1 Activity Security Template

1.1 Introduction

The purpose of the Activity Security Template (ASP) is to provide reassurance that the IP has a good working understanding of the environment it intends to conduct project activity in and, robust plans in place to implement mandated risk mitigation measures. Provided the ASP is presented in sufficient detail it will be ratified by the PIU Project Coordinator and project activity will be allowed to commence.

It must be stressed that the onus is on the IP to convince the PIU that it can operate in a safe and secure manner in, what is, one of the most extreme security environments in the world.

This document provides the template for all ASPs that must be followed by IPs wishing to undertake activity on the EA-RDIP. All IPs on award of contract will be issued a copy of this document and a copy of the Local Security Management Plans that are relevant to their proposed activity.

1.2 Local Security Management Plan

The Local Security Management Plan (SMP) is specific to a limited geographical area, within which a number of projects are conducted or is specific to an individual project, if that project is being conducted in isolation. The local SMP is tied to the local Security Risk Assessment (SRA), from which it derives all relevant threat scenarios and their risk levels.

The local SMP lists the threat scenarios and the mandated risk mitigation measures, to be adopted by IPs, for each threat scenario, within the geographical area concerned. IPs are required to pick from the SMP the threat scenarios that are relevant to their activities. Where possible, IPs are given a choice of mitigation measures to suit their operating model and will articulate which risk mitigation measures they intend to adopt in their ASP.

IPs found not in compliance with mandated risk mitigation measures and their own ASPs will be removed from the project.

1.3 .Description of IP Project activity including;

In this section provide detail on;

- *Locations of your proposed project activity (work sites, cash for works projects, etc), use mapping, be precise.*
- *Give approximate numbers of personnel and their categories, across the entire project and on each specific site, (understanding that these numbers may fluctuate)*
- *Detail specific activity on each site.*
- *Show locations of permanent infrastructure within project locations (offices, accommodation facilities) anything that can be associated to the project and is owned and operated by your organization.*
- Detail ad hoc locations used by your personnel regularly (hotels, etc).

1.4 Local Stakeholder mapping and access mapping

In this section provide detail on;

- All known local stakeholders pertinent to your project activity, provide a list including relevant contact information of individuals, their area of influence, and the reason they have an impact on your activity, include;

✓ *Friendly Security Actors - AMISOM, SNA, SPF, other national or local government security organizations. (Please note all known contact details of local commanders will be published in the Local SMPs for IPs to integrate into their ASPs, however IPs may have contact details within these organization that are not currently on the SMP)*
✓ *Clan Elders and Leaders*
✓ *Malign Actors (any and all personnel or organizations that may cause harm to your organization or the project)*
✓ *Known Private Security Companies in the area.*

- Your own internal access mapping, showing in detail those areas your organisation feels confident operating in and those it does not.

1.5 Movement Patterns

In this section you must look into your work plan in detail, understand what the likely movement patterns of your personnel are going to be in order to fulfil project activity and provide detail on these patterns. Specifically identify routes that will be used regularly (use mapping) and how often your personnel will be travelling along these routes and by which means of transport. The PIU will then assess if these patterns are likely to be discerned by malign actors through observation of your activity.

1.6 Identify Threat Scenarios relevant to the IP activity

Referring to the Local SMPs relevant to your proposed project locations, identify and list each threat scenario that is relevant to your activities, taking note of the mandated risk mitigation measures for each threat scenario. Provide a detailed description of how you intend to implement each mandated risk mitigation measure. Where the SMP allows for you to choose risk mitigation measures stipulate which measures you intend to use and then provide a description of how you intend to implement each measure.

1.7 SOPs

Provide copies of your internal security SOPs, to include;

- *Evacuation and relocation plans (including shelter in place)*
- *Headcount procedures*
- *Communication procedures*
- *Medical evacuation Plans*
- *Protocols for how to call for support in extremis*

- *Movement SOPs*
- *Escalating and deescalating you security posture*
- *Crisis Management Plan*
- *Hostage Incident Management*

1.8 Actions On'

Provide copies of 'Actions on' procedures for your personnel in the event of;

- *VBIED/PBIED/IED*
- *Complex Attack*
- *Indirect fire attack*
- *Civil unrest*
- *Shooting*
- *Armed Robbery/Raid*
- *Intimidation or Extortion*
- *Arson*
- *Illegal blockade or occupation of infrastructure by hostile protestors*
- *Compound takeover or hostage taking by hostile elements*
- *Kidnapping*
- *Hijack*

1.9 ESMF Checklist

Provide a copy of the ESMF Security Checklist completed as part of your proposal.