U.S. RESETTLEMENT AGENCY
SAFETY & SECURITY
FORUM

(Insert Logo)

Date:
Authored by:
Approved by:
Date of next review:

Generic Safety and Security Management Plan

1.Introduction

1.1 Purpose of the Plan

This plan is intended to:

1.1.2 Ensure that a coherent SSMP is put in place by ***insert organization*** to mitigate risks for its staff, assets, and clients (during the delivery of services) in accordance with ***insert organization*** *S*afety and Security Management Policies.

1.1.3 Ensure that all staff and visitors have a clear understanding of their individual safety and security responsibilities relating to both daily operational safety and emergency response.

1.1.4 Provide guidance and a framework for the generation of context specific Safety and Security Management Plans not covered in this document.

1.2 Distribution

This plan, or portions thereof as determined by the CEO is to be disseminated to the following:

insert organization all staff, and/or leadership, visitors, and clients.

1.3 Locations covered

This Security Plan covers all areas within which ***insert organization*** has operations. For multiple field sites, the plan should be adapted based on a contextualized risk assessment.

1.4 Review

1.5.1 Safety and Security Management Plan and its components including: Policy statements, Standard Operating Procedures (SOP), Appendices, Contingency Plans, and Annexes, constitute the ____________Safety and Security Management Plan.
1.5.2 These documents are to be considered 'living documents' and thus will be reviewed in case of contextual change. The Safety and Security and Field Office Plans should be reviewed at least every six months.
1.5.3 The review and revision process is to consider both strategic changes within broader context (as detailed in each of the plans) as well as any changes occurring in the local operational context. Attention should be paid to shifts affecting the NGO community and how this may impact the Security Risk Assessment Matrix.
It is recommended the review – particularly of the Risk Matrix - is performed through a participatory workshop with key staff.

1.6 Security Responsibilities

[Describe security responsibilities on Country and Field level – CD/DCD, SA, CAM, other]

2. Contextual Analysis

2.1 Scope of services

[Describe briefly historic of the program in the country and its current presence]

2.2 Threat analysis

[Describe briefly country security environment with focus on the main threats related to NGOs presence in the area]

3. General Security Policies

Below thematic policies should be based upon the Global Security Policy and transposed into the Country Plan, explaining how effectively it applies on the country level.

3.1 Arms & Armed/Uniformed Persons

[to be completed by the CO]

3.2 Armed Guards / Escorts

(an example of what can be a country specific assessment)

In the case of Somalia, the use of armed guards is authorized as per specific SRA (and in many occasions mandatory), contingent on the profile of the staffer and the specific location. At the time of reviewing this security plan, it is assessed that armed guards are necessary for international staff in South Central Somalia, Puntland (except Garowe town) and Eastern Somaliland, in order to mitigate the risk of kidnapping for ransom and/or political violence. In addition, armed escorts may be imposed or strongly recommended by Local Authorities all across Somaliland and Puntland. Such cases where the justification is not due to violence threats but imposition by authorities, compliance with the local norms must be discussed with the CD. See more details for the specific locations in the Field Security Plans. When used, the armed escort must travel in a separate vehicle.

3.3 Contact with Parties to the Conflict

[to be completed by the CO]

3.4 Personal Protective Equipment (PPE)

[if relevant to the context as per local SRA]

3.5 Counter Surveillance

[to be completed by the CO]

3.6 Incident Reporting

[explain what need to be reported and summarize the procedure based upon the Internal Reporting Regulations]

3.7 IT & Data Security

[to be completed by the CO accordingly to the IT policy and local context]

3.8 Organisational Visibility

[to be completed by the CO explaining how this aspect has been implemented locally]

3.9 Vehicles

[accordingly to the local context describe modes of transportations authorized across the mission]

3.10 Driving

[precise who is authorized to drive INSO owned or rented vehicles]

3.11 Communications

[describe means of the communication used by the program and, if relevant, specific procedures, taking into account usual movements and field missions]

3.12 Premises

[describe briefly safety procedures put in place for the staff and visitors]

3.13 Insurance

[describe CO responsibilities with regard to the insurance of the staff, premises and assets]

3.14 Others CO polices

- Personal security,
- Curfew (if applicable),
- No-go or restricted areas (if applicable)
- Movement validation- field mission,
- Confidentiality and Media Handling,
- Photography

4. Security Phases

4.1 Security Phases

In order to adequately react to changing dynamics with a context, INSO utilises a phased response approach as a way of directing both individual and organisational behaviours, taking into consideration and balancing the needs between staff security and operational needs.

4.1.2 The 5 phases are [1] Normal Operations, [2] Restricted Movement, [3] Hibernation, [4] Temporary Relocation / Team downsizing, and [5] Evacuation.

4.1.3 The SA (or a person designated), will set and change the current security phase. Notably, any security phase may be set at any time. For the purposes of this plan relocation indicates an in-country displacement and evacuation marks a move out of country.

4.1.3 The specific responses provided are recommendations only and should be adapted to reflect the specific context and location they are being utilised in. In addition, security phases are not designed to be implemented sequentially nor are there any restrictions on time or space; rather they are to be implemented based on the assessment of prevailing circumstances and in the judgement of the responsible party.

4.2 Security Phase Matrix

The five security phases are as follows:

PHASE	DIRECTION	DESCRIPTION
Phase 1	Normal Operations	● Standard movement and operations protocol in the plan with no restrictions.
Phase 2	Restricted Movement	● Due to a prevailing unstable security environment movement is minimised to operationally essential movements only. ● Urban movement plans should be reviewed and routes rehearsed, prior to movement. ● It is advisable for the SA to review the threat environment, INSO vulnerabilities and to manage extant security risks appropriately. ● If continued deterioration to free of movement is likely/ expected SA will inventory: hibernation supplies, important travel documents, etc.

Phase 3	Hibernation	● All international staff members are restricted to INSO guesthouse upon identification of a short-term threat to INSO staff or facilities. ● Vital supplies (e.g. water, cooking fuel, food, heating) should be procured and stockpiled in advance. ● National staff will be restricted to home/office depending on nature of threat, location at time of hibernation order, and risks that may hamper their movement. ● Appropriate preparations should be made to continue work from home, if necessary/possible.
Phase 4	Relocation	● INSO international staff members (and relevant national staff) may relocate from office to guesthouse on order of SA in coordination with CD (DDO in CD's absence) upon identification of a long term direct or indirect threat to INSO staff or facilities in the office neighbourhood. SA will coordinate relocation once directed by the CD, together with the assistance of Admin where necessary.
Phase 5	Evacuation	● Evacuation will occur on order of CD in consultation with the SA on the ground. SA will coordinate relocation once directed by the CD, together with the assistance of the CAM where necessary.

N.B. The current security phase will be communicated to all staff whenever there is a change. The SA or SA designate will inform CD (and DCD) of any changes immediately.

N.B. The current security phase will be posted in the common areas of both the office and guesthouse flats. Relocation and Hibernation require movements and therefore will not need to be changed.

N.B. Specific to each phase communication plan may need to be applied on the CO level.

4.2.1 Potential triggers requiring changes to security posture in Afghanistan
[describe below elements (triggers) as per local context upon which a change within sec phases is necessary, an example can be:]

- Regular asymmetric attacks (increased events at an increasing rate/ increased tit for tat) that result in mass casualties.
- Regular asymmetric attacks (increased events at an increasing rate/ increased tit for tat) targeting competing non-state actors.
- Growing negative perceptions towards foreigners.
- Increasingly passionate protests with the potential escalation to violence or civil disorder.
- Exacerbated sectarian or political tension due to demographic changes.
- Catastrophic natural or manmade disaster.
- Military Coup

**** Note***

For Sections 5, 6, 7 of the CSP, please reference appendix, contingency plans, annex, and regional security plan folders in Operations Policy; Country Security Plan; on OneDrive

5. Standard Operating Procedures Appendices 1-20 (In Blue)

The purpose of the Afghanistan CSP SOPs is to provide simple step-by-step instructions for carrying out routine operations

Appendix 1 SOP: Guards

Appendix 2 SOP: Fire

Appendix 3 SOP: Drivers

Appendix 4 SOP:

6. Contingency Plans (CP) Appendices A-F (In Yellow)

The purpose of the Afghanistan CSP Contingency Plans is to provide a brief set of instructions on how to respond to an emergency.

Appendix 10 CP

Appendix

7. Annexes 1-20 (In Green)