 5-I: Example Structure and Responsibilities.....	51
Standard 6: Collaboration with Other Actors .....	52
Standard 7: Safety and Security of Local Partner Organizations .....	55
References .....	58

## About JaNISS

Japan NGO Initiative for Safety and Security (JaNISS) is an independent network of like-minded Japanese NGOs active in the field of international humanitarian and development assistance. The objective of JaNISS is to support and coordinate capacity development so as to ensure safety and security management under international standards in the Japanese NGO community. To that end, it conducts activities such as drawing up safety and security standards and organizing safety and security management training for Japanese NGOs, and it also carries out advocacy in Japanese society to promote safety and security management by NGOs.

[www.janiss.net](http://www.janiss.net)

## Acknowledgement

This Guidebook is a result of collaborative efforts by JaNISS member NGOs. Development of the guidebook was managed by MOSS (Minimum Operating Security Standards) Task Force members throughout the drafting process, comprising: ADRA Japan, Japan International Volunteer Center, Japan Platform, Peace Winds Japan, Save the Children Japan, and World Vision Japan, co-led by Peace Boat Disaster Relief Volunteer Center, Shanti Volunteer Association and United Nations High Commissioner for Refugees (UNHCR).

JaNISS would like to thank UNHCR eCentre, InterAction and individual consultants, Randy Martin, Basile “Laky” Pissalidis and John Campbell, for sharing their expertise with us, and in particular, the UNHCR Representation in Japan for their extensive support. Many existing manuals and handbooks were helpful in the preparation of this Guidebook. Thanks also to all those Japanese NGOs who were involved and provided feedback throughout the drafting process.

## Disclaimer

JaNISS is a member-led grouping and has no separate legal status under the laws of Japan or any other jurisdiction, and references to ‘JaNISS’ in this disclaimer shall mean the member organizations, observers and secretariat of JaNISS. While JaNISS endeavours to ensure that the information in this document is correct, JaNISS does not warrant its accuracy and completeness. This document is general in nature, and its contents may not be applicable in all situations. Its contents shall be modified and adapted as appropriate, to suit the needs of particular organizations and situations. JaNISS shall not be liable for any kind of loss or damage whatsoever to you or a third party arising from reliance on the information contained in this document. This document may include the views or recommendations of third parties and does not necessarily reflect the views of JaNISS or indicate a commitment to a particular course of action.

© 2018 Japan NGO Initiative for Safety and Security

## Abbreviations

CHS: Core Humanitarian Standard on Quality and Accountability  
CIMP: Critical Incident Management Plan  
CIMT: Critical Incident Management Team  
eCentre: UNHCR Regional Centre for Emergency Preparedness  
ECHO: Directorate-General for European Civil Protection and Humanitarian Aid Operations  
GPR8: Good Practice Review 8  
HF: High Frequency  
IFRC: International Red Cross and Red Crescent Movement  
INSO: International NGO Security Organization  
ISAF: International Security Assistance Force  
JaNISS: Japan NGO Initiative for Safety and Security  
Medevac: Medical Evacuation  
MOFA: Ministry of Foreign Affairs  
MOU: Memorandum of Understanding  
NRC: Norwegian Refugee Council  
PRT: Provincial Reconstruction Team  
PTSD: Posttraumatic Stress Disorder  
R&R: Rest and Recreation  
SIF: Safety in the Field  
SLT: ‘Saving Lives Together’  
SOPs: Standard Operating Procedures  
SRA: Security Risk Assessment  
SRM: Security Risk Management  
TOR: Terms of Reference  
UNDSS: United Nations Department of Safety and Security  
VHF: Very High Frequency

## Aims of this Guidebook and How to Use It

### 1. Aims of this Guidebook

The 'NGO Standards for Safety and Security' (hereafter Standards) were adopted by the member NGOs of Japan NGO Initiative for Safety and Security (JaNISS). The Standards capture the most common denominators in the internationally accepted safety and security standards, where the signatory NGOs are expected to develop their own policies and mechanisms.

The Standards intend to complement existing safety and security frameworks of signatory NGOs which should be specific and unique to each organization.

The Standards is made of following seven Standards: ‘Commitment to Safety and Security’, ‘Organizational Safety and Security Policies and Plans’, ‘Resources’, ‘Human Resources Management’, ‘Accountability’, ‘Collaboration with Other Actors’, and ‘Safety and Security of Local Partner Organizations’.

Each NGO is ultimately responsible for determining how the seven Standards will be met within their own organization. How this is accomplished will be based on the mission, mandate, values and risk tolerance of each organization.

This Guidebook on 'NGO Standards for Safety and Security' (hereafter Guidebook) has been produced by the member NGOs of JaNISS to support Japanese NGOs in translating these seven Standards into tangible actions. This Guidebook also includes following objectives:

- To assist individual Japanese NGOs self-evaluate the extent to which they have covered the safety and security policies and procedures that should be considered according to the Standards, and to locate suggested guidance, tools and resources when they identify room for improvement.
- To provide Japanese NGOs with references to relevant documents and online information accumulated by the United Nations organizations and international NGOs
- To introduce, and encourage the introduction of, methods and ideas related to safety and security which have not been fully incorporated by Japanese NGOs such as security risk analysis, security planning and reviewing involving all relevant staff members, security related training, and clear definition of the security roles and responsibilities of managers and staff members.

Based on consultation with a wide range of humanitarian and development NGOs, this Guidebook also aims to achieve following goals:

- Applicable not only to Japanese NGOs working in conflict or high-risk areas but also to those who work in the overseas humanitarian and development operations.
- Applicable to various Japanese NGOs regardless of their organizational size and operational scale, category of staff (from paid to unpaid), presence in the field (expatriate or mission-based), and organization’s mission and mandate (from emergency relief to study tour).

- Informative to Japanese NGOs located outside the metropolitan area where access to materials on security management has been limited and to assist their capacity-building efforts by providing relevant information on guidelines, tools and resources.

## **2. What this Guidebook covers**

This Guidebook intends to cover following aspects of security management and practice:

- This Guidebook intends to cover most aspects of security management and practice that are commonly thought relevant to Japanese NGOs working in humanitarian and development operations.
- This Guidebook intends to cover both national/local and international staff equally, unless it is explicitly referred to one or the other group.
- This Guidebook intends to focus mainly on ‘security’ rather than ‘health and safety’ issues (see the definitions of ‘safety’ and ‘security’ in Standard 2.1, Guidance Note 1).
- This Guidebook is comprised of existing good practices drawn extensively from security policies and manuals produced by network NGOs such as InterAction and European Interagency Security Forum (EISF), humanitarian NGOs, UN agencies and the International Red Cross and Red Crescent Movement.

## **3. What this Guidebook does not cover**

At the same time, this Guidebook does not intend to cover following aspects of security management and practice:

- This Guidebook is general in nature, and its contents may neither be applicable to all situations nor cover aspects of security management and practice that are specific to particular locations, cultures, or type of humanitarian or development operations. Its contents should be modified and adapted as appropriate, to suit the needs of particular organizations and situations.
- This Guidebook is intended neither to provide off-the-shelf safety and security standards and policies for individual NGOs nor impose certain standards or policies on individual NGOs. It offers suggested guideline, tools and resources, designed to assist organizations to think through their security policies and procedures. Each organization has different operational context, mission and mandate, operational period, financial and human resources, and involvement into various aid and local networks, and their security policies and procedures should be established according to individual organizational and operational contexts with the involvement of all relevant international and national/local staff.
- At the moment, issues related to ‘safety’, such as health threats and natural disasters, may not be the primary focus of this Guidebook, but it also draws attention to the matters associated to vehicle accidents, insurance and medical evacuation and the need of post-incident psychosocial support. It is important to remember that health and safety threats also pose significant threats to aid workers and organizations, and should take precautions accordingly.
- This Guidebook does not cover the security or protection of local populations, refugees and displaced persons, women and children, or other vulnerable persons.

- Most of all, this Guidebook is no guarantee of ‘security’. Using this Guidebook does not replace the need for regular and inclusive planning, appropriate training, judgement based on experience, coupled with the relevant equipment and procedures, applied as each situation and operation requires.

#### 4. Structure of This Guidebook

This Guidebook follows the examples of the Sphere Handbook, and is composed of several standards, relevant key actions, key indicators, and guidance notes.

- **Key Actions:** are suggested to attain the standard. Some actions may not be applicable in all contexts, and it is up to the organizations to select the relevant actions and devise alternative actions that will result in the standard being met.
- **Key Indicators:** serve as ‘signals’ that show whether a standard has been attained. They provide a way of measuring and communicating the processes and results of the key actions. The key indicators relate to the minimum standard, not to the key actions.
- **Guidance Notes:** include context-specific points to consider when aiming at reaching the key actions and key indicators. They provide knowledge, good practices, information and resources accumulated by the global humanitarian and development community. Further details and references are provided at the end of each chapter.

#### 5. Labelling of Information

- Standards, Key Actions and Key Indicators are **bordered**.
- Guidance notes of particular importance are **highlighted in blue**.
- Information in Standard 2 that is of particular importance to those operating in conflict areas or high-risk areas are **shaded**.

#### 6. How to Use This Guidebook

- A) Senior Managers and Operational Managers of Organizations (Executive Board Members): It is strongly recommended to refer at least the following sections of this Guidebook in order to understand the general outline of security risk management including the duty of care.
- Standard 1
  - Key Actions and Key Indicators for other standards (there are three Key Actions and Indicators in the Standard 2)
  - Sections that are **highlighted in blue**
- B) Security Managers/Officers of Humanitarian Organizations: It is recommended to read through this Guidebook. For those organizations operating in conflict or high-risk areas, it is strongly encouraged to closely examine the sections that are **shaded** in Standard 2.

- C) Security Managers/Officers of Development Organizations: When appropriate, refer the shaded sections in Standard 2 which are intended for organizations operating in conflict or high-risk areas, but otherwise it is recommended to read through the rest of this Guidebook.
- D) For a Quick Overview of the Guidebook: It is recommended to refer the following sections.
- Key Actions and Key Indicators of each Standard (there are three Key Actions and Key Indicators in Standard 2)
  - The ‘Background’
  - Sections highlighted in blue
- E) Those Wishing to Conduct a ‘Self-check’ on Their Organization’s Security Plans and Procedures, or Wishing to Create Security Plans for Their Organization

Refer Guidance Notes and References in Standard 2 to assess the organization’s security management, and take necessary measures and actions to improve the organization’s security policies, procedures and plans.

It is highly recommend to compile the reflections, measures and actions taken into a document and sharing it with relevant parties. The critical part of this exercise lies in the process of planning and reviewing the security plan with the involvement of all relevant staff, and not the document itself that is produced by this exercise. Thus, the document should be kept simple and concise.

Organizations that do not have field offices and that operate on a mission-basis are recommended to take ‘2.3 Security Plan in the Field’ into consideration when they are considering ‘2.2 Security Plan at Headquarters’ and the security plan for partner organizations.

- “Safety and Security Policies”, “Reference 2-I: Sample Outline of Safety and Security Policies”
- “Security Plan at Headquarters”, “Reference 2-II: Sample Outline of a Security Plan for Headquarters”
- “Security Plan in the Field”, “Reference 2-III: Sample Outline of a Security Plan for Field Posts”

## Background

### 1. Professionalization of Security Management in Humanitarian and Development Field

Looking back on the history of Japanese NGOs, the first wave of emergence took place in the early 1960s, when several organizations were founded aiming at addressing the social development needs in Asian countries, followed by the second wave when a number of existing organizations were established around 1979 as a result of the Indochina refugee crisis.<sup>1</sup> In the 30 years since their advent, Japanese NGOs have expanded their operational size, and are now working in various sectors not only in Asian countries but also in countries in the Middle East, Africa, and Latin America. Quite a few NGOs do not limit themselves to working in development, but are proactively engaged in the humanitarian response both in natural and complex emergencies.

Regardless of whether working in a development context or a humanitarian context, expansion of operational size increases the chance of encountering various threats. According to the Humanitarian Outcomes report, the nature of the security environment has become much more complex since the 1990s. For 10 years between 2005 and 2015, the number of casualties of aid workers has been steadily increasing. Japanese staff are not immune to this trend.<sup>2</sup> Since the turn of the century, there have been reports of a number of cases in which Japanese staff have been kidnapped or abducted, taken hostage, or become victims of terrorism. Even excluding victims of security-related incidents, a number of aid workers have lost their lives due to contingent events such as road accidents and diseases.

Given the prevalence of security as well as safety related threats, what kind of security risks could NGOs face in their working environment? Take the threat of malaria as an example. Suppose that a Japanese staff managing a project in an area where malaria is endemic is infected by malaria and hospitalized in a dazed condition. As long as the organization took the decision to implement a project in such an area, it should have provided the staff with necessary measures to prevent malaria as well as all possible means to protect their life in case of infection. In the worst-case scenario of loss of life, the top management of the organization will inevitably have to explain the incident to the public.

As NGOs working in the field of international cooperation, we are responsible for ensuring the safety and security of all concerned staff and stakeholders. This means that if any person involved in our work – irrespective of whether an international staff or a national/local staff, or whether a direct employee or a beneficiary – becomes a victim of any type of incident, we are morally and legally obliged to take institutional action. If the organization does not properly respond to the incident, it may lead to serious consequences such as cessation of the project or, in the worst case, dissolution of the organization. We are therefore required to professionalize ourselves in term of security management.

---

<sup>1</sup> Japan NGO Center for International Cooperation (JANIC). (n.d.). *Understanding NGOs* [Japanese article]. Retrieved on 21 March 2018 from [www.janic.org/ngo/faq/](http://www.janic.org/ngo/faq/).

<sup>2</sup> The Aid Worker Security Database. (n.d.), Major attacks on aid workers: Summary statistics. Retrieved on 21 March 2018 from <https://aidworkersecurity.org>.

This chapter describes the threats that NGOs are facing, giving an overview of how the safety and security environment has changed over the decades since the emergence of Japanese NGOs, and describes the institutional responsibilities that organizations should take when working in high-risk environments, and concludes by stressing the importance of security management as an enabler for programs and accountability.

## **2. A Brief History of Changes in the Security Environment**

- **1960s to 1980s**  
Japanese NGOs emerged in this period. While a nuclear war was the main security threat during the Cold War, the threat of ethnic or religious conflict was not so prevalent as nowadays. The major safety and security concerns for NGOs therefore were mainly those of ordinary crime, traffic accidents, and diseases.
- **1990s**  
The end of the Cold War triggered the rise of political and religious radicalism as well as ethnic cleansing, which led to ethnic and religious conflicts worldwide. Along with the increase in humanitarian need in conflict affected areas, Japanese NGOs also began entering the field of humanitarian assistance, which required those working in the humanitarian arena to be well aware of the security concerns and to take necessary measures. Incidents directly targeting Japanese staff, however, were still rare during this period.
- **2000s**  
The establishment of Provincial Reconstruction Teams (PRT) became a controversial issue, potentially increasing security threats to humanitarian workers particularly in Afghanistan and Iraq. Kidnappings and assaults directly targeting Japanese nationals frequently occurred between 2004 and 2008 in those countries. These incidents compelled humanitarian agencies to re-assess their own security measures. This period also became a turning point in that the government of Japan shifted its stance and restricted Japanese nationals from going to medium/high-risk areas.
- **2010s**  
Protracted conflicts in the Middle East and Africa exacerbated the security environment. Japanese nationals continue to fall victim to kidnappings and assaults in countries such as Syria, Algeria and Bangladesh, giving Japanese humanitarian workers little space to operate in medium/high-risk areas. Widespread indiscriminate terrorism is another security concern; countries not affected by conflicts are no longer immune to terrorism. It requires those involved in development, whose mandate is not necessarily of a humanitarian nature, to raise their awareness of security management.

## **3. Safety & Security is an Enabler for Programmes**

Each organization has its own respective mission and, in pursuit of it, we must continuously weigh the outcomes we aim to achieve against the risks we may face. We are able to provide assistance only when we judge that the expected outcome is larger than the risks we may face.

The worldwide deterioration of the security environment since the 1990s tilts the scales against the pursuit of our missions, meaning that the security risks are often higher than the outcomes we may expect. While security threats have increased significantly over the decades, humanitarian and development needs are also increasing more than ever before. In such circumstances, it is the NGO itself that should make the decision whether or not to go to a high-risk environment, and if it decides to go, the organization must be responsible for potential outcomes that may occur as a result of taking security risks. As a result, the governing bodies of the NGO (such as the Board of Directors) will bear the duty of care for their staff and operations.

While it may be true that we should avoid taking risks where possible, we should not give up pursuing our missions simply because there is a security risk. This is because it is the mission of NGOs to address the challenges underlying the security threats. Security Risk Management (SRM) is therefore essential in order to pursue our mission. SRM is a way to properly manage the risks rather than simply avoiding them, to minimize the negative effects, to establish an environment where we can operate, and to be accountable for ourselves. Facing the threats does not necessarily mean we have to avoid them; rather, we are required to manage them. The next chapters will introduce seven standards that enable organizations to operate in high-risk environments. These standards are not the goal per se, but are a means to the end.

### **Column: Provincial Reconstruction Team (PRT)**

PRT is a military-civilian structure designed to operate in insecure environments such as post-conflict countries. It was initiated by the U.S. in post-Taliban Afghanistan in the early 2000s. A number of PRTs were formulated mainly by the NATO states and their command authority was delegated to International Security Assistance Force (ISAF). Under the command of the armed forces of the countries in charge, military units engage in security enforcement whereas civilian units provide aid assistance. As of July 2017, there are 26 PRTs led by 14 countries<sup>3</sup>. PRTs were also in operation from 2005 to 2011 in Iraq. While it has been said that PRTs improve security, support good governance, and enhance provincial development, criticisms also have been raised from civil society arguing that, because of the nature of military-oriented operation, there are concerns about the PRTs’ efficiency, speciality and equity in delivering aid assistance. Civil societies too are concerned that security threats to humanitarian workers could increase as local people could mistake humanitarian workers for military-associated personnel.<sup>4</sup>

---

<sup>3</sup> USAID. (2018). *Provincial Reconstruction Teams*. Retrieved on 21 March 2018 from <https://www.usaid.gov/provincial-reconstruction-teams>.

<sup>4</sup> Kei’ichiro Tomita. (2007). Provisional Reconstruction Team (PRT) Operations in Afghanistan [Japanese article]. *Reference 2007-03*. Retrieved 21 March 2018 from <http://dl.ndl.go.jp/info:ndljp/pid/999764>; Japan Afghan NGO Network (JANN). (2009). *On Civilian Assistance in Afghanistan Alternative to Japan’s Refuelling Mission in the Indian Ocean* [Japanese article]. Retrieved on 21 March 2018 from [http://www.ngo-jvc.net/jp/notice/2010/data/20100219\\_afghanistan\\_lobby.pdf](http://www.ngo-jvc.net/jp/notice/2010/data/20100219_afghanistan_lobby.pdf).

## Standard 1: Commitment to Safety and Security

*The management of signatory organizations commits to ensure the safety and security of its staff, volunteers, interns, and contractors in line with their duty of care and accepted international standards for safety and security.*

### Primary Responsibility

Safety and security are not only an ethical and moral concern that may arise as a result of an individual’s desire to engage in international cooperation, but are also an explicit legal obligation. This requires the recognition and acceptance of responsibility and accountability under the law, through a top-down approach driven by the organization’s governing bodies. As a result, institutional policy should not be a condensed version of amalgamated field practices. Thus, the primary responsibility of representatives of the organization is to ensure the safety and security of its own staff members.

### Duty of Care

Duty of care is an organizational obligation that has implications for SRM. The duty of care benchmark has risen significantly over the past decade, and what was once considered good enough would certainly not be considered adequate today. Although duty of care is a legal term for the responsibilities that organizations have towards their staff, there is also a moral obligation of duty of care that organizations should consider. As professionals engaged in humanitarian and development activities, duty of care to aid workers should not be undermined and indeed it should be complemented as far as possible.

### Accepted International Standards

As humanitarian programmes expanded globally in the 1990s, there was a growing recognition of the need to improve professional standards, to enhance the effectiveness of interventions, and to ensure accountability within the humanitarian system as a whole. In response, major international standards on humanitarian work emerged such as Humanitarian Principles, Code of Conduct for the International Red Cross and Red Crescent Movement and Non-Governmental Organizations (NGOs) in Disaster Relief and Core Humanitarian Standard on Quality and Accountability (CHS). They guide humanitarian action and their application is essential to distinguish humanitarian action from other forms of activities and action. There is a general consensus that compliance with these international standards enhances organizational safety and security in both humanitarian and development field.

### Key Actions:

- Make sure that the governing bodies of the organization explicitly state and communicate the organization’s legal responsibilities to all employees concerning safety and security in the workplace.
- Make sure that the governing bodies of the organization delegate responsibilities explicitly (i.e. to the chair of the board) to ensure legal and regulatory compliance concerning safety and security in the workplace.
- Incorporate accepted international standards and, if applicable to organizational mission and mandate, consider becoming a signatory.

- Make employees aware of their legal rights and obligations concerning safety and security in the workplace.

#### **Key Indicators:**

- Responsibility for legal compliance is known throughout the organization and to other relevant stakeholders.
- Compliance with laws and regulations is reviewed in line with accepted international standards on a regular basis.

#### **Guidance Notes:**

1. **Scope of Application:** National laws of the country in which NGOs are registered apply to organizations, associations, employers and employees. This includes national laws which address health and safety in the workplace. NGOs owe a legal responsibility to their employees to ensure a safe work environment, whatever and wherever that may be, and to take reasonable practical steps to protect them against any foreseeable risks. This responsibility is no less relevant to insecure field environments that often present context-specific risks and NGOs are subject to the same legal obligations and responsibilities as other organizations.
2. **Duty of Care:** The duty of care is a legal obligation imposed on an individual or organization requiring them to adhere to a standard of reasonable care while performing acts that present a reasonably foreseeable risk of harm to others. Negligence is often defined as a failure to adhere to (or breach) a standard of reasonable care, resulting in both organizational and individual loss, damage and injury. The standard of reasonable care is typically assessed by reference to the actions of a person exercising reasonable care and skill in the same or similar circumstances. The standard of reasonable care will vary from country to country.
3. **Civil Code Article 644:** In the Japanese context, the duty of care of an organization refers to “Duty of Care of Mandatory” in Article 644 of the Civil Code. The organization and the governing bodies are in a relationship in which the responsibilities of the organization are delegated to the governing bodies by the organization. In accordance with Article 644, the governing bodies (referring to board directors, supervisors, auditors, etc.) to which the organizational responsibilities are delegated “shall assume a duty to administer the mandated business with the care of a good manager in compliance with the main purport of the mandate”, i.e. duty of care. Therefore, the governing bodies, according to their position and ability, no matter whether they are paid or unpaid, whether full-time or part-time, are required to perform their authority and responsibilities with duty of care.
4. **Humanitarian Principles:** Underlining all humanitarian action are the principles of humanity, impartiality, neutrality and independence. These principles, derived from international humanitarian law, have been taken up by the United Nations in General Assembly Resolutions 46/182 and 58/114. Their global recognition and relevance are furthermore underscored by the Code of Conduct for the International Red Cross and Red Crescent Movement and Non-Governmental Organizations (NGOs) in Disaster Relief

(Guidance Note 5) and the Core Humanitarian Standard on Quality and Accountability (Guidance Note 7), and are relevant to both humanitarian and development agencies. Because humanitarian action should be non-political, humanitarian and social, the organization is guided by humanitarian principles in its response to all humanitarian issues, whether caused by conflict, violence, natural disaster or poverty. The principle of “Do No Harm”, for example, obliges an organization to prevent and mitigate any negative impact of its actions on affected populations. Humanitarian principles provide the basis for warring parties to accept humanitarian action in situations of armed conflict. It is important to ensure that organizational policies and operational decision-making on issues such as funding, beneficiaries, modes of operation, and security measures are in line with humanitarian principles.

5. **Code of Conduct for the International Red Cross and Red Crescent Movement and Non-Governmental Organizations (NGOs) in Disaster Relief:** The Code of Conduct sets out ten core principles as well as three annexes with recommendations to governments of affected states, donor governments and intergovernmental organizations. Over the years, adherence to the Code has become one important way for the International Red Cross and Red Crescent Movement (IFRC) and NGOs to define themselves as humanitarians. Since the development of the Code of Conduct, there have been many developments in terms of standards and mechanisms to improve the quality and accountability of humanitarian response. However, the Code of Conduct remains a central reference in the sector. The IFRC keeps a public listing on this site of all the humanitarian organizations that become signatories of the Code and new signatories are welcome to register at any time. The IFRC neither vets new signatories nor monitors their compliance. However, in order to be listed on this site as a signatory, each organization must (1) affirm that it is a humanitarian organization; (2) provide and update all requested contact details, including its website address; and (3) submit its request through the head of the organization. To register, please visit the IFRC’s website at: <http://media.ifrc.org/ifrc/who-we-are/the-movement/code-of-conduct/>
6. **InterAction’s Minimum Operating Security Standards (MOSS):** Reflecting the operational environment of NGOs and the rise of serious incidents such as killings, kidnappings, and attacks that cause serious injuries, as well as politically-motivated attacks against humanitarian workers, InterAction, which is the largest alliance of U.S.-based international non-governmental organizations (NGOs) who focus on disaster relief and sustainable development programs, has established a Security Unit to help members develop appropriate responses. In this context, InterAction’s MOSS was developed to assist InterAction’s members to develop their own security management system in incorporating 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 points to consider, rather than requirements, for implementing InterAction’s Security Standards. Not every point is necessarily appropriate for every organization or for every situation. MOSS-introduced systematic approaches to NGOs’ risk management and those security risk management systems have become the industry standard, which many of InterAction’s members follow. JaNISS referred to InterAction’s MOSS when developing its own NGO Standards for Safety and Security and this guidebook with technical cooperation from InterAction’s Security Unit.

- 7. Core Humanitarian Standard (CHS):** The Core Humanitarian Standard on Quality and Accountability (CHS) sets out Nine Commitments that organizations and individuals involved in humanitarian response can use to improve the quality and effectiveness of the assistance they provide. It also facilitates greater accountability to communities and people affected by crisis: knowing what humanitarian organizations have committed to will enable them to hold those organizations to account. The CHS places communities and people affected by crisis at the centre of humanitarian action and promotes respect for their fundamental human rights. It is underpinned by the right to life with dignity, and the right to protection and security as set forth in international law, including within the International Bill of Human Rights. As a core standard, the CHS describes the essential elements of principled, accountable and high-quality humanitarian action. Humanitarian organizations may use it as a voluntary code with which to align their own internal procedures. It can also be used as a basis for verification of performance, for which a specific framework and associated indicators have been developed to ensure relevance to different contexts and types of organization.

#### **Column: Case Law on Duty of Care (Dennis vs Norwegian Refugee Council)**

On 29 June 2012, Steve Dennis, an employee of the Norwegian Refugee Council (NRC), was injured and kidnapped, along with three other colleagues, following an attack during a VIP visit to the IFO II refugee camp in Dadaab, Kenya. Four days later the hostages were set free during an armed rescue operation carried out by Kenyan authorities and local militia. Three years later, Dennis submitted a claim at the Oslo District Court against his former employer, the NRC, for compensation for economic and non-economic loss following the kidnapping. With a focus on determining negligence in relation to the incident, the Court considered and reached conclusions on the following: the foreseeability of risk, mitigating measures to reduce and avert risk, gross negligence, causation and loss.

The Court found that the risk of kidnapping was foreseeable. It also found that the NRC could have implemented mitigating measures to reduce and avert the risk of kidnapping. The Court furthermore found that the NRC acted with gross negligence and that the NRC's negligent conduct was a necessary condition for the kidnapping to have occurred. In summary, the Court found that the legal requirements for compensation for injury, as well as compensation for pain and suffering were met. The Court ordered the NRC to pay Dennis approximately 4.4 million Norwegian Krone (approximately 465,000 euros (60 million yen)).

Although the terminology and approach used by the Court differ from a standard SRM approach, the ruling refers to elements familiar to security experts and uses some of the evidence of failings in these areas to find that the NRC fell short of meeting due care standards in this instance. For example, in terms of context and risk analyses, the Court found that there was an insufficient understanding of the security situation in Dadaab by the NRC decision-makers, which resulted in the risk of kidnapping not being properly analysed shortly before the VIP visit. The Court also found weaknesses with regards to the identification and implementation of mitigating measures, particularly in relation to the decision to not use an armed escort, which was contrary to existing practice and security recommendations for Dadaab at the time.

The fundamental conclusion that can be drawn from the court case is that duty of care is a legal obligation that organizations in the international aid sector must adhere to and that they must do so to the same standard as any other employer. The ruling does not argue, despite the context, that operating in Dadaab was contrary to the law. The case instead highlights that mitigating measures must be proportionate to the risk. Therefore, the ruling should not cause organizations to become more risk averse but rather cause them to institute stronger SRM procedures in line with the context they are operating in. The ruling furthermore highlights that an essential component of duty of care in high-risk environments is ‘informed consent’. The Court found that informed consent was doubtful or entirely absent in some instances leading up to the incident.

The case was covered widely in mainstream media and discussed at length by aid workers and organizations in different forums and analytical reports. It was described as: a ‘landmark case’, ‘precedent-setting’, a ‘game-changer’, and a ‘wake-up call’ for the aid industry, with significant remarks on duty of care.

### **References**

- Irish Aid. (2013). *Irish Aid Guidelines for NGO Professional Safety and Security Risk Management*.
- Shaun Bickley. (2017). *Security Risk Management: A Basic Guide for Smaller NGOs*. European Interagency Security Forum (EISF).
- Maarten Merkelbach and Edward Kemp. (2016). *Duty of Care: A review of the Dennis v Norwegian Refugee Council ruling and its implications*. European Interagency Security Forum (EISF).
- Kelsey Hoppe and Christine Williamson. (2016). *Dennis vs Norwegian Refugee Council: Implications for Duty of Care*. Humanitarian Practise Network (HPN).

## Standard 2: Organizational Safety and Security Policies and Plans

*Signatories shall have an organization safety and security policies in accordance to the organization’s mission, mandate, values and risk tolerance at headquarters’ level, and security plans at both the headquarters and field levels based on a participatory security risk assessment and analysis.*

Standard 2 states that organizations shall have: (1) **safety and security policies** and (2) **security plans** at both headquarters and field levels. Safety and security policies are protocols that guide all the agency’s security decisions. Security plan at the headquarters level defines the relationship between the headquarters and field operations as well as security procedures at the headquarters, and country-specific security plans are tailored to respond to a specific context to the location.

### 2.1. Safety and Security Policies

**Safety and security policies** apply to the entire organization. These policies will reflect the organization’s unique mission, mandate, commitments, mode of operation and risk tolerance. They should clearly articulate the expectations the organization has of its employees and the organization’s responsibility to its employees, including redress in the event the organization or its employees fail to adhere to security policies.

#### Key Actions:

- Safety and security risks, the organization’s safety and security risk attitude, key security principles, roles related to SRM and the organization’s responsibilities to its employees are explicitly defined in the safety and security policies. (see also Guidance Notes 1, 2, 3, 4 and 5; see Reference 2-1 for a sample outline of safety and security policies)
- Safety and security policies clearly state the organization’s risk management objectives and the rationale for managing security risks that are based on the security risk assessment, and make clear links to the organization’s overall mission, mandate, commitments, and mode of operation.
- The expectations the organization has of its employees and the organization’s responsibility to its employees, including redress and disciplinary action in the event the organization or its employees fail to adhere to security policies are clearly articulated in the safety and security policies. (see also Guidance Note 3)
- The safety and security policies are put in writing and are understood by all staff members including headquarters and field locations. (see also Guidance Note 5 and Reference 2-1 regarding the key issues to be considered in the safety and security policies)

#### Key Indicators:

- The organization’s safety and security policies clearly state the organization’s definition of security risk, security risk attitude, key security principles, roles and responsibilities.

- The organization’s safety and security policies include a value statement relating to safety and security of the organization’s staff, and a clear operational link between this value statement and security related Standard Operating Procedures (SOPs) at the field level.
- Both the management and staff (including employees, volunteers, interns, contractors and others) understand their obligation to comply with the organization’s safety and security policies and procedures.
- Regular reviews of safety and security policies and procedures are conducted with the participation of all relevant staff.

### Guidance Notes:

1. **Definition of Safety and Security:** ‘Safety’ refers to ‘freedom from risk or harm as a result of unintentional acts, such as accidents, natural phenomena or illness’ whereas ‘security’ refers to ‘freedom from risk or harm resulting from violence or other intentional acts’.<sup>5</sup> While ensuring the security of staff, assets and programmes against assault, abduction, robbery, terrorism or sabotage necessarily requires the investment of considerable time and resources, it is important to remember that safety threats such as vehicle accidents, malaria, water-borne diseases, HIV and other health threats, mental health, and natural disasters such as floods and earthquakes also pose significant threats to aid workers.
2. **Organization’s Mission, Mandate and Values:** It is important for the organization’s managers to understand that the mission, mandate and values impact on the security threats and risks that the staff face in the field. The vulnerability of NGOs significantly changes with the overarching mandate and field operations of the organizations. For example, those organizations working for human rights protection and development may face different security risks, and those organizations working for life-saving activities has an ethical obligation to withstand higher level of security risk than an organization involved in livelihood projects.

Every NGOs have their unique mission, mandate and values and operate in various context specific environments, which is to say that every NGOs should develop and have different thresholds of acceptable security risk, security policies and plans. An organization’s exposure to security threats is directly related to its mandate and mission. For that reason, it is essential to include the organization’s mission and mandate statement and values in the security policies so that the staff will understand the nature of its operations and the surrounding security environments.

3. **Security Strategies (Acceptance, Protection and Deterrence):** The organization’s safety and security policies should state what security strategies it uses generally and in specific contexts. There are typically three security strategies used by humanitarian agencies in all contexts.

---

<sup>5</sup> Overseas Development Institute. (2010). *Operational Security Management in Violent Environments, Good Practice Review Number 8 (New Edition)*. Humanitarian Practice Network [hereafter GPR8 (2010)], London: Overseas Development Institute, p.xvii.

- **Acceptance:** Building a safe operating environment through consent, approval and cooperation from individuals, communities and local authorities.
- **Protection:** Reducing the risk, but not the threat, by reducing the vulnerability of the organization, typically by increasing physical protection of buildings, compounds, and/or distribution sites.
- **Deterrence:** Reducing the risk by containing the threat with a counter threat, such as armed protection, diplomatic and political leverage, and temporary suspension.

Given their mission and values, humanitarian agencies find that a far more appealing security strategy is acceptance: acceptance can and should be the foundation of all security strategies.<sup>6</sup> In reality, the acceptance approach is usually not enough on its own, and humanitarian agencies need at least some protection even when there is wide local support. Deterrence is usually the strategy of last resort when acceptance and protection have not been successful or have proven inadequate, but the range of measures is very limited for humanitarian agencies.

In practice, a good security strategy needs a flexible combination of the above-mentioned approaches. The point is that security management should be proactive, involving conscious choices about the mix of approaches pursued in the light of the threats identified, and the approaches other agencies are taking. It is also important to remember that different approaches have different resource implications.

#### **References**

- Overseas Development Institute (2010), *Operational Security Management in Violent Environments, Good Practice Review Number 8 (New Edition)* [hereafter GPR8 (2010)]. Humanitarian Practice Network, Chapter 3 Security Strategy
- James Davis. (2015), *Security to Go: A Risk Management Toolkit for Humanitarian Aid Agencies, Module 4 Security Strategies: Acceptance Protection and Deterrence* [hereafter, EISF (2015)]
- European Commission’s Directorate-General for Humanitarian Aid (ECHO). (2004). *Generic Security Guide for Humanitarian Organizations* [hereafter ECHO (2004)], Section 2.3 Approaches to Security
- Mercy Corps. (2011), *Field Security Manual (March 2011)*. The Security Triangle

#### **4. Security Risk Assessment (SRA): Definition of a framework for determining an acceptable threshold of risk to staff, assets, and image of the organization**

Proper assessment of risk is a critical component of good safety and security management. The SRA is the core of any security plan. Every security plan should identify threats and address them through proper risk mitigation measures and contingency plans, based upon an appropriate SRA (see also Mitigation Measure in 2.3 Security Plan in the Field). Contemporary thinking on good practice holds that organizations should conduct a SRA before starting operations in a new location, and that this should inform programme design from the very beginning.

---

<sup>6</sup> GPR8 (2010), p.56.

The objective of the exercise is to help determine the level of risk in undertaking a programme, and weigh this risk against the benefits the programme brings to the population being helped. In this context, the SRA process should be considered as a central part of programme and project design since exposure to risk and mitigation measures are both linked to programme objectives and implementation.

The SRA can cover a broad range of threats including violence, conflict, natural hazards, terrorism, health issues, political interference, crime and corruption. The SRA should include context and programme analysis, threat and vulnerability assessment, and risk analysis (impacts, likelihood, and mitigation measures and risk threshold).

The SRA is not something to be completed and put on the shelf, but should be treated as a living document that is frequently revisited and revised as the situation changes. The SRA should be inclusive, drawing perspectives and information from all staff, in order to create a common understanding of the risk and a sense of shared responsibility for the necessary security measures.

### **References**

- GPR8. (2010). Chapter 2. Risk Assessment
  - EISF. (2015). Module 3. Risk Assessment Tool
  - ECHO. (2004). Section 2. Introduction to Security
5. **Organization’s Security Principles:** The following statements on principles relating to the safety and security of the organization’s staff might be included in the organization’s safety and security policies. The following list of principles is extracted from various safety and security policies of humanitarian organizations, and is not exhaustive. The organization may select and include some of these principles in its safety and security policies according to its mission, mandate and mode of operation.
- **Applicability of Safety and Security Policies:** Statement on who is covered under this policy. Are national/local staff covered? Are immediate family members of expatriate and national/local staff covered? What about local volunteers, contract staff from other NGOs, local government associates, consultants, interns, and/or guests? Since every member of the organization has a collective responsibility for their own and team security, a strong sense of ownership of the organization’s safety and security policies should be shared by every level of the organization, from the Executive Director/CEO through the Country Representative to locally hired drivers and volunteers. It is also important to remember that every member should behave as a positive representative for the organization.
  - **Responsibility for Security Management:** Statement on the operational responsibility for the security of staff <sup>7</sup> following the line management structure – overall, headquarters, regional, country and day-to-day management. (see also Standard 5: Accountability)

---

<sup>7</sup> In this guidebook, the term ‘staff’ means all the persons involved in any organization’s activities regardless of whether paid or unpaid, full-time or part-time, specialists or consultants, temporarily transferred employees, interns and volunteers.

- **Responsibility for Safety and Security Policies:** Statement on who will develop the organization’s safety and security policies, monitor implementation of policies, and give permission for exemption. (see also Standard 5: Accountability)
- **Security Risk Management (SRM) Plan:** Statement on how the SRM plan should be developed for each country/operation where the organization works. Such SRM plan should include an operational context and risk analysis (including threats and vulnerability assessment), and procedures for review and approval. (see also Standard 5: Accountability)
- **Priority of Human Life:** Statement on how the organization places higher priority on the security of personnel than the protection of assets, including premises, vehicles, office equipment or programme materials.
- **Humanitarian Principles:** Statement on the organization’s position on the core humanitarian principles of humanity, neutrality, impartiality and operational independence.<sup>8</sup> Its position on the Code of Conduct for the International Red Cross and Red Crescent Movement and Non-Governmental Organizations (NGOs) in Disaster Relief could be added as well.
- **Protection against Sexual Exploitation and Abuse:** Statement on the organization’s measures to prevent sexual exploitation and abuse of persons of concern to the organization, including implementing codes of conduct, training, complaints mechanisms and investigation.<sup>9</sup> (see also Standard 2.3: Security Plan in the Field, Guidance Note 11)
- **Proportionate Risk:** Definition of the organization’s threshold of acceptable risk to staff, assets and image of the organization, the point beyond which the risk is considered too high to continue operating. This may differ depending on the potential benefits of having a presence and a programme, and on the mandate of the organization.<sup>10</sup>
- **Individual and Organizational Responsibility:** Statement on the organization having a duty of care on safety and security for staff and others who have agreed to adhere to the safety and security policies, procedures and instructions. Furthermore, every staff and others who have agreed to adhere to the policies accept individual responsibility, on or off duty, for his/her personal security as well as the security of other colleagues, programmes and the organization. (see also Standard 1: Commitment to Safety and Security)
- **Requirement for Security Incident and Situation Reporting:** Statement on the requirement for the organization’s staff to report security incidents, including threats and near-misses, to the field office and headquarters in order to enable tracking, monitoring and analysis of security trends, and to inform security risk assessments (SRA) and decision-making.<sup>11</sup>

---

<sup>8</sup> The first three principles are endorsed in General Assembly Resolution 46/182, *Strengthening of the coordination of humanitarian emergency assistance of the United Nations*, A/RES/46/182 (19 December 1991), available from <http://undocs.org/A/RES/46/182>. The fourth principle was added in General Assembly Resolution 58/114, A/RES/58/114 (5 February 2004), available from <http://undocs.org/A/RES/58/114>.

<sup>9</sup> For more details, see CHA Alliance (n.d.). *Protection from Sexual Exploitation and Abuse (PSEA)*. Retrieved 21 March 2018 from <https://www.chsalliance.org/what-we-do/psea>; and Corinne Davey and Lucy Heaven Taylor (2017), *PSEA Implementation Quick Reference Handbook*. Retrieved 21 March 2018 from <https://www.chsalliance.org/what-we-do/psea/psea-handbook>.

<sup>10</sup> See GPR8 (2010), Chapter 2 Risk Assessment.

<sup>11</sup> See GPR8 (2010), Chapter 5 Incident Reporting and Critical Incident Management.

- **Failure to Follow Safety and Security Guidelines:** Statement on disciplinary action, including dismissal, against staff who do not follow safety and security guidelines or whose professional and personal behaviour puts themselves or others at risk while deployed in the field.
- **Local and Inclusive Security Planning:** Statement on how the country-level security planning will be conducted. It is recommended that each country office develop a local security management plan that reflects the global organizational mandate as well as the specific country mission. The plan should be flexible enough to allow local realities to be addressed, and the process should be inclusive involving national/local staff. Procedures for approval, monitoring, and review/update should be specified. All staff must be made aware of the contents, practical application and authority of the security plan. (see also Standard 2.2: Security Plan at Headquarters, Guidance Note 1)
- **Full Participation of National/Local Staff in Security Planning:** Statement on how national/local staff should be involved in the formulation, review and implementation of safety and security policies and plans. National/local staff, and local partner organizations as appropriate, should be included in security preparedness, training and human resources management procedures. (see also Guidance Note 5)
- **Coordination and Information Sharing:** Statement on the organization’s position on coordination with humanitarian and other agencies in managing security, especially on sharing security incident reports, and participation in regular mechanisms for sharing information. (see also Standard 6: Collaboration with Other Actors) Statement on a policy regarding the staff engagement to the press or government authorities including police and military. (see also Standard 2.3: Security Plan at Field Guidance Note 7)
- **Respect for Local Laws and Customs:** Statement on the organization’s position on dealing with local laws and customs, especially where local laws conflict with international law or widely held ethical standards.
- **Personal Property:** Statement on who will be responsible for the personal property of the organization’s staff under any circumstance.
- **Capacity-Building of Staff:** Statement on the organization’s commitment to ensure that all staff have the skills and capacity to analyse the security threats in their working environment and to minimise their vulnerability to these threats. (see also Standard 4: Human Resources Management)
- **Gender, Ethnicity and Nationality:** Statement on how the organization deals with different levels of risk which specific groups face in different societies as a result of their gender, ethnicity and/or nationality, and how the organization will implement alternative and/or additional measures for its staff that face particular risks. (see also Standard 4: Human Resources Management)
- **Bribes, Gratuities and Gifts:** Statement on the organization’s position on offering rewards, inducements, or bribes to local officials or others outside the organization to carry out their normal tasks or to perform illegal services; and on receiving gratuities or gifts related to their roles or the performance of their duties for the organization.
- **Kidnap and Abduction:** Statement on the organization’s response to kidnapping and abduction, position on ransoms for the release of kidnapped staff, support to

immediate family, and post-incident support to the kidnapped staff.<sup>12</sup> (see also Standard 2.3: Security Plan in the Field, Guidance Note 14)

- **Right to Withdrawal:** Statement on the right of staff (and family members) to decline to enter high-risk environments or to withdraw from such an area, irrespective of the judgement of the line manager or organization on the risk in a particular situation, without impacting employment or suffering disciplinary action, and consecutive operational and human resource review processes at both local and headquarters levels.
- **Order to Withdrawal and Return:** Statement on the organization’s right to withdraw its staff from situations that it considers to be dangerous, obligation of staff to obey such instructions, and line of authority to decide the withdrawal from and return to a programme area and country. (see also Standard 2.3: Security Plan in the Field, Guidance Note 12)
- **Evacuation:** Statement on the extent of the organization’s responsibility to evacuate its staff based on different contractual relationships – international, national and their family members. (see also Standard 2.3: Security Plan in the Field, Guidance Note 13)
- **The Use of Armed Protection:** Statement on the organization’s baseline position on the use of armed protection, and procedure for approving the use or hire of armed personnel in ad hoc and extreme situations. The statement may also cover the organization’s position on staff carrying arms while on duty and firearms in the organization’s vehicles.
- **Relationship with the Armed Forces:** Statement on the organization’s position on engagement (including information sharing) with military forces, such as national, multinational and United Nations Peacekeeping Operations. (see also Standard 6: Collaboration with Other Actors)

## **References**

- InterAction. (2015). *InterAction Minimum Operating Security Standards*
- Mercy Corps. (2010). *Field Security Manual (March 2011)*
- Concern Worldwide. (2016). *Concern’s Security Policy (March 2016)*
- Care International. (2008). *Care International Safety and Security Principles*
- Care International. (2013). *Care International Safety and Security Standards*
- Irish Aid. (2013). *Irish Aid Guidelines for NGO Professional Safety and Security Risk Management*
- People in Aid. (2008). *Policy Guide and Template: Safety and Security (Revised)*
- Lutheran World Federation. (2016). *LWF Safety and Security Policy (March 2016)*

---

<sup>12</sup> See GPR8 (2010), Chapter 14 Kidnapping and Hostage Situation.

## Reference 2-I: Sample Outline of Safety and Security Policies

### I. Introduction

- Purpose of establishing the safety and security policies
- Organization’s statement on the importance of staff safety and security
- Organization’s legal and moral obligation to manage workplace hazards and reduce the risk of harm to employees (duty of care)
- Identification of the person(s) responsible for designing and modifying the safety and security policies
- Who is covered by the safety and security policies
- Organization’s definition of safety and security

### II. Organization’s Mission and Values

- Purpose of including the organization’s mission and values in the safety and security policies
- Mission statement
- Values

### III. Organization’s Risk Management Strategies

- Organization’s definitions of three basic security approaches: acceptance, protection and deterrence
- Organization’s approach to Security Risk Management (SRM)

### IV. Organization’s Security Principles

- Explanation of the organization’s security culture, security risk attitude and the key security principles that shape the organization’s approach to staff safety and security, including brief statement on security roles, responsibilities, redress in the event of non-compliance and structures
- See 2.1. Safety and Security Policies Guidance Note 3 “Organization's Security Principles” for a list of key principles.

### V. Policy Monitoring and Review Process

- Timing and the scope of reviewing the organization’s safety and security policies
- The responsibility for initiating and conducting the review and approving the reviewed safety and security policies
- Ensuring the consultative and participatory nature of the review process

## 2.2. Security Plan at Headquarters

**Security Plan at Headquarters:** An organization is responsible for ensuring security for all the staff and all the locations of the organization as a whole. While a security plan for a field location should be tailored to the location’s specific context, a security plan at the headquarters sets out the relationship between the headquarters and field locations as well as security procedures at the headquarters.

There are organizations that do not have field locations or offices and that travel to the field when necessary. A security plan of such an organization should include both the matters described here for the headquarters and those described in ‘2.3 Security Plan in the Field’ below insofar as they are applicable to the organization.

### Key Actions:

- Clarify the relationship between the headquarters and field locations and their respective responsibilities. Such responsibilities to be clarified include security risk assessment, security planning based on the security risk assessment, daily security measures, monitoring and evaluation of project operations and security management and Critical Incident Management. Describe security risk assessment, security planning and measures and procedures to take according to the clarified responsibilities of the headquarters. (see also Guidance Note 1)
- Ensure that there are operational security procedures at the headquarters as well as those between the headquarters and field locations. These include the following: appointment, clarification of responsibilities and management of those who handle security at the headquarters (see also Standard 5: Accountability); human and financial resource management in terms of security (see also Standard 3: Resources); chain of command and communication procedures between the headquarters and field locations as well as those at the headquarters; and security procedures for staff movements between the headquarters and field locations while considering respective security plans at field locations. (see also Guidance Note 2)
- Ensure there are procedures for situation, every incident and accident reporting (subjects to be reported, chain of reporting, reporting frequency and reporting formats to be included). (see also Guidance Note 3)
- Ensure there is a Critical Incident Management Plan (CIMP) including the following: a Critical Incident Management Team (CIMT) and respective responsibilities of the Team members as well as those of other relevant staff members; procedures in responding to a crisis operating together with CIMP at field locations; a list of emergency contacts and channels to reach them within and outside business hours; procedures for contacting and maintaining communication with families of employees; procedures for media relations for risk management; procedures for controlling the use of communication tools immediately following a critical incident in particular in order to optimise the management of information to the headquarters, families and the media; and post-incident management including mental and psychosocial support. (see also Guidance Note 4)

- Conduct regular reviews of security plans as well as reviews after critical incidents with the participation of all relevant staff members and update security plans incorporating any lessons learnt.

#### **Key Indicators:**

- The security plan for headquarters specifying the above key actions is put in writing and is understood by all the staff members including headquarters and field locations.
- Regular reviews of security plans as well as reviews after critical incidents with the participation of all relevant staff members are made, and security plans are updated incorporating any lessons learnt.

#### **Guidance Notes:**

##### **1. Clarification of relationship between the headquarters and field locations with respective responsibilities. Headquarters’ actions and procedures according to its responsibilities:**

It is vital that the relationship between the headquarters and field locations is clearly defined with respective responsibilities. Confusion and conflicts of responsibilities might cause a security risk even though both sides are making efforts to respond to the original security risk. In most cases, as security risk assessment and security planning based on security risk assessment are pre-conditions for taking daily security measures and delegating responsibilities for such measures to field locations, both headquarters and field locations should cooperate with each other in making such assessment and planning. In most cases, responsibilities for daily security measures can be delegated to field locations as they have a better knowledge of the situation and so can make better decisions more quickly. On the other hand, the headquarters should be also responsible for intervening in field security measures if field locations may have made or be about to make errors or mistakes. The headquarters are usually also responsible for project operations, which itself affect security and security management at field locations, monitoring and evaluation of security and security management, as well as organizational decisions such as critical incident management, in close consultation with field locations. There are also organizations which do not have field offices or Japanese staff members based in the field. In such cases, the headquarters might be more responsible for security measures than in cases where there are field offices or Japanese staff members based in the field.

In all cases, both sides should make efforts to build confidence in each other through good communication as well as the exchange of human and financial resources.

In addition to clarifying the extent of responsibilities, it is also necessary to describe security risk assessment, security planning and measures and procedures to be taken according to the clarified responsibilities of the headquarters.

##### **2. Operational security procedures at the headquarters as well as those between the headquarters and field locations:** These procedures are necessary in order for the headquarters and field locations to fulfil respective responsibilities indicated above. They include the key actions illustrated above.

3. **Procedures for situation, incident and accident reporting (including subjects to be reported, chain of reporting, reporting frequency and reporting formats):** Information is vital in order to take necessary and appropriate security measures, and so the headquarters needs to receive information from field locations. In order to receive information of sufficient quality and quantity and to follow the situation regularly and promptly, there should be procedures (subjects to be reported, chain of reporting, reporting frequency and reporting formats to be included) on regular situation reports and incident reports to respond to a specific situation.
  
4. **Critical Incident Management Plan (CIMP):** An organization might face a serious crisis such as:
  - Death or serious injury of a staff member
  - Forceful suspension of activities
  - Security situation and disaster affecting activities
  - Major change such as relocation or evacuation
  - Communications failure
  - Major fraud
  - Compensation claim against the organization arising out of a security incident
  - Any incident which may generate media interest
  - Bomb and any other armed attack
  - Hostage taking
  - Kidnap and ransom demand

In such a situation, the headquarters must make an organizational response to the situation as indicated in the above key actions in coordination with all the relevant sections, officers and staff members at the headquarters, field locations and other offices.

### **References**

- GPR8. (2010). Chapter 5 Incident Reporting and Critical Incident Management
- ECHO. (2004). Sections 3 (Security Preparation for the Field), 8 Headquarters management of Security), and 10 (Donors); and Sections 5 (Security Incidents), 6 (Suspension, Hibernation, Relocation, Evacuation), 7 (Closing a Programme) and 9 (Learning and Training)

## Reference 2-II: Sample Outline of a Security Plan for Headquarters

### **I. Introduction**

- Purpose of establishing the security plan at headquarters
- Inclusion of the organization’s vision, mission, values, and safety and security policies in the security plan
- What is covered by the safety plan (headquarters and relationship between the headquarters and field locations)

### **II. Relationship between the headquarters and field locations with respective responsibilities. Headquarters’ actions and procedures according to its responsibilities**

- Security risk assessment
- Security planning based on security risk assessment
- Daily security measures
- Monitoring and evaluation of project operations and security management
- Critical incident management (for details, refer to V.)

### **III. Operational security procedures at the headquarters and those between the headquarters and field locations**

- Appointment, clarification of responsibilities and management of those who handle security at the headquarters
- Human and financial resource management in terms of security
- Chain of command between the headquarters and field locations as well as those at the headquarters
- Communication procedures between the headquarters and field locations as well as those at the headquarters
- Security procedures for staff movements between the headquarters and field locations while considering respective security plans at field locations

### **IV. Procedures for situation, incident and accident reporting**

- Subjects to be reported
- Chain of reporting
- Reporting frequency
- Reporting Formats

### **V. Critical Incident Management Plan (CIMP)**

- Critical Incident Management Team (CIMT) and respective responsibilities of the Team members as well as those of other relevant staff members
- Procedures in responding to a crisis operating together with CIMP’s at field locations
- List of emergency contacts and channels to reach them within and outside business hours
- Procedures for contacting and maintaining communication with families of employees
- Procedures for media relations for risk management
- procedures for controlling the use of communication tools immediately following a critical incident in particular
- Post-incident management including mental and psychosocial support

### **VI. Review and Update of Security Plan**

## 2.3. Security Plan in the Field

### Need for Individualized Security Plans in the Field

A security plan is based upon an individual organization’s safety and security policies that reflect its overall approach to security. Each organization is likely to take a different approach based upon the organization’s mission, mandate (if applicable), values, policies and programme, as well as on their understanding of the context. It is important to conduct a SRA at the planned field location and establish an appropriate security management plan when establishing the field office.

In many cases organizations do not have field offices in the countries and only travel to the field. In such cases organizations generally fulfil their SRA remotely through researching the possible security risks that their travellers may encounter and by talking to other humanitarian actors. Risk mitigating measures, CIMP, etc. are then prepared at the headquarters level. There are cases where all the above components of a security plan are addressed in a long email.

### Planning Process

The process of developing, implementing and updating a plan is as important as the plan itself. An individual should be designated responsible for leading the development of the security plan as well as for the periodic review and updating of the plan. Staff expected to implement the plan should be involved in its development. This helps to foster consistent implementation through ensuring that (1) the plan is realistic in its assumption about the situation and threats, (2) the staff understand all aspects of the plan, and (3) the plan improves staff ownership, willingness and ability to implement the plan, thereby promoting adherence to the plan. All 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.

### Context Oriented

Each organization operating in an area should develop and implement a contextual security plan specific to that operating environment. The security plan must be based on a SRA and address the identified threats. The security plan is based upon the organization’s safety and security policies, and so the security plan of each organization will differ depending on the operating environment, and on the organization’s mission, mandate and values.

### Ownership of the Plan

When implementing the security plan, each individual staff member should respect the SOPs and line management (see Guidance Note 4). If he/she no longer feels comfortable with the plan for any reason, it is his/her responsibility to bring this to the attention of the Country Representative. Individual staff members should also feel free to make observations and proposals to improve the plan. Finally, all staff should respect the confidentiality of the field security plan.

### Key Actions:

- Conduct a Security Risk Assessment (SRA) in the target area of your activities to identify any potential security risks and threats. (see also Guidance Notes 1 and 2)
- Consider any potential risk mitigating measures addressing security risks as identified in the SRA in line with safety and security policies. (see also Guidance Note 3)
- Create Standard Operating Procedures (SOPs) that provide outlines of daily operations and routines as they pertain to security including staff movement, communication, office and residence management, staff health, limitation on handling cash, implementation of CIMP and external contacts. (see also Guidance Notes 5, 6, 7, 8, 9, 10 and 11)
- Create an organization chart that describes communication and document line management at the local level and within the overall context of the organization for decisions about: shifting from one security phase to another, stopping or restarting activities/staff movement, evacuating international staff, and closing programs. (see also Guidance Notes 12 and 13)
- Create Critical Incident Management Plans (CIMP) that identify the Critical Incident Management Team (CIMT), staff members’ responsibilities and procedures in responding to a crisis including reactions to identified threats in security risk assessment, and cases of evacuation, relocation, hibernation, business continuity, medical evacuation (Medevac) and death of staff (national/local and international), in close liaison with headquarters. (see also Guidance Notes 3, 14 and 15)
- Describe guidance for staff’s stress management including Rest and Recreation (R&R). (see also Standard 4: Human Resources Management)
- Establish an incident and situation reporting system along with the formats of those types of reporting including close liaison with headquarters.
- Conduct regular reviews of plans as well as reviews after critical incidents with the participation of all relevant staff members.

#### **Key Indicators:**

- The security plan for field posts specifying the above key actions is put in writing and is understood by all the staff members including headquarters and field locations.
- Regular reviews of plans as well as reviews after critical incidents with the participation of all relevant staff members are made.

#### **Guidance Notes:**

1. **Security Risk Assessment (SRA):** Organizations normally carry out a SRA before a final decision is taken to deploy a team to the field. The aim of the SRA is to understand the situation sufficiently to enable the operating team to plan their security measures appropriately. This assessment covers a wide range of security related factors such as both general and specific potential threats to aid organizations, the vulnerability of the organization, and mitigation measures. It is better to visit the field for long enough to achieve the aim, but the assessment can be done remotely if it is not possible to visit. A SRA can be done solely or jointly with other organizations, and combined with other aims, for example, a needs assessment. For more details, see GPR8 (2010) Chapter 2 (Risk Assessment) and ECHO (2004) A26 Security Assessment. (see also Standard 6: Collaboration with Other Actors)

2. **Information Gathering:** The gathering of security and safety related information is important for a successful SRA as well as to build one’s own security network after starting activities. Embassies and foreign governmental agencies provide security notices and host governments also share important security matters and other contextual backgrounds. For example, many U.S. and British embassies provide security related information on their websites. Meanwhile, the Japanese government, in addition to providing security information for travellers on its website, allows anyone to register with Tabi-Regi to receive security notices from the local embassy. In many countries, humanitarian and development actors including NGOs, the UN and bilateral agencies have mechanisms for sharing security information including incidents that have occurred in past projects. Apart from the government and NGOs, there are security consulting organizations for humanitarians such as RedR and Safer Edge, as well as security firms which provide security services including guards, vehicle escort and consulting services. Some insurance firms offer consulting services on security risks and threat information in some areas of the world. In addition to continuous efforts to collect information from international and national media, it is recommended to gather information from the local government and local community in the area of activity. It is important to note that organizations should utilize various information resources and contact channels to collect enough information to make appropriate decisions on the security situation. For more details on security networks, see Standard 6: Collaboration with Other Actors.
3. **Mitigation Measures:** A mitigation measure means to consider what can be done to reduce risks to an acceptable level. In general terms, there are three possible courses of action: (1) Reduce the threat. If feasible, reach out to or have others negotiate on your behalf with potential adversaries; (2) reduce the consequences and lessen the impact of the threat. These might usefully be termed ‘contingency measures’, such as first-aid protocols, crisis response procedures and in extremis pre-emptive evacuation and guidance on how to behave in the event of a serious incident; (3) Reduce or eliminate exposure by adopting additional protective measures or changing locations, for instance. The extreme version of this would be ‘risk avoidance’, i.e. removing the organization entirely from the threat, either permanently or temporarily. It is also important to note that there may be unique security risks for national/local staff and female staff, and to prepare appropriate mitigation measures (see also Standard 4: Human Resources Management). For more details, see GPR8 (2010) Chapter 2.7 (Risk Analysis) on mitigation measures, Standard 4: Human Resources Management on considerations for national/local and female staff, and Standard 7: Safety and Security of Local Partner Organizations on the involvement of local partner organizations.
4. **Critical Incident Management Plan (CIMP) and Critical Incident Management Team (CIMT):** In order to respond to a critical incident an organization should develop both a CIMP and a CIMT. The CIMP should take into consideration possible critical incidents such as evacuation, relocation, hibernation, business continuity, medical evacuation (Medevac) and death of staff (national and international), and clarify the response processes. The CIMT should establish hierarchical responsibilities and draw a clear distinction between the roles played at the country office level, the regional office and global headquarters. Everyone needs to understand where they fit in. For some incidents,

a CIMT may operate only at the field level, but there needs to be a clear understanding of when to bring in the headquarters as necessary. Serious or prolonged incidents (an assassination, bomb attack, kidnapping, hostage situation or forced hibernation) or major changes such as a relocation or evacuation will typically require a dedicated CIMT. The CIMT’s decisions include suspension of activities, personnel withdrawal, setting of a certain level of confidentiality, and the end-state objective (injured person evacuated, body repatriated, kidnapped staff member released). CIMT members consist of representatives of the organization, managers, and communicators at both the headquarters and field level. Communication with authorities, media, donors, and family of staff is important, and the CIMT must also include administrative, legal and financial considerations especially for the people affected by an incident who need appropriate psychological support. After an incident, the staff members involved should undergo debriefing and counselling if necessary. An after-action review should be standard practice. For more details, see GPR8 (2010) Chapter 5 (Incident Reporting and Critical Incident Management).

5. **Standard Operating Procedures (SOPs):** Safety and security plans should clearly outline the various SOPs. SOPs are designed to ensure that safety and security best practices are maintained on a day-to-day basis and should set out clear parameters for staff (basically the ‘dos and don’ts’) which, if followed, will help staff to prevent or minimise safety and security risks in that particular location. SOPs might be called “operation manuals” or “guidelines” depending on the organization. SOPs can cover a wide variety of issues, such as: personal security; local laws and customs; site security and safety; staff travel and movements; vehicle safety; communications; staff health and welfare; financial management; reporting incidents; and managing information.
6. **Communication:** Communications equipment helps strengthen security if used properly. The leader of a field team should ensure that the team’s communications requirements are thought through in good time to allow the despatch of any vital equipment with the team as it deploys. It is good practice, in insecure situations, for staff to have two independent means of communication (e.g. radio and satellite phone), so that if one breaks down communication will still be possible. In particular, avoid dependency on mobile phones. In a crisis a cellular telephone system is particularly vulnerable to becoming overloaded, damaged, or simply switched off by a belligerent. No communications system is fully secure. All staff should be aware of the need for information security, and the risks that can arise from interception of communications.
7. **Media:** The media can have an impact on the security management of the organization and its staff. Contact between your organization and the media should ideally be channelled through senior management or the media response office. As well as gathering information from aid agencies, the media often like to interview staff directly in the field. Responding to media interviews requires a certain set of skills (answering sensitive questions under pressure, providing contextual and correct information, etc.), and therefore they should normally be handled by staff experienced at being interviewed. After a security incident, the organization should disseminate accurate reports and appropriate responses through the media in order to avoid the spread of biased information and exaggerated rumours. The organization’s managers should therefore be

aware of media reporting, and able to deal with the media effectively when appropriate. It is essential to provide media training.

8. **Travel and Movement Security:** In many field operations, the greatest security risks to staff occur during routine travel and movements, either while travelling in the field or moving to and from the office (this applies to both humanitarian and development agencies). Vehicle accidents, ambushes, shootings, carjacking, abductions, landmine incidents and other incidents while on the road account for the majority of safety and security incidents affecting aid workers. In insecure environments, vehicles are an essential tool for avoiding potential danger. However, in some situations they can actually be the cause of insecurity. An aid organization’s vehicle and its occupants can be an easily identifiable target for those who want to vent their anger against a particular organization, or against humanitarian organizations in general. The new and expensive vehicles often used by organizations can also make them an ideal target for criminal groups. All the organization’s vehicles, including rental vehicles, should be equipped with the appropriate safety equipment (first aid kits, fire extinguishers, seat belts, etc.). Many organizations set up guidelines for visitors to determine whether in-country visits are appropriate and if so, the travel criteria and appropriate locations for visitor accommodation.
9. **Site Security:** Organizations should determine the locations for offices, as well as hotels/guest houses for temporary lodging of staff visitors with appropriate safety and security equipment prior to project implementation. Site management includes: physical conditions and strength of the building; examination of the boundaries of the site to make sure that perimeter walls are secure; ensuring that all doors, gates and windows have adequate locks; ensuring that access points and the street area outside are well lit; considering possible escape routes; and considering vehicle parking and assembly areas. The office also should have effective controls and procedures in place to manage access. For field offices in high-risk environments, a guard force should be employed, either through direct hire or by using the services of a reputable contractor.
10. **Financial/Cash Security:** The management of financial/cash security is one of the critical issues in field operations, particularly in insecure environments, and operational managers should be familiar with financial procedures. It is also important to provide financial training for the staff to be deployed. Good financial management is a major subject, beyond the scope of this Guide. Detailed advice on financial procedures, including simple guides to NGO accounting, can be found at [www.mango.org.uk](http://www.mango.org.uk). Cash storage, management, transfer, and distribution are significant points of vulnerability for a field office. Cash management and transfer are security issues, with related standards, policies, and guidelines that must be implemented and adhered to at all times. Every office in a country must decide on a safe location for cash reserves (including a reserve for emergency evacuation) and a reliable way to receive funds. A field office should consult with the financial and legal officers and advisors of local partner organizations regarding what banks, if any, are used and for what purposes. The Country Office also should assess the cash management possibilities in the area, such as the reliability and cash-withdrawal limitations of local banks or the availability of electronic payment to local businesses.

11. **Sexual Aggression:** In any area, sexual harassment and assault are incompatible with providing a safe and secure working environment and are unacceptable. Sexual aggression can be directed at men or women, but women are most often the targets. Staff members should be aware that everyone is a potential victim of sexual assault and sexual assault is the most under-reported violent crime. Each organization should clearly set Sexual Harassment Guidelines and ensure that all staff know and comply with them. Organizations will investigate all sexual harassment complaints in accordance with their policies and procedures. Female staff should receive a briefing on sexual aggression immediately upon hire. If there are security concerns for female staff, organizations should consider upgrading the accommodation or arranging a shared house for female staff members, taking into consideration the local culture and security environment.
12. **Medical Evacuation (Medevac):** If a staff member is injured or falls ill and local medical facilities cannot provide sufficient treatment, Medevac may be needed. This normally happens only when a doctor advises that it is necessary. Many humanitarian organizations insure against the costs of Medevac, and have arrangements with specialist Medevac companies. If so, it is vital that all relevant staff know the procedure for making use of these. See GPR8 (2010) A20 (Medical Evacuation) for a suggested Medevac procedure.
13. **Suspension or Hibernation of Project, Relocation or Reduction of Staff:** Suspension or hibernation of a project, and relocation or reduction of staff have recently been used as measures to mitigate the security risk in insecure environments. Such action may be necessary in order to allow time for reflection on a changed security situation. It may also be used to send a signal to local authorities or to other groups that threats to humanitarian organizations are not acceptable. Suspension is likely to be more effective if carried out by all humanitarian organizations at the same time, and for the same stated reasons. Suspension may be announced in the media. Alternatively it may be unannounced, depending on the circumstances, the threats, and on the purpose of the suspension. It is advisable to discuss the possible options for suspension with donors during the project design phase, so that funding problems are minimised if such action becomes necessary. A longer period of suspension, where staff remain at home or in a safe place for a considerable time in order to allow danger to subside, is sometimes known as hibernation. Ensure that sufficient resources (water, food, essential goods, fuel, etc.) are available for the duration of the hibernation period. An alternative to suspension or hibernation is to relocate staff to a safer location, without leaving the country. A further alternative is to reduce the number of staff working, so as to reduce the security risk.
14. **Evacuation Plan:** Evacuation is conceived as the ultimate step in a gradual reduction of exposure – from suspension of movements of certain types of staff, to suspension of operations, to partial withdrawal of staff from a site, to total withdrawal and the closure of activities. It is absolutely imperative to consider and establish the evacuation plan beforehand, especially in high-risk environments. Bear in mind, however, that events can overtake plans. Planning through security phases, although useful, can give the impression of a linear progression, when this may not always be the case. In many

situations, evacuation routes are blocked, the logistical capacity for evacuation is insufficient, or it simply becomes too dangerous to try to evacuate and staff have to stay put and weather the crisis. Security plan should be an over-arching document which includes relocation plan, hibernation plan and evacuation plan etc., thus, evacuation plan should not be considered as separated while it is one of the most important parts of security plan. Relocation and especially evacuation are difficult decisions – not just from a programmatic but also from an ethical point of view. It needs to be clear not only under what conditions an organization will evacuate or relocate, but also who has the ultimate authority to make that decision: headquarters or field representative? Can regional offices make decisions by themselves? Who has the authority after withdrawal? Is it clear to all staff that the decisions taken by management are mandatory? It is important to include evacuation in the organization’s safety and security policies and plans. As far as possible, the rights and responsibilities of employers and employees should be laid down in employment contracts or in the safety and security policies. For international staff, it should be considered with the organization’s human resources management. It is encouraged to consult beforehand regarding measures related to evacuation with national/local staff and local partner organizations. The evacuation/relocation plan should be regularly reviewed and discussed with staff, especially if it is becoming increasingly likely that a withdrawal will be necessary. This can be carried out through simulation exercises or a simple team meeting to review policies, procedures and plans. In the height of a crisis, individual staff may be tempted to take all sorts of unplanned steps and go to places other than the planned assembly points. The effect is likely to increase confusion, delay the evacuation and heighten the risk for everybody. No individual initiatives that deviate from the plan should be taken without prior authorization by the head of the CIMT. Key considerations are: feasible transportation under difficult scenarios; utilising mitigation measures to reduce risks; availability of transport for how many; and who can provide means of transport and other requirements including a charter plane in the absence of pre-agreement. Many evacuations and relocations depend upon collaboration between different organizations. Do not draw up a plan in isolation. While it is usually safer to travel in a vehicle convoy with other NGOs, this also means less control over how the evacuation is carried out. Discuss with other agencies beforehand, if possible, how these issues will be handled.

15. **Kidnapping/Hostage Incident:** Kidnapping refers to forced capture and detention with the explicit purpose of obtaining something in return for the captive’s release. The objective and hence the motive for kidnapping vary: often it is money, though kidnappers may also demand political concessions. In other cases, what may ostensibly be a political cause may in fact be little more than an extortion racket. Globally, kidnapping has become increasingly common in recent years, including in the aid world. High-risk countries include Yemen, Iraq, Syria, Somalia, Darfur (Sudan), Afghanistan, Pakistan and the Philippines (Mindanao). Kidnapping can be hard to prevent, at least against a well-organized and determined group of perpetrators, and can be a very effective way of raising funds or increasing political visibility. It is therefore a very serious threat. Key actions for reducing risks of kidnappings are: avoiding routines; reducing visibility; in-country vetting of personnel; removing potential vulnerabilities; site protection; heightened awareness and counter-surveillance; seeking local support protection; armed protection; etc. The organization’s attitude toward ransom (whether to pay or not)

should be set in its safety and security policies. Personal security training covers kidnapping situations. Generally speaking, kidnapping situations cannot be dealt with only at field level, but must involve the organization’s headquarters and regional offices. A kidnapping is a very complex and challenging situation, and inevitably requires the involvement of a wide range of people and organizations, including law enforcement, government agencies, the media and insurance companies, and the victim’s family. Critical incident management capabilities will be required, including training, planning, preparedness exercises and the proper allocation of resources (financial, human, equipment, etc.). It is essential that NGOs make themselves aware of the resources available e.g. hostage negotiators who will have to be called upon by NGO HQs at a very early stage. Time will not be available to research this once a hostage incident is underway.

### **Column 1: Low-Profile Approach**

Low-visibility programming has become an increasingly common protective tactic among aid organizations in high risk environments. It involves removing organizational branding from office buildings, vehicles, residences and individual staff members. It can also involve the use of private cars or taxis, particularly vehicles that blend into the local context, limiting movement and removing tell-tale pieces of equipment, such as Very High Frequency (VHF) radios or satellite phones and HF antennas. In certain very high-risk environments, anything that might link staff to an organization – memory sticks, organization identity documents, cell phones, and computers – may be ‘sanitised’. Staff likely to stand out from the local population may be redeployed. In Iraq, more radical steps have included staff using false names, working with no fixed operating address and not being told the identities of colleagues. Beneficiaries were purposefully not made aware of the source of their assistance. Another tactic of a low-visibility approach is to use removable (e.g. magnetic) logos for vehicles, which can be removed in areas where visibility is discouraged. Knowing when to display a logo and when to take it off demands a very good, localised and dynamic risk assessment. A low-profile, low-visibility approach poses significant challenges. It can make programming more complicated, particularly in extreme cases, and can distance the organization from sources of information that might otherwise enhance its security. It might also lead to suspicions and misperceptions of what the organization is doing, undermining acceptance.

### **Column 2: Use of Armoured Vehicles**

Whether or not aid agencies should use armoured vehicles in environments requiring high security has long been debated due to organizations having different approaches to security concerns. The Generic Security Guide, produced by the Directorate-General for European Civil Protection and Humanitarian Aid Operation (ECHO) under the European Commission, suggests that armoured vehicles should be used in extreme cases by some humanitarian organizations. “They are expensive, heavy and require special training to drive. Most civilian armoured vehicles provide protection against only a limited range of threats. In most cases such vehicles are not necessary, and if they are necessary it may be best not to work in that area at all. Seek experienced advice before deciding to procure them.” It is better to carefully consider when to use them, for what purpose and for how long. See also, ECHO (2004) Section 4.10 (b) Vehicles.

## Reference 2-III: Sample Outline of a Security Plan for Field Posts

### 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 the organization’s mission, mandate, principles and safety and security policies
- Summary of the situation (political, economic, historical, military, etc.)

### III. Security Risk Assessment (SRA)

- The current security levels in country.
- Threat assessment (indicating most likely types of threats NGOs will face)
- Mitigation measures (list the necessary responses to reduce risks)
- Risk analysis (identify impacts, likelihood, and mitigation measures and risk threshold)

### IV. Standard Operating Procedures (SOPs)

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.)

### V. Critical Incident Management Plan (CIMP)

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

- Evacuation
- Medical evacuation (Medevac)
- Death of staff
- Other high risk, foreseeable events
- Critical Incident Management Team (CIMT)

### VI. Supporting Information

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

### Standard 3: Resources

*Signatories shall make available the appropriate financial, human and other resources to mitigate the safety and security risks identified through the organization’s security risk analysis.*

#### Key Actions:

- Maintain a clear guideline for budget planning to cover appropriate safety and security expenses to meet the requirement of the Standards. The budget design should include expenses for line items, personnel, project cycle design, administrative/overhead costs and budget for local partner organizations when necessary. (see also Guidance Notes 2 and 3)
- Revise the original project plan and avoid imposing intolerable risks and overcapacity on staff members, in case sufficient resources are not available for appropriate safety and security management. (see also Guidance Note 4)
- If appropriate expenses are not covered by a donor, work as a member of NGO community or collaborate with other NGOs to change the donor policy to include funding on safety and security measures. (see also Guidance Note 4)

#### Key Indicators:

- Organizations have a procedure to share the results of security risk analysis with all relevant sections/persons in charge of budget planning.
- Organizations allocate sufficient budget for staffing in terms of number, salary with benefits and working environment, including that for local partner organizations.
- Organizations secure expenses for project cycle design such as research/needs assessment, local stakeholder engagement<sup>13</sup>, networking with other humanitarian and development actors and monitoring/evaluation.
- Organizations secure sufficient resources, in case of remote management of a project, to hold appropriate communication with partner organizations (i.e. meeting in a third country or in Japan) and to conduct proper monitoring and evaluation. (Refer to Standard 7 for guidance)
- Organizations secure sufficient financial and human resources for internal and external security training and human development, including that for local partner organizations.
- Organizations adopt an open policy for sharing security costs with other NGOs to pursue scale merit and cost effectiveness, i.e. security advisors, offices, special types of vehicle, evacuation, etc.
- Organizations work with NGO networks for donor advocacy if they face rejection of a funding request for appropriate security related expenses by a donor

---

<sup>13</sup> Stakeholders for project implementation by NGOs may include local authorities, non-state actors, local leaders, local communities, local NGOs, local partners/staff, international NGOs, the UN and governmental organizations.

## Guidance Notes:

1. **Resources to Meet the Standards - A Challenge for Japanese NGOs:** Based on the security risk analysis, organizations inevitably need to take some mitigation measures and this in turn requires appropriate financial, human and other resources. However, this Standard may be one of the greatest challenges for Japanese NGOs in comparison with those of the U.S. and Europe, and some deliberate and innovative approaches by the NGO community are expected to fill the gap between the supply and demand of resources.
2. **Budget Planning Policy:** Budget planning based on proper security risk analysis is a crucial part of security management in forming a project. As security management involves human resources management and collaboration with other humanitarian and development actors, the planning requires not only expenses for facilities and equipment but also other resources like personnel as well as stakeholder engagement to fulfil all the safety and security standards.
  - In some organizations, budgets are planned independently by persons in the administration or finance section and thus security measures to be taken both at the headquarters and field levels may not be properly reflected in the budget. To avoid such practice, organizations should have procedures in place for sharing the results of security risk analyses with all relevant persons and sections or should conduct an analysis involving all persons and sections concerned with budget planning.
  - The cost for research, assessment and stakeholder engagement including the local community is essential for NGO security in terms of “acceptance” strategy. Thus, resources should be planned in advance when forming a project.
  - Resources for collaborating with other humanitarian and development actors need to be put aside as administrative/overhead costs, which are essential for security information sharing, training and coordination.
  - When implementing projects with local partner organizations, the organizations should analyse security risks specific to the local partner organizations, and secure the resources required to take necessary security measures.
3. **Budget Designing:** For NGOs that utilize government or UN funding, some security related costs can be included in line items such as office security, proper transportation, communication means, insurance and security related personnel. Notwithstanding, other expenses like research, assessment, training, stakeholder engagement, and participation in humanitarian and development security networks should be included in budget designing as administrative/overhead costs.
  - Information on supporting programs for external security training is given in attached Reference 3-I.
  - Organizations should share information with the NGO community on line item coverage of safety and security related expenses by donors to set standard practices for the NGO community and donors. Security related expenses that can be included in line items by major Japanese donors are given in attached Reference 3-II.
  - Cost sharing with other NGOs is one way of reducing security expenses. Costs can be shared by joining an existing security network of NGOs active in the field or by forming

an ad hoc consortium in response to particular crises. Examples of expenses include: security related personnel, office or communication means, special type of transportation, evacuation means including insurance, security information, etc.

4. **Revision of the Project and Advocacy by the NGO Community:** If organizations find it difficult to mobilize sufficient resources to take required security measures, they should revise the security plan as well as project plan itself. If the difficulty is mainly on account of the donor policy of funding for security expenses, organizations should express opinions as a NGO community member to raise awareness and change the policy of donors. (see also Standard 6: Collaboration with Other Actors)
- Organizations need to be aware that project implementation without sufficient resources for safety and security can pose intolerable risks and overcapacity on their staff members.
  - Organizations should work on or collaborate with a NGO community for advocacy for donors that the costs of security measures should include personnel expenses with proper working conditions, training as well as stakeholder engagement and networking.
  - When Japanese donors cannot approve some appropriate expenses for safety and security, organizations can work with network NGOs in Japan working for advocacy including JaNISS.

### Reference 3-I: Support Program for External Security Training

#### 1. UNHCR Regional Centre for Emergency Preparedness (eCentre)

- eCentre annually hosts a SRM and Safety in the Field workshop once or twice in Thailand, along with various other workshops.
- Currently in 2017, eCentre has hosted a SRM, and training of trainers for SRM and SIF in Japan.
- All costs for training, travel and accommodation are covered by eCentre.
- As eCentre’s mission is capacity-building for emergency preparedness of the UN, G.O. and NGO personnel in the Asian Pacific region, participants should be stationed in the region in principle. Usually, two or three seats are allocated to Japanese NGOs for each workshop and participants are selected from a long list of applicants. However, applicants stationed outside of the Asian Pacific region are sometimes accepted as substitutes to fill vacancies.
- Workshop information can be obtained from UNHCR’s Tokyo Office as well as the website of JaNISS.

#### 2. NGO Overseas Study Program of the Ministry of Foreign Affairs of Japan (MOFA)

- This program is offered by the NGO division of the Ministry of Foreign Affairs (MOFA) to help NGOs send their staff members overseas to receive training for the capacity-building and human resource development of Japanese NGOs. MOFA entrusts the secretariat of the program to a third party (it is JANIC in 2017), and announces the call for proposals usually two or three times each fiscal year.

- Though its guideline states that the duration of training should be more than one month, security training for shorter periods has been approved in practice, such as one-week security training by European and U.S. training providers.
- The cost for training, travel and accommodation will be covered by the program (each line item has a maximum limit).
- Information can be obtained on the website of MOFA.

### **3. Japan NGO Initiative for Safety and Security (JaNISS)**

- JaNISS hosts SRMs and PSFs in Japan and overseas on an ad hoc basis.
- In principle, participants are supposed to cover a part of the training cost. Travel and accommodation costs may be covered by JaNISS depending on the funding situation.
- Information can be obtained on the website of JaNISS.

### **4. Japan Platform (JPF)**

- Depending on the programme, external training cost can be included in a line item of a project budget, if its necessity is approved by the secretariat.
- When approved, the external training cost for both international and national/local staff members as well as those of partner organizations can be covered.
- For staff members at the headquarters level, the training cost will be approved when the necessity of the training, such as for travel to the field, is acknowledged.
- When appropriate training is not available in the country where an office is located, travel to and training in a third country is approved.

## **Reference 3-II. Security Expenses that Can Be Included in Budget Supported by Japanese Donors**

### **A. Japan Platform (Based on the guideline for project implementation and subsidy revised on March 17<sup>th</sup> 2017)**

- Insurance: War-premium insurance can be included in “insurance expense” and insurance for evacuation in “security and labour safety expenses”.
- Visa: The visa issuance fee for a third country for evacuation can be included in “visa expense”.
- Office facility: Security related office facility cost can be included in “field post set-up expenses” or “security and labour safety expenses”.
- Office equipment: Security related equipment can be included in “security and labour safety expenses”.
- Vehicle: Security related vehicle cost can be included in “local transportation expense”.
- Communication: Communication equipment necessary for security management can be included in “field office admin equipment and supply expenses” and communication cost in “communication and bank transfer expenses”.
- Personnel: Both for international and national/local staff, all personnel costs including the part of legally regulated welfare benefits covered by the employer can be included in personnel expenses, under the limit of the JPF personnel expense standard. Personnel costs for security managers and security officers can also be included.

- Security training expenses: In some programs, security training expenses can be included in the budget. (refer to Article 4. of Reference 3-II above)
- Expense for travel to headquarters during the project period and R&R: It can be included in “travel expense”.
- Guard and other security related expenses: Guard and other security related expenses can be included in “security and labour safety expenses”.
- General administrative expenses: As general administrative expenses, 5% of field expenditure can be allocated but documented evidence must be submitted.

**B. Grant Assistance for Japanese NGO Projects (N-Ren, based on guideline for fiscal year 2017)**

- Insurance: War-premium insurance or insurance for evacuation can be included in “expenses for other security measures”.
- Visa: The visa issuance fee for a third country for evacuation can be included in “expenses for other security measures”.
- Office facility: Security related facility cost can be included in “expenses for other security measures”.
- Office equipment: Security related equipment can be included in “office supply expense” or “expenses for other security measures”.
- Vehicle: Security related vehicle cost can be included in “vehicle procurement/lease expenses” or “expenses for other security measures”.
- Communication: Communication equipment related to security can be included in “Office equipment procurement/lease expenses” or “expenses for other security measures” and communication cost in “communication expense”.
- Personnel: For international staff, basic salary with some allowances including that for managerial positions can be included. However, the part of legally regulated welfare benefits covered by the employer and other allowances including those for over-time or accommodation can NOT be included. For national/local staff, only basic salary and legally regulated social benefits including the part covered by the employer can be included. They can be approved within the limitation rate for MOFA’s standard both for international and local staff. The salary for paid holidays can NOT be included for either international or local staff.
- Expense for travel to headquarters during the project period and rest and recreation (R&R): The expense for travel between the field and headquarters can be approved for only one time at the beginning and end of a project period. In principle, the expense for travel to headquarters for meetings and rest during the project period, as well as R&R in a third country, cannot be approved.
- Security training: Security training expenses cannot be included. However, for the security training and exercises provided by the Japan International Cooperation Agency (JICA), the travel expenses to the venue(s) can be included both in Japan and in a country of activities, only for one person of Japanese nationality, once in one project, if the person has not participated in the training before.
- Guard and other security measure expenses: Guard and other security related expenses can be included in “expenses for other security measures”.

- General administrative expenses: As general administrative expenses, 5% of field expenditure can be allocated but documented evidence must be submitted. Direct costs for the project can NOT be included here.

## Standard 4: Human Resources Management

*Signatories shall have personnel guidelines and procedures that prepare employees to cope with safety and security issues at their post of assignment, support them during their service, and address post assignment issues.*

Organizations should work on hiring and retaining qualified staff and demonstrate their duty of care to staff, through proper orientation, training, insurance and support. Organizations shall have policies and procedures in place that include national/local staff in the security risk management systems and that address the unique security concerns of national/local staff.

### Key Actions:

- Ensure there are human resource rules that include clear Terms of Reference (TOR) and responsibilities for all positions, and that all positions are responsible for security management. (Guidance Notes 1, 3, 9)
- Ensure there are policies for safety and security which include stress management, training on security issues and first aid, insurance, and the well-being of both international and national/local staff. (Guidance Notes 2, 7, 8, 11)
- Pay special attention to the unique issues of international staff, who can be exposed to external threats as well as stress and sickness. (Guidance Notes 4, 5, 6)
- Pay special attention to the unique issues faced by national/local staff which are often different from those faced by international staff, and ensure that policies and plans for safety and security are translated into the local language. (Guidance Notes 4, 5, 6, 10)

### Key Indicators:

- Staff have access to: written policies on safety and security, individual health, care and support; ToR explicitly stating responsibilities; and programme plans including a written assessment of security, travel and health risks specific to the country or region.
- The above-mentioned policies are reviewed on a regular basis.
- All levels of staff are trained on: assessing threats to the organization; awareness of world trends affecting the security of humanitarian and development organizations; handling of media and caring for family during security incidents; and personal security management in the field.

### Guidance Notes:

1. **Pre-assignment briefing:** Before an international assignment, organizations are responsible for ensuring that all staff receive verbal and written briefings on all risks relevant to the role to be undertaken, and that measures are in place to mitigate those risks, including insurance. It is important that the chain of command regarding security is clear for all staff so that communication between the headquarters and field office flows smoothly. See CHS for more details of the general aspects of human resources management. (also see Standard 1: Guidance note 7)

2. **Stress Management:** Managing stress is the responsibility of not only the individual but also the organization. Organizations should be aware that more staff experience stress than security threats, and that stress affects their performance, motivation, and also their turnover. Staff often work long hours in risky and stressful conditions. An organization’s duty of care to its workers includes actions to promote well-being and avoid long-term exhaustion, burnout, injury or illness. When the organization deploys staff to a high-pressure area, they are required to receive regular ‘rest and recreation (R&R)’ to help prevent stress and illness and to improve efficiency. Post-deployment support including PTSD response is also required if necessary. Speaking about managing stress may be received differently in some cultures, and organizations should be aware that national/local staff may have a different attitude towards stress.
3. **Roles of Managers:** Managers must make aid workers aware of the risks and protect them from exposure to unnecessary threats to their physical and emotional health. Measures that can be adopted include effective security management, preventive health advice, active support to work reasonable hours and access to psychological support when required. Managers can promote a duty of care by demonstrating good practices and personally complying with policy. Aid workers also need to take personal responsibility for managing their own well-being. Psychosocial support should be immediately available to workers who have experienced or witnessed extremely distressing events.
4. **Special attention to female staff:** Be aware that female staff may have greater threats and risks than male staff and may need special attention and support. Female staff tend to be more aware of their particular vulnerabilities, especially to sexual aggression. It is also important to remember that male staff can also be victims of sexual assault. (see also Sexual Assault in Standard 2)
5. **Family care:** The organization’s security policy and plan should include care and support for staff’s families during critical incidents.
6. **Relocation and Evacuation:** Staff policy regarding relocation and evacuation is clearly communicated to all staff in advance. International staff need to understand that they must follow the decision of the organization to evacuate, while individual staff members have the right to request to withdraw from risky areas when they feel insecure. Should international staff refuse or decline to be evacuated they should be informed that they will no longer be covered by insurance and will be separated from the organisation. It is good practice to discuss with national/local staff what their intentions would be in the event of their being relocated within the country during the periods of emergency. Would they wish to remain or relocated? Those remaining could be utilised to implement the continuity of operations when the international staff evacuated. It is better to do this during a period of calm rather than when the emergency is imminent.
7. **Providing Security Risk Management (SRM) training opportunities:** Security training should be provided which is relevant to the security responsibilities described in the employee’s job description and any reasonably anticipated responsibilities that individuals may be expected to assume. It is also important to learn from other agencies

and networks, as well as to utilise experienced staff as trainers, briefers, advisers, and evaluators.(see also Standard 3: Resources, Reference 3-1)

8. **Insurance:** All staff are covered by appropriate insurance, and war risk coverage when assigned to high-risk countries. The insurance for compensation liability and emergency evacuation are also available, but the cost of these insurance services is tend to be expensive. The organization may buy these insurance through consortium of NGOs or network organization. For staff members employed in Japan, the Act on Industrial Accident Compensation Insurance regulates that an employer should enrol its employees in this insurance to compensate for injury, disease, disability and death during work and commuting. Organizations must be aware that for accidents that occur while an employee is deployed and stationed at a field office (not just for travel), prior procedures for special enrolment in insurance coverage are necessary (For more details, refer to the website of the Ministry of Health, Labour and Welfare). National/local staff require appropriate insurance cover that does not exclude relevant risks. Failure to maintain adequate insurance could lead to large claims made against an employer, which in some cases could drive the employer into bankruptcy. Lawsuits are possible even if there is adequate insurance, if the organization has been negligent.
9. **Staff recruitment:** Recruiting the right national/local staff is crucial when an organization is new to an environment and needs to respond urgently to an emergency. Professional references should be consulted, and when in a new environment and in a hurry, short-term contracts may be appropriate.
10. **Special care for national/local staff:** It is mandatory that national/local staff are involved in formulating, reviewing and implementing security and safety policies and plans, to make sure that their culture is considered. National/local staff should be given an explanation of the organization’s rules and regulations on human resources in their own language(s). Their TORs, evacuation plans and crisis management should also be explained. The recruitment and assignment of staff requires consideration of a well-balanced team, with respect for local culture and customs. National/local staff, on the one hand, have a better understanding of the social, cultural and political environment in the field and better access to local networks which help them to gather information from the local context, but on the other hand, they may face various pressures from other actors in society that should also be taken account of.
11. **First Aid Training:** In addition to security trainings, all staff should be actively encouraged to undergo first aid training commensurate with operating in remote and possibly hostile environments.

### **References**

- CHS Alliance, Group URD and the Sphere Project. (2014). *Core Humanitarian Standard on Quality and Accountability*, Commitment 8.
- People in Aid. (2003). *Code of Good Practice in the Management and Support of Aid Personnel*, Principle Seven (Health, Safety and Security)
- ECHO. (2004). A25 (Rest and Recreation) and A35 (Stress)

- GPR8. (2010). Chapter 4 (Evacuation, Hibernation, Remote Management Programming and Return), Chapter 6 (People in Security Management), and Annex 5 (Insurance).

## Standard 5: Accountability

*Signatories shall incorporate management systems that will ensure accountability for safety and security at both headquarters and field levels, and all personnel understand their respective roles and responsibilities.*

Setting standards for security and safety will be more likely to be sustained if there is a good structure of accountability in place with clear lines of responsibility for each of them, and a process by which people are held accountable for these responsibilities. Those with responsibilities must have proportionate authorities. An effective security management structure will foster a positive security culture and help the organization to fulfil its duty of care obligations.

### Key Actions:

- Create a structure of accountability based on the organization’s safety and security policies and plans (see also Standard 2) both at field and headquarter levels, regardless of the size of the organization. (see also Guidance Note 1)
- Define the security responsibilities and specific decision-making roles of each of these positions in respective staff members’ job descriptions. (see also Guidance Note 1)
- Identify an individual or a group of staff within the organization who can act as a security focal point and/or working group in order to take the lead in developing and implementing the security management framework. (see also Guidance Note 1)
- Organize briefing and induction sessions on the organization's mission and values, security roles and responsibilities for staff members at all levels, both at the field and headquarters. (see also Guidance Note 2)
- Conduct a periodic organizational security review including evaluations of both employees and the management. (see also Guidance Note 3)
- Establish procedures to address non-compliance and violations of safety and security policies and procedures, and make them known to staff members at all levels. (see also Guidance Note 3)

### Key Indicators:

- Reporting lines for authority and decision-making are clearly established and staff understand to whom they are accountable.
- All staff with security responsibilities have their duties clearly articulated in their job descriptions.
- Staff at all levels within the organization, from the governing bodies to individual staff members, share a collective responsibility for safety and security.
- A security focal point and/or working group is in place and functional.
- Security roles and responsibilities are incorporated into the organization’s performance reviews.
- Staff members comply with the organization’s safety and security policies and plan, and their procedures.

## Guidance Notes:

1. **Create an Effective Security Risk Management Structure:** Ultimate accountability for staff security and safety rests with the governing bodies, such as the Board of Trustees, who then delegate responsibility to the Executive Director/CEO, or a position of similar seniority, to ensure that effective SRM is in place. Day-to-day management and responsibility for security is shared across different levels in the organization, following the line of management.

Therefore, it is necessary to identify existing positions with a critical role in staff security and safety, including managers based in the field and at the headquarters. Furthermore, the security responsibilities and specific decision-making roles of each of these positions should be defined in respective staff members’ job descriptions. Their security responsibilities should be included in the organization’s safety and security policies so that all staff member are informed.<sup>14</sup>

Many organizations appoint individual staff or a group of staff to act as a security working group and/or security focal point to support the development of the organization’s SRM framework, ensure there are agreed policies and procedures in place, as well as provide advice to the line of management if required. The advantage of appointing a group of staff representing different roles and levels within the organization is to bring a wide range of experience and perspectives, and encourage a greater sense of ownership. It is important that these people are given adequate time, support and training to do these tasks in addition to their usual tasks. It is also important to note that the security focal point or working group is not responsible for managing security risks. Instead, security management responsibilities must remain embedded within the normal line management (see “Example Structure and Responsibilities” on the following page).

When identifying specific security roles and responsibilities, it is necessary to be realistic for the organization considering its size, the complexity of its structure, and existing roles and capacities.

2. **Collective Responsibility for Safety and Security:** Security awareness is an ongoing collective responsibility. Each staff, therefore, is obliged to actively participate in and contribute to the maintenance of security measures, be aware of and responsible for their own security risks and team security, and understand and adhere to security measures. It is important to develop a culture of security within the organization, and to treat security as a staff-wide priority, not a sensitive management issue to be discussed only by a few staff members behind closed doors. For example, the following considerations could be useful to develop a culture of security in the organization:

---

<sup>14</sup> For concrete examples of security responsibilities, see GPR8 (2010) Chapter 6 (People in Security Management); Care International. (n.d.) *Role of Safety and Security Management in an Emergency*. Retrieved on 21 March 2018 from <https://www.careemergencytoolkit.org/management/14-safety-and-security/1-role-of-safety-and-security-management-in-an-emergency/>; and Mercy Corps. (2011). *Field Security Manual* (March 2011).

- Staff designated as Security Focal Points must be encouraged to attend security training courses as run by INSO, UNHCR or other NGOs and to enrol in online courses run by EISF.
- Make sure that all staff are familiar with the context, risk and commitments of the organization in terms of risk reduction and security management.
- Make sure that all staff are clear about their individual responsibilities with regard to security, teamwork and discipline.
- Advise and assist staff to address their medical, financial and personal insurance matters prior to deployment to a high-risk environment.
- Be clear about the expectations of managers and management styles under normal and high-stress circumstances.
- Ensure that security is a key consideration in all programme planning.

Mainstreaming a security culture means considering the security implications involved in everything the organization does, from discussions about programme design and public messages to funding decisions and the hiring of external contractors. It is also crucial to make sure that all staff, including national/local staff, know the organization and its mission in any given context. Staff need to be told what the organization is about. Key questions include:

- Why is this organization here?
- What is it doing here?
- Where does it get its money from? What does it use that money for?
- Who directs its activities?
- Is it serving foreign political interests?
- What is its political agenda?
- Does it want to change local society, culture, values or religion?

Consider providing staff with some written materials in their own language(s), and go through them with staff in an interactive way. Furthermore, periodically bring staff together to hear from them what sorts of questions and comments they most regularly get from those in the community and how they answer them. It is important to remind every member that they should behave as a positive representative of the organization. Each member is responsible for reporting to their line manager regarding any action or behaviour that breaches policy or jeopardises team security.

3. **Measures to Enhance Accountability:** The following activities may enhance the organization’s accountability for security.

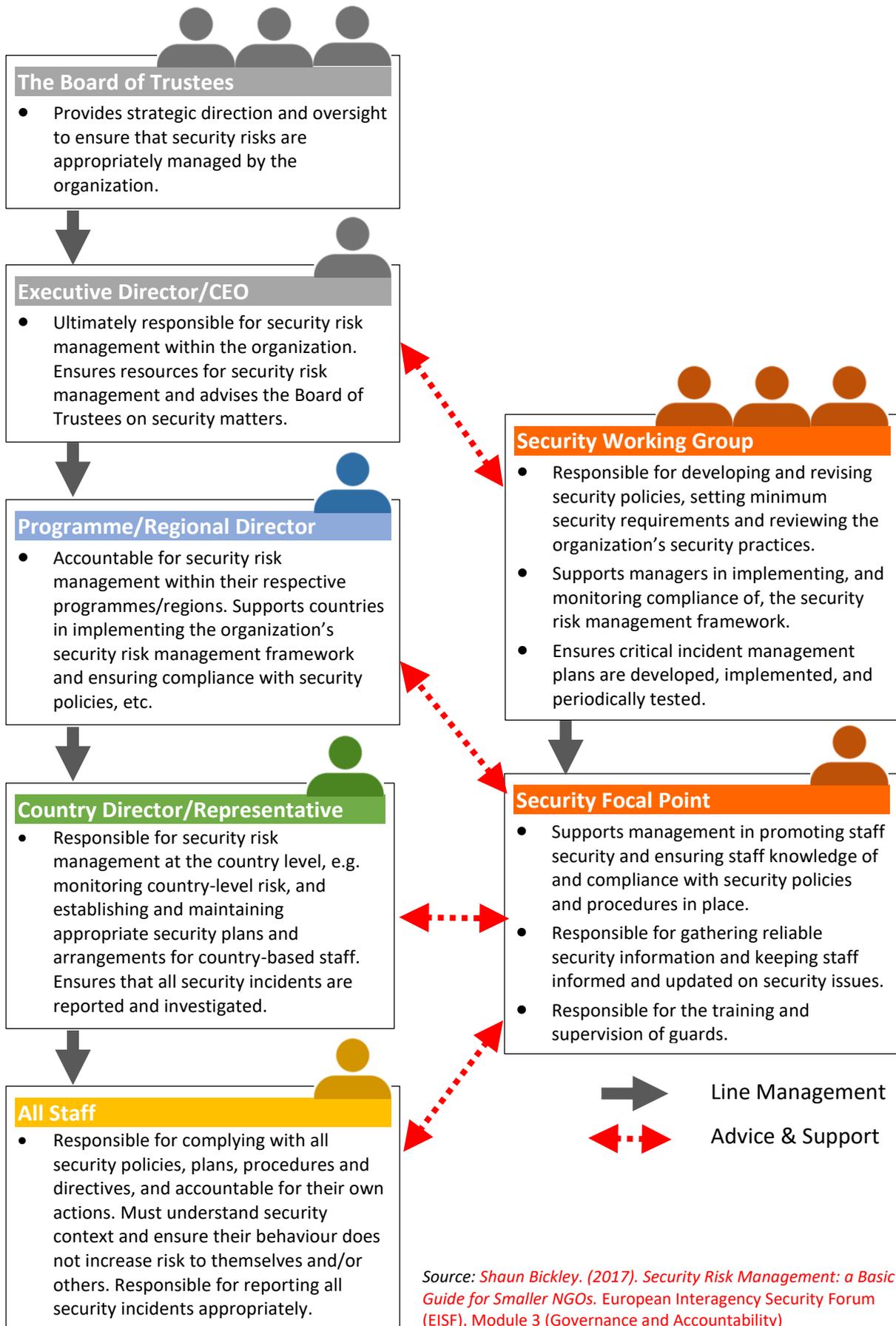
- **Periodical security briefings and drills** will enhance staff members’ knowledge of lines of responsibility and authority. Outcomes of drills will help review the organizational effectiveness of management systems and structures (lines of responsibility, human resources, technology, procurement, etc.).
- All staff with security responsibilities must have their duties clearly articulated in their **job description**, and, for accountability, assessed in their **performance review**.
- **Violations of security policies and procedures** have clear consequences for the violators which are spelled out in the human resources policy. Procedures to address

non-compliance and violations of established safety and security policies and procedures should be in place and made known to staff members at all levels.

**References**

- GPR8. (2010). Chapter 1.2 (Organisational Security Management)
- InterAction. (n.d.). *Security Risk Management – NGO Approach*
- Shaun Bickley. (2017). *Security Risk Management: A Basic Guide for Smaller NGOs*. European Interagency Security Forum (EISF). Chapter 3 (Governance and Accountability)

**Reference 5-I: Example Structure and Responsibilities**



## Standard 6: Collaboration with Other Actors

*Signatories shall actively participate in safety and security related forums at both headquarters and field levels and collaborate with other members of the humanitarian and development communities to advance their common safety and security interests.*

Although security management is considered to be largely agency-centred, there are many good reasons why the agencies should cooperate with the community for security management. Security will be dramatically enhanced through coordination, information sharing and the recognition that the behaviour of an individual NGO impacts on the security of the entire humanitarian community (which could be described as a “sense of community”).

### Key Actions:

- Raise the importance of collaboration with the humanitarian and development communities for safety and security within the organization. (see also Guidance Note 1)
- Participate in humanitarian and development communities at both headquarters and field office levels in order to cooperate on security management. (see also Guidance Notes 2 and 4)
- Actively participate in security forums organized by NGOs and/or the UN at the headquarters and/or field office levels. (see also Guidance Notes 3 and 4)
- Appoint a staff responsible for security to identify and participate in security forums. (see also Guidance Note 3)

### Key Indicators:

- Staff in the headquarters and field offices are provided with adequate information of the members in the humanitarian and development communities and about joint security initiatives.
- Official and non-official personal relationships increase the exchange of security information from reliable sources.
- The organization has a written list of security forums.
- The responsibility to play an active part in security forums is clearly stated in the job description of the person in charge.
- Financial and human resources are secured for taking collaborative action.

### Guidance Notes:

1. **Advantages of Collaboration:** Some of the advantages of collaboration include:
  - A better alert system: Agencies can receive a fuller picture of actual or possible security threats or alerts in their environment, thus increasing the chance of avoiding an incident (such as using a ‘communications tree’ for wireless radios, walkie-talkies, satellite phones, etc.).
  - Better SRA: Maintaining a shared record of all incidents in an operating environment provides a better basis for a risk assessment than a partial or incomplete record.

- Strategic and tactical monitoring and analysis of the operating environment: All agencies do this by contacting other agencies informally to obtain information. Trust and confidentiality make it possible to collaborate in a more structured way.
  - Cost-effective services: For example, the costs for security training can be shared, rather than each agency individually covering the costs of bringing in or hiring specialists.
  - Liaison with the authorities: Rather than negotiating individually, agencies can make a stronger and more consistent case together. This would include exchanging information with military actors.
  - Advocacy with donors: If the security situation deteriorates and several agencies conclude that they need extra financial resources for additional mitigating measures, they may be able to make a more effective case with donors collectively.
  - The operations of and/or conduct of one organization can impact the security of other members of the humanitarian and development communities. Actively seeking to minimize all the negative impacts that the organization’s operations have on others can make a difference.
2. **Information Sharing:** Making good decisions requires reliable and accurate information. All information must be considered against the reliability of the source, the number of individuals and organizations reporting the same information, and any local bias. 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 analyses, situation reports, threat assessments, and security training. In order to share security related information with other actors, the organization should establish policies and procedures for sharing such information (who decides what information could be shared with whom and how).
3. **Participation in Security Forums:** There are many security related forums at both headquarters and field office levels. Participation in these security forums provides opportunities to share useful information, exchange good practices, and consider the larger picture of safety and security in both the global and operational environments. It is strongly advised that organizations join such security forums to gather information and to identify good practices for the particular operation. Security forums are usually chaired by one organization and attended by respective security focal points.

When appointing a staff member to attend the coordination meetings, ensure the person is supported to dedicate time as a priority, and is fully briefed on the rules for participation. The staff should know how the information is to be shared and managed. If there is no security forum, NGOs are encouraged to take the initiative with other agencies to collaborate on holding a meeting. Security forums are useful mechanisms for improving organizations' understanding of the current international standards related to security management, and for improving awareness on security management for small NGOs. Security forums can also share the costs of organizing training for staff, and act as a coordination point with other actors such as the United Nations Department of Safety and Security (UNDSS).

When deemed appropriate by an organization, it can participate in “Saving Lives Together (SLT)”<sup>15</sup>, which is a framework aimed at enhancing UN and NGO security collaboration in field operations. The objective of SLT is to enhance the ability of partner organizations to make informed decisions and implement effective security arrangements to improve the safety and security of personnel and operations, while operational decisions made on the basis of such information remain the responsibility of the respective organizations. In larger operations it will be found that UN OCHA conduct regular security/coordination briefings at which NGOs are welcomed. Attendance at such gatherings is encouraged.

4. **Sources of Additional Information:** There are a number of sources of additional information that organizations can link into to improve the flow of information on security incidents, find advice on how to mitigate security risks from various threats and improve security capacity:
  - Host government departments;
  - National governments, including donor governments and their embassies;
  - United Nations Department of Safety and Security (UNDSS), UN Office for the Coordination of Humanitarian Affairs (UN OCHA), and other UN Agencies such as United Nations High Commissioner for Refugees (UNHCR);
  - Insurance providers, which often have a threat advisory service linked to various countries and regions;
  - NGO security consultants, such as International NGO Security Organization (INSO);
  - Local commercial security providers (guard companies);
  - International and national media;
  - Other NGOs and their partner organizations – both national and international NGOs;
  - Host and beneficiary communities; and
  - National staff.

### **References**

- Inter-Agency Standing Committee (IASC). (2015). *Saving Lives Together: A Framework for Improving Security Arrangements Among IGOs, NGOs and UN in the Field (October 2015)*
- GPR8. (2010). Chapter 1.3 (Interagency Security Management), Annex 2 (The United Nations Security Management System), Annex 3 (Saving Lives Together)
- InterAction. (2015). *InterAction Minimum Operating Security Standards*
- Mercy Corps. (2011). *Field Security Manual (March 2011)*
- Care International. (2008). *Care International Safety and Security Principles*
- ECHO. (2004). Section 4.5 (Relations with Other Organisations)

---

<sup>15</sup> See Inter-Agency Standing Committee. (2015). *Saving Lives Together: A Framework for Improving Security Arrangements Among IGOs, NGOs and UN in the Field (October 2015)*. Retrieved on 21 March 2018 from <https://interagencystandingcommittee.org/collaborative-approaches-field-security/content/saving-lives-together-framework-improving-security-0>; and Christian Aid. (2010). *Saving Lives Together: A Review of Security Collaboration between the United Nations and Humanitarian Actors on the Ground*. Retrieved on 21 March 2018 from <https://reliefweb.int/report/world/saving-lives-together-review-security-collaboration-between-united-nations-and>.

## Standard 7: Safety and Security of Local Partner Organizations

*Signatories shall incorporate local partner organizations into their safety and security management system, based on mutual respect and shared responsibility and endeavour to achieve the above six Standards.*

### Key Actions:

- When conducting joint projects with local partner organizations, organizations should conduct a joint Security Risk Assessment (SRA) of the project area with the local partner organizations and take security measures by methods and in ways that they can agree on, reducing possible security risks as much as possible. (see also Guidance Notes 1 and 2)
- Agree on concrete responsibilities and roles in an emergency, as well as to the usual security measures, and share them among related actors. (see also Guidance Notes 3 and 4)
- Secure necessary training, briefing, equipment, and funding for the security of the staff of local partners. (see Standard 3: Resources)

### Key Indicators:

- When implementing projects with local partner organizations, organizations should understand the security risks that they may face, respect the safety and security policies, and agreed on the security risk measures to be taken. It should also be written in a memorandum of understanding (MOU).
- Close and smooth communication with local partners is ensured. If necessary, budget for consultations in third countries or invitation to the headquarters is secured.
- In accordance with the security compliance ability of local partner organizations, it is necessary for organizations to secure human resources and training opportunities, and to ensure there is sufficient budget for equipment and materials for security and crime prevention measures.

### Guidance Notes:

1. **Security measures when implementing partner projects:** Partnerships with local partner organizations are effective when implementing projects. Recently, project implementations through local partners have increased due to the operations in high-risk countries where international NGOs cannot directly implement projects. Therefore, when considering cooperative projects in countries with poor security, organizations should not just transfer any possible risks to local partner organizations but should consider security concerns and measures to be taken. In addition, organizations should understand that organizations and local partner organizations have different security risks. International NGOs with overseas headquarters and local NGOs established in their own countries often have different understandings of and responses to the security risks they may encounter. Also, acceptance in local society differs among them, and so details of the safety and security policies may also be different. With this understanding, the project should be implemented accordingly.

- Regardless of security problems in particular, there are cases where a project can be implemented in partnership with local organizations only through business trips and remote management. Even so, as there is always a possibility of becoming involved in general crimes, diseases, accidents, etc., organizations should endeavour to achieve all six standards for safety and security.
- When conducting a project through remote management without deploying international staff in the field, not only risk countermeasures during business trips but also security measures for threats that local partner organizations may confront in daily work shall be examined and agreed upon by both organizations.
- When the project is fully remote controlled and there is no chance to visit the project site at all, it is important to communicate closely (e.g. conduct a meeting with local partner organizations in different countries) and to ensure that security measures are taken.

## 2. Points to include in the agreement:

- Visibility: Depending on the situation, organizations may refrain from using logos and signs of donors, own organization, and local partner organizations.
- Right to make a decision on security issues in the local area: Clarify the responsibility of the representative and appropriately make decisions on the site.
- Public relations activities as an organization: If there is a fight between ethnic groups or religious groups, organizations should be aware that public relations activities could interfere with the activities of those groups. Also, when publishing something on SNS (Social Networking Service) which could reveal the movements of international staff, organizations should pay special attention to language, place, timing, etc. with consideration for security, the method and frequency of monitoring, and reporting.
- The method of handling SOPs and security plans by both groups should be clarified (including emergency contact list), so that the latest information can be shared among groups.
- Emergency response: Clarify the criteria for deciding on withdrawal or suspension, and how to settle expenses in such a case, etc.

3. **Communication with Local Partner Organizations:** Close communication is vital for taking security measures among different organizations. It is necessary to formulate project plans in collaboration with local partner organizations and to communicate frequently during project implementation. It is also important to exchange opinions directly with the staff of local partner organizations through business trips and on-site visits as well as usual communication by e-mail, telephone, etc. Especially when organizations cannot visit the project site due to deterioration of security, etc., it is necessary to try to meet the staff of local partner organizations in a different country.

4. **Security Measures on Relocation:** When the project is suspended temporarily or terminated in the middle due to deterioration of the security situation, organizations should take appropriate measures not only for their own staff but also the staff of the local partner organization. Even if the organization evacuates only its own staff and the

project continues with the local partner team staying, it is important to consider possible security risks and take countermeasures.

**References**

- ECHO. (2004). Section 4.5 (Relations with Other Organisations)
- InterAction. (2015). *InterAction Minimum Operating Security Standards*.
- OCHA. (2011). *Safety and Security for National Humanitarian Workers. Annex I to: To Stay and Deliver – Good Practice for Humanitarians in Complex Security Environment*. Section 5 (Organisational Policies and Approaches to Duty of Care)

## References

- Bickley, Shaun. (2017). *Security Risk Management: A Basic Guide for Smaller NGOs*. European Interagency Security Forum (EISF). Retrieved on 21 March 2018 from <https://www.eisf.eu/library/security-risk-management-a-basic-guide-for-smaller-ngos/>.
- Care International. (2008). *Care International Safety and Security Principles*. Retrieved on 21 March 2018 from <https://www.careemergencytoolkit.org/management/14-safety-and-security/3-complying-with-cares-safety-and-security-policies-and-procedures/>.
- Care International. (2013). *Care International Safety and Security Standards*. Retrieved on 21 March 2018 from <https://www.careemergencytoolkit.org/management/14-safety-and-security/3-complying-with-cares-safety-and-security-policies-and-procedures/>.
- Care International (n.d.) *Role of Safety and Security Management in an Emergency*. Retrieved on 21 March 2018 from <https://www.careemergencytoolkit.org/management/14-safety-and-security/1-role-of-safety-and-security-management-in-an-emergency/>.
- Christian Aid. (2010). *Saving Lives Together: A Review of Security Collaboration between the United Nations and Humanitarian Actors on the Ground*. Retrieved on 21 March 2018 from <https://reliefweb.int/report/world/saving-lives-together-review-security-collaboration-between-united-nations-and>.
- CHS Alliance, Group URD and the Sphere Project. (2014). *Core Humanitarian Standard on Quality and Accountability*. Retrieved on 21 March 2018 from <https://corehumanitarianstandard.org/the-standard/language-versions>.
- Concern Worldwide (2016), *Concern’s Security Policy (March 2016)*, Retrieved on 21 March 2018 from <https://www.concern.net/resources/security-policy>.
- Davis, James. (2015). *Security to Go: A Risk Management Toolkit for Humanitarian Aid Agencies*. European Interagency Security Forum (EISF). Retrieved on 21 March 2018 from <https://www.eisf.eu/library/security-to-go-a-risk-management-toolkit-for-humanitarian-aid-agencies/>.
- Davis, James and Reilly, Lisa (2015), *Security to Go: A Risk Management Toolkit for Humanitarian Aid Agencies*, European Interagency Security Forum (EISF), Retrieved 21 March 2018 from <https://www.eisf.eu/library/security-to-go-a-risk-management-toolkit-for-humanitarian-aid-agencies/>.
- European Commission’s Directorate-General for Humanitarian Aid (ECHO). (2004). *Generic Security Guide for Humanitarian Organisations*. Retrieved on 21 March 2018 from <https://reliefweb.int/report/world/generic-security-guide-humanitarian-organisations-enar>.

- Hoppe, Kelsey and Williamson, Christine. (2016). *Dennis vs Norwegian Refugee Council: Implications for Duty of Care*. Humanitarian Practise Network (HPN). Retrieved 21 March 2018 from <https://odihpn.org/blog/dennis-vs-norwegian-refugee-council-implications-for-duty-of-care/>.
- InterAction. (2015). *InterAction Minimum Operating Security Standards*. Retrieved on 21 March 2018 from <https://www.interaction.org/document/interaction-minimum-operating-security-standards-and-suggested-guidance-language>.
- InterAction. (n.d.). *Security Risk Management - NGO Approach*. Retrieved on 21 March 2018 from [https://www.interaction.org/sites/default/files/2581/NGO\\_SRM\\_APPROACH\\_FINAL\\_SAG\\_APPROVED.pdf](https://www.interaction.org/sites/default/files/2581/NGO_SRM_APPROACH_FINAL_SAG_APPROVED.pdf).
- Inter-Agency Standing Committee (IASC). (2015). *Saving Lives Together: A Framework for Improving Security Arrangements Among IGOs, NGOs and UN in the Field (October 2015)*. Retrieved on 21 March 2018 from <https://interagencystandingcommittee.org/collaborative-approaches-field-security/content/saving-lives-together-framework-improving-security-0>.
- Irish Aid. (2013). *Irish Aid Guidelines for NGO Professional Safety and Security Risk Management*. Retrieved 21 March 2018 from <https://www.irishaid.ie/news-publications/publications/publicationsarchive/2013/august/guidelines-for-ngo-professional-safety-security/>.
- Japan NGO Center for International Cooperation (JANIC). (n.d.). *Understanding NGOs* [Japanese article]. Retrieved on 21 March 2018 from [www.janic.org/ngo/faq/](http://www.janic.org/ngo/faq/).
- Japan Afghan NGO Network (JANN). (2009). *On Civilian Assistance in Afghanistan Alternative to Japan's Refuelling Mission in the Indian Ocean* [Japanese article]. Retrieved on 21 March 2018 from [http://www.ngo-jvc.net/jp/notice/2010/data/20100219\\_afghanistan\\_lobby.pdf](http://www.ngo-jvc.net/jp/notice/2010/data/20100219_afghanistan_lobby.pdf).
- Lutheran World Federation. (2016). *LWF Safety and Security Policy (March 2016)*. Retrieved on 21 March 2018 from [https://www.lutheranworld.org/sites/default/files/lwf\\_safety\\_and\\_security\\_policy\\_-\\_march\\_2016.pdf](https://www.lutheranworld.org/sites/default/files/lwf_safety_and_security_policy_-_march_2016.pdf).
- Mercy Corps. (2011). *Field Security Manual (March 2011)*. Portland: Mercy Corps.
- Merkelbach, Maarten and Kemp, Edward. (2016). *Duty of Care: A review of the Dennis v Norwegian Refugee Council ruling and its implications*. Retrieved 21 March 2018 from <https://www.eisf.eu/library/duty-of-care-a-review-of-the-dennis-v-norwegian-refugee-council-ruling-and-its-implications/>

- Office for the Coordination of Humanitarian Affairs (OCHA). (2011). *Safety and Security for National Humanitarian Workers. Annex I to: To Stay and Deliver – Good Practice for Humanitarians in Complex Security Environment*. Retrieved on 21 March 2018 from <https://reliefweb.int/report/world/safety-and-security-national-humanitarian-workers>.
- Overseas Development Institute. (2010), *Operational Security Management in Violent Environment, Good Practice Review Number 8 (New Edition)*, London: Overseas Development Institute. Available from <https://odihpn.org/resources/operational-security-management-in-violent-environments-revised-edition/> (as of 21 March 2018).
- People in Aid. (2003). *Code of Good Practice in the Management and Support of Aid Personnel*. Retrieved on 21 March 2018 from <https://reliefweb.int/report/world/people-aid-code-good-practice-management-and-support-aid-personnel>.
- People in Aid. (2008). *Policy Guide and Template: Safety and Security (Revised)*. Retrieved on 21 March 2018 from <https://www.chsalliance.org/files/files/Resources/Tools-and-guidance/safety-and-security-policy-guide-and-template.pdf>.
- Tomita, Kei'ichiro. (2007). Provisional Reconstruction Team (PRT) Operations in Afghanistan [Japanese article]. *Reference 2007-03*. Retrieved 21 March 2018 from <http://dl.ndl.go.jp/info:ndljp/pid/999764>.
- USAID. (2018). *Provincial Reconstruction Teams*. Retrieved on 21 March 2018 from <https://www.usaid.gov/provincial-reconstruction-teams>.