# Guidebook for NGO Standard for Safety and Security [ENG]

Version DRAFT 1.2 – 2017-11-07

**Japan NGO Initiative for Safety and Security（JaNISS）**

## Contents

## Abbreviation

CHS: Core Humanitarian Standards on Quality and Accountability
CIMPs: 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

# Aim of this Guidebook and How to Use this Guide

## 1. Aim of this Guidebook

NGO Standards and the Guidebook for Safety and Security have been produced by a voluntary contribution from Japan NGO community working in humanitarian and development context. The Standards and the Guidebook is prepared in Japanese and English language, and aim to offer the following:

- To serve as standard documents, and to provide managers and staff of Japan NGO s with a common understanding on the context and the terminologies related to safety and security to facilitate better information sharing and cooperation among them.
- To present Japan NGOs, which are in a wide diversity, with the safety and security related items commonly regarded as important, regardless of their scale, mission, mode of operation, activity and operating location
- To help individual Japan NGOs make self-evaluation on to what extent they have covered the safety and security related items that should be given consideration, and locate resources and references when they find room to improve
- To provide Japan NGOs with references to relevant documents and online information accumulated by the United Nations organizations and international NGOs
- To introduce, and encourage to introduce methods and ideas related to safety and security which had not been fully incorporated by Japan NGOs such as “security risk analysis”, “security planning and reviewing involving all relevant staff members ”, “security related trainings”, and “clear definition security roles and responsibilities of managers and staff members”.
- To serve as comprehensive documents to describe the concept and methods of security management by humanitarian and development NGOs, and to raise awareness among Japan’s society that Japan NGOs carry out their duties as professionals.

## 2. What this Guidebook and the Guidelines Covers/Highlights

- Compatible with Japan NGOs working in both humanitarian and development context, not intended for only those working in conflict areas.
- Compatible with NGOs regardless of their scale and the formulation of organization i.e., whether the organization is composed of paid or unpaid staff, resident or deployment base staff in the field
- Compatible with NGOs located in the regions in Japan where occasions for capacity building were previously limited, and to serve for their capacity building efforts by providing information on safety and security in a comprehensive way
- To cover most aspects of security that are commonly thought relevant, yet composed in a user-friendly layout so that each user can find out and read only those relevant parts based on his/her purpose.
- Covers safety and security related items that should be taken into consideration by wide variety of organizations. However, it remains to be open for individual organizations to

decide how and to what extent they implement those based on their own information gathering, judgement and responsibilities.

## 3. What this Guidebook and the Guidelines Do Not Cover/Highlight

- The Standards and the Guidebook are not designed to serve as standards of safety and security for individual NGOs as they are.
- They do not intend to enforce certain standards or policies on individual NGOs
- They do not provide stand-alone templates and formats, as it is not intended that individual NGOs make security guidelines and plans as documents, just as a matter of formality.
- They just offer suggested standardized resources and are designed to assist organizations to manage their security with their own initiative. This does not in any way means the Standards and the Guidebook nor JaNISS take the responsibility for security management of individual NGOs nor guarantee security for any organization by referring to the Standards and the Guidebook.

## 4. How this Guidebook is composed

This Guidebook has been composed following 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:** serves 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 action.

- **Guidance Note:** includes context-specific points to consider when aiming at reaching the key actions and key indicator. It provides knowledge, good-practices, information and resources accumulated by global humanitarian and development community. Further details and references are provided at the end of each chapter.

## 5. How Information Are Labeled

- Standards, Key actions and Indicators are bordered
- Guidance notes of particular importance are highlighted in blue
- Information in Standard 2 that are 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)

Senior Managers and Operational Managers of organizations such as Executive Board members may want to refer to the following sections of this Guidebook:

- Standard 1
- Key actions and Key indicators for other standards (there are three key indicators for Standard 2)
- Sections that are highlighted in blue

B) Security Managers/Officers of Organizations

Security Managers/Officers of organizations may wish to refer to the whole Guidebook. However, those who do not work in conflict or high risk may not necessary find sections that are shaded in Standard 2 to be relevant, and in such case, one may skip to the next section.

C) Organizations Working in Development Projects

Organizations that do not work in conflict or high risk areas may not necessary find sections that are shaded in Standard 2 to be relevant. In such case, one may skip to the next section.

D) Organizations Working in Conflict and High Risk Areas

Sections that are shaded in Standard 2 are intended for organizations working in conflict and high risk areas. You may wish to conduct a security risk analysis (SRA), and if results show that some action is required, you may wish to carefully read through this Guidebook and employ improvement measures.

E) Those Who Wish to Have a Quick Summary View of the Guidebook

You may wish to refer to the following sections:

- Key actions and key indicators of each standards (there are three key indicators for Standard 2)

Furthermore, you may wish to refer to the following sections for a better understanding:

- The “Background” section before Standard 1
- Sections highlighted in blue

F) Those Who Wish to Conduct a “self-check” on Their Organization’s Security Plans and Procedures, or Wish to create Their Organization’s Security Plans

You may wish to consult with the resources and the three Guidance Notes provided in Standard 2, assess the situation within the organization, and take necessary measures and actions to improve your security policies, procedures and plans.

We highly recommend the reflections, measures and actions taken to be put together

in a document and shared amongst relevant parties. The critical part of this exercise lies in the planning and reviewing process of the security plan with the involvement of all relevant staff, and not the document which is produced from this exercise. Thus the document should be kept simple and concise.

For organizations which do not have field offices, and operate on a deployment base are suggested to refer to "2.3 Security Plan at Field" as a part of "Security Plan at Headquarters (2.2)" and 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 at Field", "Reference 2-III: Sample Outline of a Security Plan for Field Posts"

**Disclaimer:** These documents are general in nature, and their contents may not be applicable in all situations. The advice they offer may be inappropriate in some circumstances and in some cases could even place people at risk of death or injury. They are not designed as stand-alone documents and their contents should be modified and adapted by operational managers as appropriate to suit the needs of particular organizations and situations.

# 0. Background

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

Looking back on the history of the Japanese NGOs, the first wave of the emergence took place in early 1960's, 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. Over 30 years after the advent, Japanese NGOs expanded their operational size, working in various sectors and having presence not only in Asian countries but also in Middle-Eastern, African, and Latin American countries. Quite a few NGOs do not limit themselves to working in the development context, but are proactively engaged in the humanitarian response both in natural and complex emergencies.

Regardless of working in a development context or a humanitarian context, expansion of the operational size will increases the chance of encountering various threats. According to the Humanitarian Outcomes report, the dimension of the security environments has become much more complex since 1990's. For 10 years between 2005 and 2015, the casualties of the aid workers have been steadily increasing. Japanese staff are not immune to this a trend, too. Since 2000's, quite a few cases, in which Japanese staff had been kidnapped/abducted, taken as hostages, or become victims of terrorism, have been reported. Though not becoming victims of such security-related cases, a number of aid workers had lost their lives due to contingent event such as road accidents and diseases.

Given that security as well as safety related threats are prevalent, what kind of security risks could NGOs face in their working environment? Take a threat of malaria as an example. Suppose that a Japanese staff managing a project in a malaria endemic area were infected by malaria and hospitalized in a groggy condition. As long as the organization made a decision to implement a project in a malaria endemic area, the organization should have provided the staff necessary measures for malaria prevention as well as all possible means to protect the life of the staff in case of the infection. In the worst case scenario of loss of his/her life, the organization inevitably has to face the situation where the top-management needs to explain the incident to the public.

We, as NGOs working in the field of international cooperation, are responsible for ensuring the safety and security of all concerned staff and stakeholders. It means, if any person involved in our work – irrespective of being an international staff or a national/local staff, of being a direct employee or a beneficiary – become a victim of any type of incidents, we are morally and legally obliged to take an institutional action. If the organization should not a properly respond to the incident, it would lead to a grave consequence 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.

This chapter describes the threats that NGOs are facing, capturing an overview of how safety and security environments had changed between the emergence of Japanese NGOs and present, then mentions institutional responsibilities that organizations should take in working

in high risk environments, and concludes the chapter by stressing the importance of security management as an enabler for programs and accountability.

## 0.2. A Brief Chronicle on Change in Security Environments

- 1960's to 1980's
  The emergence of Japanese NGO took place in this period. While a nuclear war was the main security threat under the Cold War regime, the threat of ethnicity or religion oriented conflict was not so prevalent as nowadays. The major safety and security concerns for NGOs therefore were mainly those of ordinary crime, traffic accident, and diseases.

- 1990's
  The end of the Cold War triggered the rise of political and religious radicalism as well as ethnic cleansing, which led to the ethnic and religious conflicts worldwide. Along with the increase in humanitarian need in the 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. The incidents directly targeting Japanese staff, however, were still rare during this period.

- 2000's
  Establishment of Provincial Reconstruction Team (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 a way that the government of Japan shifted its stance to prohibiting Japanese nationals from going to the medium/high risks areas.

- 2010's
  Protracted conflicts in Middle East and Africa exacerbated the security environments. Japanese nationals continue becoming victims of 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 the conflict are no longer immune to the terrorism. It requires development actors, whose mandate is not necessarily a humanitarian nature, to raise their awareness on security management.

## 0.3. Safety & Security is an Enabler for Programmes

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

The world-wide deterioration of the security environment after 1990's tilts the scales against pursuit of our missions, meaning the security risks are often higher than the outcomes we may expect. While security threats are increasing significantly over decades, humanitarian and development needs are also increasing than ever before. In such circumstances, it is NGO itself that should make a decision on "Go" or "No Go" in a high risk environment, and once the "Go" decision is made, 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 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 NGO's mission 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 effect, 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 7 standards that would enable the organization to operate in the high risk environments. These standards are not the ends per se. These are means to the ends.

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

PRT is a military-civilian structure designed to operate in semi-permissive environment such as post-conflicted countries. It was initiated by the US in post-Taliban Afghanistan in early 2000's. A number of PRTs were formulated mainly by the NATO states and their command authority was delegated to International Security Assistance Force (ISAF)[1]. 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[2]. PRTs were also in operation from 2005 to 2011 in Iraq[3]. While it has been said that PRTs improve security, support good governance, and enhance provincial development[4], criticisms also have been raised from civil society arguing that, because of the nature of military-oriented operation, there were concerns on PRTs' efficiency, speciality and equity in delivering aid assistance. Civil society also concerns that security threats to humanitarian workers would increase as local people could confound humanitarian workers with military-associated personnel.[5]

[1] 「アフガニスタンで活動する地方復興支援チーム(PRT) : 民軍共同による紛争後の平和構築支援活動」, http://dl.ndl.go.jp/info:ndljp/pid/999764

[2] USAID, Provincial Reconstruction Team, https://www.usaid.gov/provincial-reconstruction-teams

[3] United States Institute of Peace, Provincial Reconstruction Team in Iraq, https://www.usip.org/publications/2013/03/provincial-reconstruction-teams-iraq

[4] 「アフガニスタンで活動する地方復興支援チーム(PRT) : 民軍共同による紛争後の平和構築支援活動」, http://dl.ndl.go.jp/info:ndljp/pid/999764

[5] インド洋での給油活動に代わるアフガニスタンでの 民生分野支援の活動について, http://jnne.org/%83A%83t%83K%83%93%8Ex%89%87%8D%F4%83%8D%83r%81%5B%83%8C%83%5E%81%5B%8D%C5%8FI%94%C5.pdf

## Standard 1: Commitment to Safety and Security

*The management of signatory organizations commit to ensure the safety and security of its staff, volunteers, interns, 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, even not being liable to individual passion toward 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, ensuring safety and security of its own staff members is the primary responsibility of representatives of the organization.

**Duty of Care**

Duty of care is organizational obligations and its implications that these have 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 organizations have towards their staff, there is also a moral obligation of duty of care that organizations should consider. As professionals of humanitarian activity, duty of care to humanitarian workers should not be undermined and indeed it should complement 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 were 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, People in Aid Code of Good Practice in the Management and Support of Aid Personnel and Core Humanitarian Standards 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 wide recognition that compliance with those international standards enhances organizational safety and security in the fields.

**Key Actions:**

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

**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, Duty of Care of organization refers to "Duty of Care of Mandatary" in the article 644 of the Civil Code. The organization and the governing bodies are in a relationship that responsibilities of the organization is delegated to the governing bodies by the organization. In accordance with Article 644, the governing bodies which are delegated the organizational responsibilities (that refers

to board directors, supervisors, auditors etc.) "shall assume a duty to administer the mandated business with the care of a good manager 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 how they are paid or unpaid neither full-time nor 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 is 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 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 and poverty. The principle of "Do No Harm," for example, obliges 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 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 web site address; and (3) submit its request through the head of the organization. To register, please visit IFRC web page: 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 on the rise of serious incidents – killings, kidnappings, or attacks that cause serious injuries – and politically-motivated attacks against humanitarian workers, InterAction, which is the largest alliance of U.S.-based international nongovernmental 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 the incorporation of MOSS in their respective institutional approaches to security. Recognizing that every organization will have differing needs, the "Suggested Guidance" section for each standard below represents point(s) to consider, rather than requirements, for implementing InterActions' Security Standards. Not every point is necessarily appropriate for every organization or for every situation. MOSS introduced systematic approaches to NGO's risk management and those security risk management systems have become the industry standard, which many of InterAction's members follow. JaNISS has been referring to this InterAction's MOSS during the development of own "NGO Standards for Safety and Security" with technical cooperation from the InterAction's Security Unit.

7. **People in Aid Code of Good Conduct:** People in Aid has been bringing together agencies working in the aid and development sector, to enhance the impact they make through better management and support of staff and volunteers. The People in Aid Code of Good Practice devotes one of its seven principles to health, safety and security. When the Code was first formulated it was explicit that the end product was 'staff security and well-being'. The six principles which preceded it all enabled the agency to assure itself that staff were being looked after, in the broadest sense. Strategy, planning, budgeting, briefing, training, consultation and more all contributed to staff security and well-being. That in turn is reflected in staff retention rates and quality of aid delivery.

8. **Core Humanitarian Standards (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 EUR or 60 million JPY).

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 a significant remark on duty of care.

**Reference**


- Irish Aid Guidelines for NGO Professional Safety and Security Risk Management, 2013.
- European Interagency Security Forum (EISF), Security Risk Management: A Basic Guide for Smaller NGOs, 2017.
- Kemp, E. & Merkelbach, M. (2016). Duty of Care: A review of the Dennis v Norwegian Refugee Council ruling and its implications. European Interagency Security Forum (EISF).

- Hoppe, K. & Williamson, C. (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 safety and security Plans at both the headquarters and field levels based on a participatory 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 protocol that guides all the agency's security decisions. Security plans are headquarters and country specific plans to manage risk at a given country offices.

### 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 operations 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:**

- Define safety and security risk, the organization's safety and security risk attitude, key security principles, roles related to SRM and organization's responsibilities to its employees. (Guidance Notes 1, 2, 3, 4 and 5; see Reference 2-I for a sample outline of safety and security policies)
- Align safety and security policies with the organization's mission, mandate, commitments, and mode of operation. (Guidance Note 2)
- 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 failed to adhere to security policies. (Guidance Note 3)
- Communicate disciplinary mechanisms to treat non-compliance of policies and procedures. (Guidance Note 3)

**Key Indicators:**

- Safety and security policies clearly state the organization's definition of security risk, security risk attitude, key security principles, roles and responsibilities.
- Safety and security policies include a value statement relating to safety and security of organization's staff, and a clear operational link between this value statement and security related Standard Operating Procedures (SOPs) at a field level.
- Safety and security policies clearly state the organization's risk management objectives, the rationale for managing safety and security risks, and make clear links to the organization's overall mission and mandate.
- Employers and employees are explicitly require to comply with the organization's safety and security policies and procedures.
- Safety and security policies specifying the above key actions are set in place in a written form and understood among all staff members including Headquarters and field locations.
- Regular reviews of safety and security policies as well as reviews after critical incidents with participation of all relevant staff members are made.

**Guidance Notes:**

1. **Definition of Safety and Security**: The "safety" refers "freedom from risk or harm as a result of unintentional act, such as accidents, natural phenomenon or illness" whereas "security" refers "freedom from risk or harm resulting from violence or other intentional acts". [6] While ensuring the security of staff, assets and programmes from 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 disease, HIV and other health threats, mental health, natural disasters such as floods and earthquakes also pose significant threats to aid workers.

2. **Organization's Mission, Mandate and Values**: It is important to include the organization's mission and mandate statement and values in the security policies since it is important for all staff to understand the nature of the organization that they are working for. It is important for the organization's managers to understand that these mission, mandate and values impact on the threats and risks that the staff face in the field.[7]

[6] Humanitarian Practice Network (2010), Operational Security Management in Violent Environment, Good Practice Review Number 8 (New Edition), p.xvii.

[7] See MercyCorps (2011), Field Security Manual, "Impact of Agency Mandate and Mission on Security" for more detailed explanations.

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

   - **Acceptance**: Building a safe operating environment through consent, approval and cooperation from individuals, communities and local authorities (EISF, 4:02).
   - **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 acceptance by far more appealing security strategy, and "acceptance can and should be the foundation of all security strategies".[8] 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 last resort strategy 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 abovementioned approaches. The point is that security management should be proactive, involving conscious choices about the mix of approaches pursed 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.[9]

Reference


- Humanitarian Practice Network (2010), Operational Security Management in Violent Environments, Good Practice Review Number 8 (New Edition), Chapter 3 Security Strategy.
- James Davis and Lisa Reilly (2015), Security to Go: A Risk Management Toolkit for Humanitarian Aid Agencies, European Interagency Security Forum, Module 4 Security Strategies: Acceptance Protection and Deterrence
- ECHO (2004), Generic Security Guide for Humanitarian Organizations, 2.3 Approaches to Security
- MercyCorps, 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. 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 appropriate SRA (See also Mitigation Measure in 2.3 Security Plan at Field). Contemporary

[8] GPR08, p.56.
[9] GPR08, p.56.

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.

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, SRA process should be considered as "an integral part of programme and project design" since "exposure to risk and mitigation measures are both linked to programme objectives and implementation".[10]

SRA can cover a "broad range of threats including violence, conflict, natural hazards, terrorism, health issues, political interference, crime and corruption" (EISF Guide, 3:02). SRA should include context and programme analysis, threat and vulnerability assessment, 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. SRA should be "inclusive, eliciting 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".[11]

Reference

- GPR08, Ch.2
- EISF Guide, Sec.3
- ECHO, 2.4

5. **Organization's Security Principles**: Following statements on principles relating to safety and security of organization's staff might be include in the organization's safety and security policies. Following list of principles are extracted from various safety and security policies of humanitarian organizations, and does not constitute an exhaustive list. The organization may select and include some of these principles in their safety and security policies according to its mission, mandate and mode of operations.

   - **Applicability of Safety and Security Policies**: Statement on who is covered under this policy. Are national/local staff covered? Are family members of expatriate and national/local staff covered? What about local volunteers, contract staff from other NGO, local government associates, consultants, interns, and/or guests? Since every member of the organization has collective responsibility for their own and team security, strong sense of ownership to 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 every member should behave as a positive representative for the organization.

[10] EISF Guide, 3:02.
[11] GPR08, p.28.

- **Responsibility for Security Management**: Statement on the operational responsibility for the security of staff [12] following the line management structure – overall, headquarters, regional, country and day-to-day management. (see also Standard 5: Accountability)
- **Responsibility for Safety and Security Policies**: Statement on who will develop the organization's safety and security policies, monitor policies implementation, and give permission for exemption. (see also Standard 5: Accountability)
- **Security Risk Management (SRM) Plan**: Statement on how SRM plan should be developed for each country/operation where the organization works, and such SRM plan should include an operational context and risk analysis (including threats and vulnerability assessment), and procedure for review and approval. (see also Standard 5: Accountability)
- **Priority of Human Life**: Statement on how the organization put the security of personnel higher priority than the protection of assets, including premises, vehicles, office equipment or programme materials.
- **Humanitarian Principles**: Statement on the organization's position on core humanitarian principles of humanity, neutrality, impartiality and operational independence.[13] Status with 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 the persons of concern to the organization, including implementing codes of conduct, training, complaints mechanisms and investigation. [14] (see also Standard 2.3: Security Plan at Field, Guidance Note 11)
- **Proportionate Risk**: Definition of 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.[15]
- **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 the policies accepts individual responsibility, on or off duty, for his/her personal security as well as the security of the other colleagues, programmes and the organization. (see also Standard 1: Commitment to Safety and Security)
- **Requirement for Security Incident and Situation Reporting**: Statement on 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,

[12] In this guidebook, the term "staff" means all the persons involved in any organisation's activities regardless to be paid or non-paid, for example, including full-time and part-time staff, specialists or consultants, temporary transferred employees, interns and volunteers.

[13] The first three principles are endorsed in General Assembly Resolution 46/182, passed in 1991. The fourth principle was added in 2004 under Resolution 58/114.

[14] See, CHS Alliance (July 2017): http://www.chsalliance.org/what-we-do/psea.

[15] See GPR08, Chapter 2 Risk Assessment.

monitoring and analysis of security trends, and to inform security risk assessments (SRA) and decision-making.[16]

- **Failure to Follow Safety and Security Guidelines**: Statement on disciplinary action against staff who do not follow safety and security guidelines or at in ways that put themselves or others at risk in both professional and personal behaviour 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 local security management plan that reflect 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. Procedure of approval, monitoring, 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 resource management procedures. (see also Guidance Note 5)
- **Coordination and Information Sharing**: Statement on the organization's position on coordination with other humanitarian agencies in managing security, especially on sharing security incident reports, participation into regular mechanism for sharing information. (see also Standard 6: Collaboration with Other Actors)
- **Respect of Local Law and Custom**: Statement on the organization's position on dealing with local law and custom, 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)
- **Gender, Ethnicity and Nationality**: Statement on how the organization deal 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)
- **Bribes, Gratuities and Gifts**: Statement on organization's position 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 receiving gratuities or gifts related to their roles or the performance of their duties for the organizations.
- **Kidnap and Abduction**: Statement on organization's response to kidnapping and abduction, position on ransoms for the release of kidnapped staff, support to

[16] See GPR08, Chapter 5 Incident Reporting and Critical Incident Management.

immediate family, and post-incident support to the kidnapped staff.[17] (see also Standard 2.3: Security Plan at Field, Guidance Note 14)

- **Right to Withdrawal**: Statement on rights 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, line of authorities to decide the withdrawal from and return to a programme area and country. (see also Standard 2.3: Security Plan at Field, Guidance Note 12)
- **Evacuation**: Statement on 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 at 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 armed personnel in *ad hoc* and extreme situations. The statement may also cover the organization's position on staff carrying arms while on duty, 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, multi-national and United Nations Peacekeeping Operations. (see also Standard 6: Collaboration with Other Actors)

Reference


- MercyCorps, Field Security Manual, March 2011
- Concern Worldwide Security Policy, April 2003
- Care International Safety and Security Principles, March 2007
- Irish Aid Guidelines for NGO Professional Safety and Security Risk Management, 2013
- People in Aid, Policy Guide and Template: Safety & Security, 2008
- Lutheran World Federation, LWF Safety and Security Policy, March 2016


[17] See GPR08, 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 in 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

- The organization's definition on three basic security approaches – acceptance, protection and deterrence
- The organization's approach to Security Risk Management (SRM)

### IV. Organization's Security Principles

- Explain 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 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 respond to a specific context to the location, 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 which do not have field locations or offices and travel to the fields when necessary. A security plan of such an organization should include both those described here for the headquarters and those described at 2.3 “Security Plan at Field” below as much as they are applicable to the organization. ”

**Key Actions:**

- Clarify relationship between the headquarters and field locations with respective responsibilities. Such responsibilities to be clarified include security risk assessment, security planning based on 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 headquarters. (Guidance Note 1)
- Have operational security procedures at the headquarters as well as those between the headquarters and field locations. Those 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. (Guidance Note 2)
- Have guideline for a situation, incident and accident reporting (format and frequency to be included). (Guidance Note 3)
- Have Critical Incident Management Plan (CIMPs) 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 with reference to CIMPs 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 the media relation for risk management and; post-incident management including mental and psychosocial support. (Guidance Note 4)
- Make regular reviews of a security plan as well as reviews after critical incidents with participation of all relevant staff members.

**Key Indicators:**

- Security plan for headquarters specifying the above key actions is set in place in a written form and understood among all the staff members including headquarters and filed locations.
- Regular reviews of a security plan as well as reviews after critical incidents with participation of all relevant staff members are made.

**Guidance Note:**

1. **Clarification of relationship between the headquarters and field locations with respective responsibilities. Actions and procedures to take according to the clarified responsibilities of headquarters:** It is vital that a relationship between the headquarters and field locations is clearly defined with respective responsibilities. Confusion and conflicts of responsibilities might possibly cause even a security risk even though both sides are making efforts to respond to the original security risk. In most of the 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, to whatever extent, both headquarters and field locations cooperate each other in making such assessment and planning. In most of the cases, responsibilities for daily security measures can be delegated to field locations as those at the field locations have better knowledge of the situation, so that they can make a better decision and can do so in a timely manner. On the other hand, the headquarters should be also responsible for intervening in field security measures in case there are possible or existing errors or mistakes by field locations. The headquarters are, in most of the cases, also responsible for monitoring and evaluation of project operations, which itself affects security and security management at field locations, as well as an organizational decision such as critical incident management, while in good consultation with field locations. There are also organizations which do not have field offices or Japanese staff members based in the field locations. In such cases, the headquarters might be more responsible for security measures than the cases where there are field offices or Japanese staff members based in the field. In all the cases, both sides should make efforts to build confidence in each other with good flow of information as well as human and financial resources. And it is necessary not only to clarify the extent of responsibilities but also to describe security risk assessment, security planning and measures and procedures to take according to the clarified responsibilities of 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 in the above. Those include the above illustrated key actions.

3. **Guideline for a situation, incident and accident reporting (including format and frequency):** Information is vital in order to take a necessary and appropriate security measure. It is thus necessary for the headquarters to receive information from a field location. In order to have enough information in quality and quantity and to follow the situation at a regular basis and in a timely manner, it is encouraged to have a guideline

(format and frequency) for a situation report at a regular basis and an incident report to respond to a specific situation.

4. **Critical Incident Management Plan (CIMPs):** An organization might possibly face a serious crisis such as:
   - Death or serious injury of a staff member
   - Forceful suspension of activities
   - Security situation and disaster affecting activities,
   - Any major change such as a relocation or evacuation.
   - Communications failure
   - Major fraud
   - Compensation claim against the organization arising out of a security incident
   - Any incident which has generated or is likely to generate media interest
   - Bomb and any other armed attack
   - Hostage taking
   - Kidnap and ransom demand

   In such a situation, it is necessary for the headquarters to make an organizational response to the situation as indicated in the above key actions in coordinating all the relevant sections, officers and staff members at the headquarters, field locations and any other offices.

Reference
- GPR08, Cha.5
- ECHO, 3, 8, 10 (partly, 5,6,7,9)

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

**I. Introduction**

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

**II. Relationship between the headquarters and field locations with respective responsibilities. Actions and procedures to take according to the clarified responsibilities of headquarters**

- 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 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. Guideline for a situation, incident and accident reporting (including Format and frequency)**

**V. Critical Incident Management Plan (CIMPs)**

- 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 with reference to CIMPs 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 the media relation for risk management
- Post-incident management including mental and psychosocial support.

**VI. Review of Security Plan**

## 2.3. Security Plan at Field

**Need for Individualized Security Plans at Field**

A security plan is based upon an individual organization's safety and security policies that reflects 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 SRA at the planned field location and establish 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 traveller may encounter and by talking to other humanitarian actors. Risk mitigating measures, CIMPs 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 responsibility 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 understands all aspects of the plan, and (3) 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. A security plan must be based on a SRA and address the identified threats. A security plan is based upon organization's safety and security policies, thus, each security plan to each organization should be differentiated at operating environment, based on 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 Security Risk Assessment (SRA) in the target area of your activities to identify any potential security risks and threats (Guidance Notes 1 and 2)
- Consider any potential risk mitigating measures addressing security risks as identified in SRA in line with safety and security policies (Guidance Note 3)
- Standard Operating Procedures (SOPs) outlines for daily operations and routines as they pertain to security including staff movement, communication, office and residence management, staff health, limitation of handling cash, implementation of contingency plans and external contacts. (Guidance Notes 5, 6, 7, 8, 9, 10 and 11)
- Organization chart 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. (Guidance Notes 12 and 13)
- Have Critical Incident Management Plans (CIMPs) that identifies 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. (Guidance Notes 3, 14 and 15)
- Guidance for staff's stress management including Rest and Recreation (R&R) should be mentioned. (see also Standard 4: Human Resource Management)
- Establish an incident and situation reporting system along with a form of those types of reporting including close liaison with headquarters.
- Make regular reviews of plans as well as reviews after critical incidents with participation of all relevant staff members.

**Key Indicators:**

- Security plan for field posts specifying the above key actions is set in place in a written form and understood among all the staff members including headquarters and filed locations.
- Regular reviews of plans as well as reviews after critical incidents with participation of all relevant staff members are made.

**Guidance Note:**

1. **Security Risk Assessment (SRA)**: Organizations normally carried 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 wide range of security related factors such as

potential threats in general and specific to aid organizations, vulnerability of your organization and mitigation measures. It is better to visit to the field for enough long to achieve its aim, however, it can be done by remote, if a visit is not possible. A SRA can be done solely or jointly with other organizations, and combined with other aims, for example a needs assessment. See more details at Good Practice Review (GPR8) Chapter 2 and ECHO A26 Security Assessment. (see also Standard 6: Collaboration with Other Actors)

2. **Information Gathering**: Security and safety related information gathering is very important factor to make a SRA successful as it is also important to build an own security network after starting activities. In many cases, embassies and foreign governmental agencies provide security notice and host government also share important security matters and other contextual backgrounds. For example, many US embassies and British embassies are providing security related information from their websites, and the Japanese government in its web page provide security information for travellers, in addition, by registering to Tabi-Regi anyone can be eligible to security notice from the local embassy. In many countries, humanitarian and development actors including NGOs, UNs and bilateral agencies has mechanisms to share security information including past incidents occurred in projects. Apart from the government and NGOs, you can contact security consulting organizations notably RedR and Safer edge, and security firms offer security services including guards, vehicle escort and consulting. Some insurance firms have security risk and threats information and consulting services in some areas of the world. In addition to continuous efforts to collecting information from international/national media, it is highly recommended to gathering information from local government, and local communities in the area of activity. It is important to note that organizations should have various information resources and contact channels to collect enough information to make an appropriate determination on security situation. See more details for security network at Standard 6: Collaboration with other Actors.

3. **Mitigation Measures**: Mitigation measure is 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/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 take account that there would be unique security risks for national/local staff and female staff, and prepare appropriate mitigation measures (see also Standard 4: Human Resource). See more details at GPR8 Chapter 2.7 on mitigation measures, Standard 4 Human Resources on consideration to national/local and female staff, and Standard 7 Safety and Security of Local Partner Organizations on involvement of local partner organizations.

4. **Critical Incident Management Plans (CIMPs) and Critical Incident Management Team (CIMT)**: In order to respond to a critical incident an organization should develop both a

CIMPs and a CIMT. CIMPs should take consideration of 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. 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 field level, but there needs to be a clear understanding of when to bring in the headquarters levels 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. CIMT's decisions include suspension of activities, personnel withdrawal, set certain level of confidentiality, and the end-state objective (injured person evacuated, body repatriated, kidnapped staff member released). CIMT member are consist with representative of the organization, mangers, communications in both headquarters and field level. Communication with authorities, media, donors, staff family is very important as well as the CIMT is required to manage administrative, legal and financial consideration especially the people affected by incident needing appropriate psychological supports. After the incidents, the staff members involved in an incident should have debriefing and counselling if necessary. An after-action review should be standard practice. See more details at GPR8 Chapter 5.

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 practice is 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 organizations. 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 help you to strengthen security if properly used. 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 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 interview requires certain set of skills (answering to 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 response through the media in order to avoid the spread of biased information and exaggerated rumours. Organizations' managers should therefore be aware of media reporting, and able to deal with the media effectively when appropriate. Provide media training is essential.

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 organizations 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 organization can also make them an ideal target for criminal groups. All organization's vehicles, including rental vehicles, are advised to 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, hotels/guest houses for temporary lodging of staff visitors with appropriate safety and security equipment in prior to project implementation. Site management includes: physical conditions and strength of the building; examine the boundaries of the site making sure perimeter walls are secure; ensure all doors, gate and windows have adequate locks; access points and the street area outside is well light; consider possible escape route; consider vehicle parking and assembly area. The office also should have effective controls and procedures in place to manage access. For field offices in high risk environment, 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 the field operations, particularly in insecure environment, 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 large 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. 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 time. Every offices in 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 capacity for electronic payment to local businesses.

11. **Sexual Aggression**: In any area, sexual harassment/assault is incompatible with providing a safe and secure working environment and as such is 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 all staff know and comply with them. Organizations will investigate all sexual harassment complaints in accordance with organization's policies and procedures. Female staff should receive a briefing on sexual aggression immediately upon hire. If there is a security concern for the female staff, organizations should consider upgrading the accommodations, arrange a share house for female staff members, by taking consideration of 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 Annex 20 for a suggested Medevac procedure.

13. **Suspension or Hibernation of Project, Relocation or Reduction of Staff**: Suspension or hibernation of project, relocation or reduction of staff have recently been used as measures to mitigate the security risk in insecure environment. It may be necessary in order to allow time for reflection on a changed security situation. It may also be used in order 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 it becomes necessary to suspend activities. 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 numbers 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 environment. 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. Too many security plans only consider evacuation, neglect the relocation option and fail to consider hibernation. 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?; regional office can make decisions by themselves?; who have the authority after the withdraw?; Is it clear to all staff that the decisions taken by management are mandatory?. It is highly important to set evacuation in 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 resource management. It is encouraged to consult beforehand regarding measures related to evacuation with national/locoal 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 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. Address 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, Somalia, Darfur (Sudan), Afghanistan and Pakistan. 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: avoid routines; reduce visibility; in-country vetting of personnel; remove potential vulnerabilities; site protection; heightened awareness and counter-surveillance; seek local support protection; armed protection and 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 situation. Generally speaking, kidnap 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.).

**Column 1: Low-Profile Approach**

Low-visibility programming has become an increasingly common protective tactic among aid organizations. 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 antenna. 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 Vehicle**

Whether aid agencies should use armoured vehicles in high security field or not is a decade long discussion due to organizations having differences in approaches to take account for security concerns. "Generic Security Guide", produced by Directorate-General for European Civil Protection and Humanitarian Aid Operation (ECHO) under the European Commission has suggested that armoured vehicles are 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 have a careful consideration when to use, for what purpose and for how long of a period. (ECHO 4.10 Technical Issues (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 organization mission, mandate, principles and safety and security policies
- Summary of the situation (political, economic, historical, military, etc.)

### III. Security Risk Assessment (SRA)

- Threat assessment (indicating most likely types of threats NGOs will face)
- Mitigation Measures (list 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 Plans (CIMPs)

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

## 3. 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 risk analysis.*

### Key Actions:

- Maintain 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 cost and budget for local partner organization when necessary. (Guidance Notes 2 and 3)
- Revise the original project plan and avoid posing intolerable risks and overcapacity situation to staff members, in case sufficient resources are not available for appropriate safety and security management (Guidance Note 4).
- Make advocacy as NGO Community to change donor policy for funding on safety and security measures, when appropriate expenses are not covered (Guidance Note 4).

### Key Indicators:

- Organizations have a procedure to share the result of security risk analysis with all relevant sections/persons in charge for budget planning.
- Organizations allocate sufficient budget for staffing in terms of its numbers, salary with benefit and working environment, including that for local partner organizations.
- Organizations secure expenses for project cycle design such as research/assessment, stakeholder engagement, networking with other humanitarian/ 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 cycle(Refer to Standard 7 for guidance).
- Organizations secure financial and human resources sufficient for internal and external security training and human development including that for local partner organizations.
- Organizations take open policy for sharing security cost with other NGOs to pursue scale merit and cost effectiveness, i.e. security advisors, offices, special type of vehicle, evacuation etc.
- Organizations work with NGO networks for donor advocacy if they face with the cases where funding request for appropriate security related expense is not admitted by a donor.
- Stakeholders for project implementation of NGOs can be supposed as local authority, non-state actors, local leaders, local community, local NGOs, local partners/staff, international NGOs, UN and governmental organizations.

**Guidance Note:**

1. **Resources to Meet the Standards - A Challenge for Japanes NGOs**: Based on the security risk analysis, organizations inevitably need to take some mitigation measures and this in turn require appropriate financial, human and other recourses. However, this Standard may be one of the greatest challenges for Japanes NGOs in comparison with those of U.S. and Europe, and some deliberate and innovative approaches as NGO community are expected to fill the gap between the demand and supply 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 resource management and collaboration with other humanitarian/development actors, the planning requires not only the expenses for facility and equipment but the other resources like personnel as well as stakeholder engagement to fulfil all the safety and security standards.

   - In some organizations, budget are planned independently by persons of admin or finance section and security measures to be taken both at headquarters and field levels may not be properly reflected in the budget. To avoid such practice, organizations should have procedure to share the result of security risk analysis with all relevant persons or conduct analysis involving all the persons concerned with budget planning.
   - The cost for research/assessment and stakeholder engagement including local community is an essential part for NGO security in terms of “acceptance” strategy. Thus the resource should be planned in advance when forming a project.
   - The resources for collaboration with other humanitarian/development actors need to be put aside as administrative/overhead cost, which is essential as 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 resources to take necessary security measures.

3. **Budget Designing**: For NGOs that utilize government or UN funding, some security related cost 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, participation in humanitarian/development security networks should be in budget designing as administrative/overhead cost.

   - For the information on supporting program for external security training, a list is attached as Reference 3-I.
   - Organizations should share information with NGO community on line item coverage of safety and security related expenses by donors to set standard practice for NGO community and the donors. As Reference 3-II, a list is attached for security related expenses that can be included in line items by major Japanese donors.
   - Cost share is an option to lower the security expenses. It can be shared by joining an existing security network of NGOs active in the field or forming ad hoc consortium in

response to certain crises. The examples of the expenses are as follows; 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 as 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. In case it is mainly on account of the donor policy of funding for security expenses, organizations should make voices as community to raise awareness and change the policy of donors (See also Standard 6 Collaboration with Other Actors).

   - Organizations are aware that project implementation without sufficient resources for safety and security can pose intolerable risks and overcapacity to their staff members.
   - Organizations should work on advocacy for donors that costs of security measures 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 SRM and Safety in the Field workshop both once or twice in Thailand, along with other variety of workshops.
- Currently In 2017, eCentre hosts a SRM, training of trainers for SRM and SIF in Japan
- Cost for training, travel and accommodation will be totally covered by eCentre.
- As eCentre's mission is capacity building for emergency preparedness of UN, G.O. and NGO personnel in Asia/Pacific, participants should be basically stationed in Asia/Pacific. The allocated seats for Japanese NGOs are usually 2-3 for each workshop and participants are selected from a long list of applicants. However, including those stationed outside of Asia/Pacific, applicants were accepted as substitutes to fill vacancy in some cases.
- Workshop information can be obtained from UNHCR Tokyo Office as well as on the web site of JaNISS.

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

- The program is offered by NGO division of Ministry of Foreign Affairs (MOFA) to support NGOs to send its staff members overseas to get training for the purpose of capacity building of Japanese NGOs through human resource development by. MOFA entrusts the secretariat of the program to a third party (it is JANIC in 2017), and it announces the call for proposal usually 2-3 times in a fiscal year.
- Though its guideline states that a training should be more than a month, shorter period training were approved for security training in practice(e.g. a week security training by European/U.S. training provider).

- 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 web site of MOFA.

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

- JaNISS hosts SRM and PSF in Japan and overseas on ad hoc basis.
- Basically, participant are supposed to cover a part of training cost. Travel and accommodation cost can be covered by JaNISS depending on funding situation.
- Information can be obtained on the web site of JaNISS.

4. Japan Platform (JPF)

- Depending on programme, external training cost can be included in line item of a project budget, if the need is approved by the secretariat.
- When approved, external training cost can be covered for international and national/local staff members as well as those of partner organization.
- For staff members at headquarters level, the training cost will be approved when the need for training such as travel to the field is acknowledged.
- When an appropriate training is not available in a country where the office is located, travel 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 revised on March 17th 2017)

- Insurance: War-premium insurance can be included in “insurance expense” and insurance for evacuation in “security and labour safety expenses”.
- Visa: Visa issuance fee for a third country for evacuation can be included in “visa expense”.
- Office facility: Security related facility cost can be included in “field post set-up expenses” or “security and safety expenses”..
- Office equipment: Security related equipment can be included in “security and 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 the personnel cost including employer coverage part of legally regulated social benefit can be included in personnel expenses, under the limit of JPF personnel expense standard. Personnel cost for security managers and security officers can be also included.
- Security training expenses: In some programs, security training expenses can be included in budget (refer to Article 4.of Reference 3-II above).
- Guard and other security related expenses: Guard cost and other security related cost can be included in “security and labour safety expenses”.

- General administrative expenses: As general administrative expenses, 5 % of field expenditure can be allocated but submit of documented evidence is required.

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: 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 position can be included. However, employer coverage part of legally regulated social benefit 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 benefit including employer coverage part can be included. They can be approved within the limitation rate for MOFA’s standard both for international and local. The salary for the paid holidays can NOT be included for both. l.
- Travel to headquarters during project period and rest and recreation(R&R): The cost for travel between the field and headquarters can be approved for only once during a project period. The cost for travel to headquarters for meetings and rest during project period, as well as R&R in a third county cannot be approved.
- Security training: Security training expenses cannot be included .However, for the security training and exercise provided by Japan International Cooperation Agency(JICA), the travel expenses for the venue(s) can be included both in Japan and in a country of activities, only for one person with Japan’s nationality, once in one project for each, if the person has not participated in the training before.
- Guard and other security measure item: Guard cost and other security related cost can be included in “expenses for other security measures”.
- General administrative expenses: As general administrative expenses, 5 % of field expenditure can be allocated but submit of documented evidence is required. No direct cost for the project (e.g. legally regulated social benefit cost for the project staff) can NOT be included here.

## Standard 4: Human Resources Management

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

Organizations work on hiring and sustaining qualified staff and demonstrate their duty of care for sustainable organizations, through proper orientation, training, insurance and support. Organizations shall have policies and procedures in place that include national/local staff into the organizations risk management systems and address national/local staff's unique security concerns.

### Key Actions:

- Have Human Resource rules that include clear Terms of Reference (TOR) and responsibility for all positions, and all positions have responsibility of security management.
- Have policies for the safety and security, which include stress management, training for security issue and insurance, and the well-being of all the staff including both international and local staff.
- Special attention is paid to the unique issues of international staff, who can be exposed to external threats as well as stress and sickness.
- Special attention is paid to the unique issues of national/local staff that is different from international staff in many cases, and the policies and plan for the safety and security is translated into local language.

### Key Indicators:

- Written policies are available to staff on safety and security, individual health, care and support, ToR explicitly stating responsibility, and program plans including written assessment of security, travel and health risks specific to the country of region .
- Above mentioned policies are reviewed in regular basis.
- All levels of staff are trained for assessing threat to organization, awareness of world trends affecting the security of humanitarian/development organizations, handling media and caring family during security incidents, and personal security management in the field.

**Guidance Note:**

1. **Pre- assignment briefing**: Before international assignment, organizations are responsible that all staff receive verbal and written briefing on all risks relevant to the role to be undertaken, and the measure in place to mitigate those risks, including insurance. It is important that chain of command regarding the security is clear for all staff so that the communication flow between headquarters and field office smoothly.

See CHS for more details of general aspect of human resource management (also see Standard 1: Guidance note 7).

2. **Stress Management**: Managing stress is not only the individual responsibility, but also the organizational responsibility. Organizations should be aware that more staff experience stress than security threats, and their 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 the staff to the high pressure area, they are required to receive the 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 conceived differently in some culture, and organizations should be aware that national/local staff may have a different approach 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, preventative health advice, active support to work reasonable hours and access to psychological support when required. Managers can promote a duty of care through modelling good practice and personally complying with policy. Aid workers also need to take personal responsibility for managing their 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**: Organization's security policy and plan should include staff's family care and support during critical incidents.

6. **Evacuation etc.**: Staff policy regarding relocation and evacuation is clearly communicated to all staff in advance. International staffs need to understand that they should follow the decision of organization's evacuation, while the individual staffs has the right to request to withdraw from the risky area when they feel insecure.

7. **Providing Security Risk Management (SRM) training opportunities**: The 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 the individuals may be expected to assume. Leaning from other agencies and networks is also important as well as utilizing experienced staff as trainers, briefers, advisers, and evaluation.

8. **Insurance**: All staff is covered by appropriate insurance, and war risk coverage when assigned to high-risk countries. For staff members employed in Japan, it is regulated by Act on Industrial Accident Compensation Insurance that an employer should enrol its employees in this insurance to compensate for injury, disease, disability and death during work and commutation. Organizations must be aware that for accidents while an employee being deployed and stationed at field office(not just for travel), prior procedures for special enrolment is necessary for the insurance coverage(For more details, refer to the web site of Ministry of Health, Labour and Welfare).. Most field staff requires insurance cover; need to have appropriate 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 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 reference should be consulted and it is a way to start with short-term contract in new environment and in a hurry.

10. **Special care for national/local staff:** It is mandatory that national/ local staff is involved in the formulation, review and implementation of security and safety policies and plans; to make sure that their culture is considered. National/local staff should be explained of organization's rules and regulations on human resources in their languages. Their TORs, evacuation plans and crisis management should be also explained. Staff assignment and recruitment require consideration for balanced team composition in respect to local culture and custom. Local staff, on the one hand, has better understandings of the social, cultural and political environment in the field and better access to local network which helps to gather information from local context, but on the other hand, may face various pressures from other actors in society as belonging to the society that should also be taken account of.

<u>Reference:</u>

- CHS (Commitment 8) / people in aid code (principle seven: health, Safety &Security)
- ECHO 12 Generic Security Guide Annex R&R, and STRESS
- GPR8 Operational Security Management in Violent Environments

## Standard 5: Accountability

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

Setting standards for security and safety will be more likely to be sustained if there are good accountable structure are in place with clear lines of responsibility related with 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 fulfilling its duty of care obligations.

**Key Actions:**

- Create an accountable structures based on respective organization's safety and security policies and plans (Standard 2) both at field and headquarter levels, regardless of size of the organization (Guidance Note 1).
- Define the security responsibilities and specific decision-making roles that each of these positions should have in respective staff member's job descriptions (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 lead on developing and implementing the security managment framework (Guidance Note 1).
- Organize briefing/induction sessions on organization's mission and values, security roles and responsibilities to staff members at all levels both at field and headquarters (Guidance Note 2).
- Conduct periodic organizational security review including evaluations of both employees and the management (Guidance Note 3).
- Establish procedure to address non-compliance and violation of safety and security policies and procedures and known by staff members at all levels (Guidance Note 3)

**Key Indicators:**

- Reporting lines for authroity and decision making are clearly established and staff understood to whom they are accountable.
- All staff with security responsibilities has their duties clearly articulated in their job descriptions.
- Staff at all levels within the organization, from the governing bodies to the individual staff member, share a collective responsibility for safety and security.
- Security focal point and/or working group is in place and functional.
- Security roles and responsibilities are incorporated into respective organization's performance review.
- Staff members comply with respective organization's safety and security management policies and 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 management line.

   Therefore, it is necessary to identify existing positions with critical role in staff security and safety, including managers based at field and headquarters. Furthermore, define the security responsibilities and specific decision-making roles that each of these positions should have in respective staff member's job descriptions. Their security responsibilities should be included in the organization's safety and security policies so that all staff member are informed.[18]

   Many organizations appoint individual staff or 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 management line if required. The advantage of appointing group of staff representing different roles and levels within the organization is to bring a wide range of experiences and perspectives, and encourage 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 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" in the following page).

[18] For concrete examples of security responsibilities, see Chapter 6 of Humanitarian Practice Network (2010, new edition) Operational Security Management in Violent Environments: Good Practice Review, Care International Safety and Security Principles (2007), and Mercy Corps Field Security Manual (2011).

When identifying specific security roles and responsibilities, it is necessary to be realistic for respective 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 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 treat security as a staff-wide priority, not a sensitive management issues to be discussed only by a few staff members behind closed doors. For example, following considerations could be useful to develop a culture of security in the organization:
   - Make sure that all staff are familiar with the context, the risk and the 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.
   - Advice and assist staff to address their medical, financial and personal insurance matters prior to development in 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 involving 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 it with them in an interactive way. Furthermore, periodically bringing 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 very important to remind every member that they should behave as a positive representative for 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**: following activities may contribute to enhance organization's accountability for security.

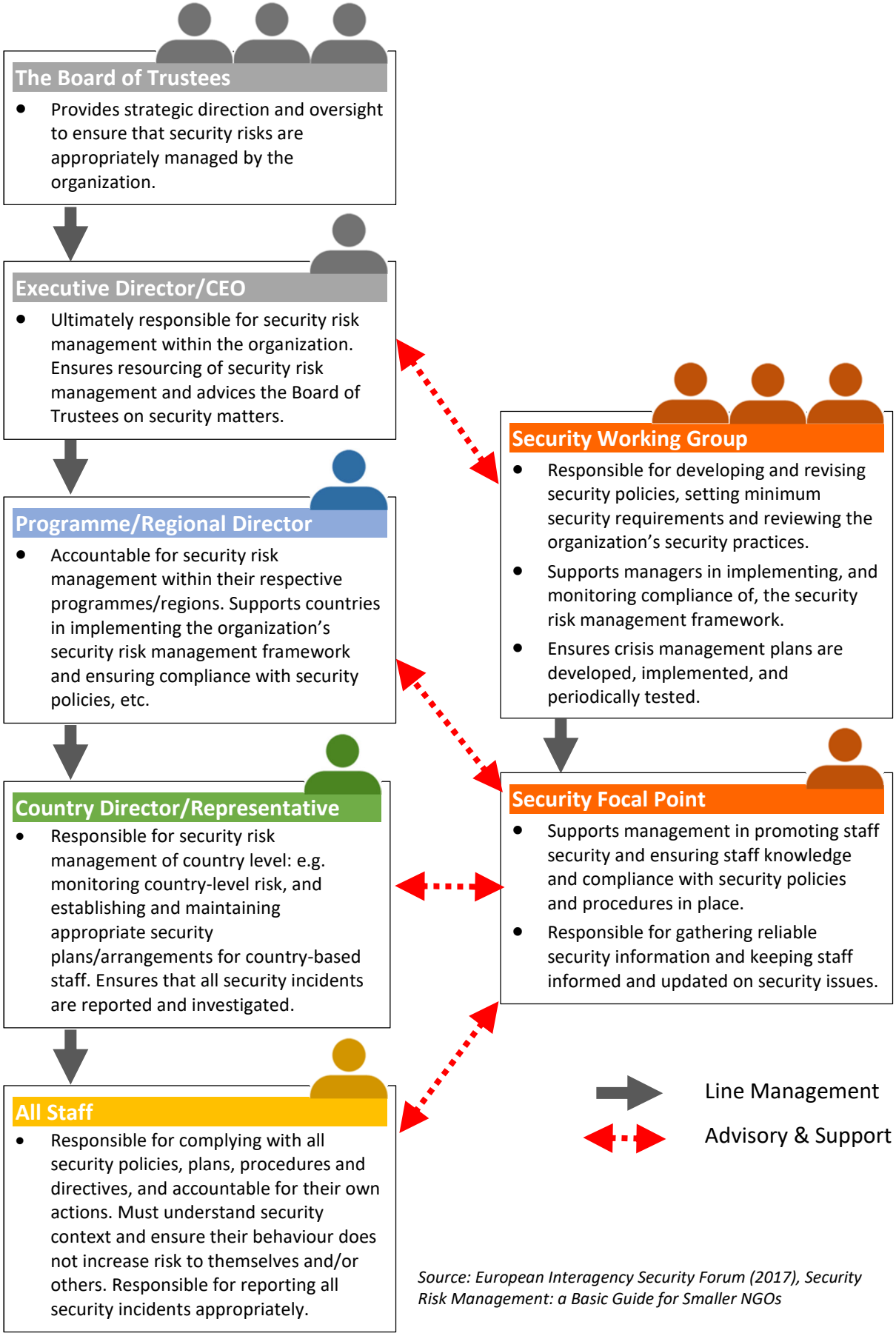
- **Periodical security briefings and drills** will enhance staff members' knowledge of lines of responsibility and authority. Outcomes of drills will help review organizational effectiveness of management systems and structures (lines of responsibility, human resources, technology, procurement, etc.).
- All staff with security responsibilities must have their duties clearly articulated in their **job description**[19], 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 resource policy. Procedure to address non-compliance and violation of established safety and security policies and procedures should be in place and known by staff members at all levels.

**Reference:**

- GPR08, 1.2
- EISF Guide, Standards 2 & 5
- Security Risk Management – NGO Approach
- Security Risk Management: a basic guide for smaller NGO, Chapter 3

[19] For concrete examples of job descriptions of staff with security responsibilities, see Care International Safety and Security Principles (2007), and Mercy Corps Field Security Manual (2011).

## Reference 5-I: Example Structure and Responsibilities




*Source: European Interagency Security Forum (2017), Security Risk Management: a Basic Guide for Smaller NGOs*

## 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-centered, 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 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 /development community for safety and security within the organization. (Guidance Note 1)
- Both headquarters and field offices need to participate in their located humanitarian /development community in order to cooperate for safety and security. Headquarters and field offices should share such cooperation interest within the organization. (Guidance Notes 2 and 4)
- Actively participate in security fora organized by NGO and/or UN at the levels of headquarters and/or field offices. (Guidance Notes 3 and 4)
- Appoint a staff responsible (security focal) to identify and participate in security fora. The appointed person will be responsible for the security management. (Guidance Note 3)

### Key Indicators

- Staff in the headquarters and field operations is provided with adequate information of the members in the humanitarian / development community and about joint security initiatives.
- Official / non-official personal relationship increases the exchange of security information from reliable source.
- The organization has a written list of security fora.
- The responsibility is clearly stated in job descriptions for the person in charge to be an active part within the security fora.
- Financial and human resources are secured to take action with collaboration.

**Guidance Note:**

1. **Advantages of Collaboration**: Some of the advantages for collaboration include:
   - A better alert system: Agencies can receive a fuller picture of actual or possible

security threats or alerts in their environment, which would increase the chances of avoiding an incident (such as, use of a 'communications tree' for wireless radios, walkie-talkies, and satellite phones, etc.).

- Better SRA: To have a shared record of all incidents in an operating environment has 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 makes it possible to collaborate in a more structured way.
- Cost-effective extra capacity services: Rather than each agency individually covering the costs of bringing in or hiring specialists, for example, the costs for training on security can be shared.
- Liaison with the authorities: Rather than negotiating individually, agencies can make a stronger and more consistent case together. This would include military actors to exchange information.
- 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.
- Operations of and/or conduct of one organization can impact the security of other members of the humanitarian community. It will make a difference actively seeking to minimize all the negative impacts one organization's operations have on others.

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 analysis, 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 into Security Fora**: There are many security related fora in both headquarters and field offices levels. Participation into these security fora 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 the security fora to gather information and to identify good practices for the particular operation. Security fora are usually chaired by one organization and attended by security focal persons.

   When appointing a staff member to attend the coordination meetings, ensure the staff is supported in dedicating time as a priority as well as being 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 initiative with other agencies to collaborate for holding a meeting. Security fora are useful mechanisms for improving organization's understanding on the current international standards related to security management, and improve the awareness on security management for small NGOs. Security fora can also share the costs of organizing training for staff, and act as a

coordination point with other actors such as United Nations Department of Safety and Security (UNDSS).

When, in an organization's view it is appropriate, it can participate in "Saving Lives Together (SLT)" [20], which is a framework aimed at enhancing UN and NGO security collaboration in the 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 remains the responsibility of the respective organizations.

4. **Source 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:
   - National governments, including donor governments and their embassies;
   - Host government departments;
   - Insurance providers – often have a threat advisory service linked to various countries and/or 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:**

- Saving Lives Together
- Good Review Practice 8
- InterAction's MOSS Revision and Guidance 2015
- Mercy Corps Field Security Manual – 2011
- Care International Safety and Security Principles, 2007

[20] See, "Saving Lives Together, A Review of Security Collaboration between the United Nations and Humanitarian Actors on the Ground (2010)" and Inter-Agency Standing Committee (IASC), "Saving Lives Together: A Framework for Improving Security Arrangements Among IGOs, NGOs and UN in the Field, October 2015".

## 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 ways that they can agree, reducing possible security risks as much as possible (Guidance Notes 1 and 2).
- Agree on concrete responsibilities and roles at emergency, as well as to the usual security measures, and share them among related actors (Guidance Notes 3 and 4).
- Secure necessary training, briefing, equipping, and funding necessary for security to staff of the 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 risks measures to be taken. It should be also written in the memorandum of understanding (MOU) as well.
- Close and smooth commination with local partners is ensured. If necessary, the budget for consultations in the 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, training opportunities, and to ensure the budget of equipment and materials necessary for security and crime prevention measures.

### Guidance Note

1. **Security measures when implementing partner project**: Partnerships with local partner organizations are effective methods in implementing projects. However, in particular, since Japanese NGOs cannot directly conduct projects in countries or regions with high security risks (restrictions are imposed by donors and governments). When considering cooperative projects in countries or regions with poor security situation, organizations should not just transfer any possible risks to local partner organizations but to consider any security concerns and measures to be taken. In addition to above, organizations should also 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 and responses to the security risks they may encounter. Also the acceptance in the local society differs among them. Thus, details of the safety and security policies may also be different. Under this understanding, project shall be implemented accordingly.

- Regardless of security problems in particular, there are cases to implement project by partnership with local partner organizations only through business trips and remote management. Even so, as there is always a possibility of getting involved in general crimes, diseases, accidents, etc. Therefore organizations should endeavour to achieve the six Standards for safety and security.
- When conducting a project through remote management without locating international staff in the field, not only risk countermeasures at the time of business trip but also security measures local partner organizations may confront in implementation of daily work shall be examined and agreed upon by both organizations.
- When the project is remote controlled completely, and there is even 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 regions/countries) and enforce to take any security measures.

2. Points to include in the agreement:
   - Visibility: Depending on the situation, organizations may refrain from using logos and signs of donors, self-organizations and local partner organizations.
   - Right to make a decision on security issue at local area: Clarify the responsibility of representative and appropriately give decisions on the site.
   - Public relations activities as an organization: If there is a fight between ethnic groups or religion groups, organizations should be aware that public relations activity may interfere activities of those groups. Also when publishing something on SNS which could see the movement of international staff, organizations should pay a special attention to languages, places, timing etc. with the security manner. Method and frequency of monitoring, and reporting.
   - Method and frequency of monitoring and reporting.
   - How to handle SOPs and security plan by both groups should be clarified (including emergency contact list), so that the latest information can be shared among groups.
   - At emergency: Clarify about the criteria for withdrawal/suspension judgment, and the correspondence such as how to settle expenses in that case.

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 the project implementations. It is also important to exchange opinions directly with staff of local partner organizations through business trips and on-site visits as well as usual communication with 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 staff of local partner organization in different region/country.

4. **Security Measures on Evacuation**: When the project is suspended temporarily or the process is terminated in the middle due to deterioration of the security situation, organizations should take appropriate measures not only staff of the own organization but also staff of the local partner organization as well. Even in the case where only organizations group evacuates and the project is continued with the local partner team staying, it is important to consider any possible security risks and take countermeasures.

**References:**

- ECHO Generic Security Guide 4.5 (i)
- InterAction Minimum Operating Security Standards
- OCHA Policy and Studies Series 2011, Section 5

## References


- CHS Alliance, Group URD and the Sphere Project (2014) Core Humanitarian Standard on Quality and Accountability
- Care International (2007) Safety and Security Principles
- Concern Worldwide (2013) Security Policy
- ECHO (2004), Generic Security Guide for Humanitarian Organizations
- EISF (2017) Security to go: a risk management toolkit for humanitarian aid agencies
- European Interagency Security Forum (EISF). (2017) Security Risk Management: A Basic Guide for Smaller NGOs
- Humanitarian Practice Network (2010), Operational Security Management in Violent Environments, Good Practice Review Number 8 (New Edition)
- Hoppe, K. & Williamson, C. (2016). Dennis vs Norwegian Refugee Council: Implications for Duty of Care. Humanitarian Practise Network (HPN).
- InterAction (2015) Minimum Operating Security Standards (MOSS)
- InterAction Security Unit (2007) Security Risk Management – NGO Approach
- IFRC (2011) Stay safe: The International Federation's guide for security managers, Third Edition.
- IASC (2011) Saving Lives Together: A Framework for Improving Security Arrangements among IGOs, NGOs and the UN in the Field
- Irish Aid. (2013) Irish Aid Guidelines for NGO Professional Safety and Security Risk Management.
- James Davis and Lisa Reilly (2015), Security to Go: A Risk Management Toolkit for Humanitarian Aid Agencies, European Interagency Security Forum
- Kemp, E. & Merkelbach, M. (2016). Duty of Care: A review of the Dennis v Norwegian Refugee Council ruling and its implications. European Interagency Security Forum (EISF).
- Lutheran World Federation (2016) LWF Safety and Security Policy
- MercyCorps. (2011) Field Security Manual
- OCHA (2011) To Stay and Deliver: Good practice for humanitarians in complex security environments. Policy and Studies Series 2011.
- OCHA, NRC and JSIC (2016) Presence and Proximity to Stay and Deliver: Five Years on.
- People in Aid (2008) Policy Guide and Template: Safety & Security