Ministry of Energy and Mineral

Government of Somaliland

GOVERNMENT OF SOMALILAND

Ministry of Energy and Minerals

Somali Electricity Sector Recovery Project

(SESRP) (Project: P173088)

Project Security Management Plan

(SMP)

December 9, 2024

Acronyms and Abbreviations

BESS	Battery Energy Storage Systems
BOQ	Bill of Quantities
BSSF	Business Services Support Firm
E&S	Environmental and Social
EAPP	Eastern Africa Power Pool
ESI	Electricity Supply Industry
ESCP	Environmental and Social Commitment Plan
ESP	Energy Services Provider
ESRC	Environmental and Social Risk Classification
ESWG	Energy Sector Working Group
FCV	Fragility, Conflict and Violence-
FGS	Federal Government of Somalia
GHG	Greenhouse Gas
GRS	Grievance Redress Service
HIPC	Highly Indebted Poor Country
HOAI	Horn of Africa Initiative
HOA RISES	Horn of Africa Regional Integration for Sustainable Energy Supply
HSDG	High Speed Diesel Generator
IDA	International Development Association
IDP	Internally Displaced Persons
IFC	International Finance Corporation
LV	Low Voltage
M&E	Monitoring and Evaluation
MIS	Management Information System
MoEM	Ministry of Energy and Minerals
MoEWR	Ministry of Energy and Water Resources
NDC	Nationally Determined Contribution
NDP	National Development Plan
O&M	Operation and Maintenance
PDO	Project Development Objective
PIM	Project Implementation Manual

PIU	Project Implementation Unit
PSC	Project Steering Committee
SDG	Sustainable Development Goal
SEAH	Sexual Exploitation Abuse and harassment
SEAP	Somalia Electricity Access Project
SecMF	Security Management Framework
SESRP	Somalia Energy Sector Recovery Project
SHS	Solar Home Systems
SL	Somaliland
SMP	Security Management Plan
SRA	Security Risk Assessment
SOP	Series of Projects
TA	Technical Assistance
TOR	Terms of Reference
USAID	United States Agency for International Development
WDR	World Development Report
BEC	Berbera Electric Company
AEC	Awdal Electric Company

1. Introduction

1.1 Background

The energy sector in Somaliland reflects characteristics common to nations in or emerging from conflict, where private entities have filled the void by establishing small electricity companies known as Energy Service Providers (ESPs). These ESPs typically operate decentralized, private electricity networks using medium voltage (MV) and low voltage (LV) systems with embedded small-scale high-speed diesel generators (HSDGs), initially catering to their own needs and gradually expanding to serve entire neighborhoods.

Despite facing numerous challenges over the past decade, the Somaliland government has made strides in fortifying the legal and policy framework governing the energy sector. The Ministry of Energy and Minerals (MOEM) oversees the sector, while the Somaliland Energy Commission (SEC) regulates it. Electricity services are predominantly provided by privately owned ESPs.

To bolster the sector further, the government, with support from development partners, has implemented various initiatives such as approving a National Energy Policy, enacting an Electrical Energy Act, and launching distribution guidelines. Key planning documents like the power master plan and electrification plan have also been finalized. The World Bank, through funding, is now supporting the Somalia Electricity Sector Recovery Project (SESRP).

The SESRP aims to enhance access to lower-cost and cleaner electricity services, and to re-establish the Electricity Supply Industry in the designated project areas. The Somaliland Electricity Sector Recovery Project (SESRP) is a five-year initiative led by the Government of Somaliland (GoSL) with financial assistance of $50 million from the World Bank. Forming part of a Series of Projects (SOP), this endeavor aims to rebuild and expand Somaliland's electricity sector, enabling it to fulfill its mandate of expanding access, improving service delivery, facilitating the clean energy transition, and attracting new investments. the project is structured around four key components: The MoEM will oversee project implementation through a Project Implementing Unit (PIU). Key components of the SESRP include increasing electricity access, enhancing service reliability and efficiency, and strengthening sector institutions and regulations.

Component 1 - Distribution Network Reconstruction and Operations Efficiency:

This component focuses on reconstructing and reinforcing distribution networks in major load centers. By integrating ESPs' networks and existing generation, the aim is to optimize distribution network operations and scale up generation capacity for enhanced efficiency.

Component 2 - Renewable Energy Generation Optimization:

Through hybridization and optimization of existing generation, this component seeks to increase

electricity supply sustainably. The installation of Battery Energy Storage Systems (BESS) and solar PV systems at diesel-based generation stations is central to this effort.

Component 3 - Electricity Services for Improved Public Services Delivery (Health and Education):
Targeting rural and peri-urban areas, this component aims to provide reliable electricity to public facilities. Standalone solar PV systems augmented by BESS will be installed, enabling these institutions to attract skilled workers and effectively respond to emergencies such as COVID-19.

Component 4 - Sector Capacity Enhancement and Project Implementation Support:
Activities under this component include strengthening sector governance and regulation, enhancing operational efficiency, and conducting sector integrated planning analytics. The development of a Sector Least Cost Development Plan and an Electricity Access Plan, particularly for rural areas, will be supported. Business Support Services will also be provided to rebuild and capacitate the Somali electricity sector through policy guidance, operations management training, and staff capacity building.

In alignment with the World Bank's environmental and social standards, the SESRP includes a comprehensive security management plan to assess, manage, and monitor potential social risks, ensuring effective risk mitigation strategies throughout the project's implementation.

1.2 Security Management Plan

Objective of the Security Management Plan:

The objective of the Security Management Plan (SMP) is to establish and uphold a secure physical environment and regulate staff activities to minimize the risk of personal harm and property damage throughout the implementation of the SESRP Project. This SMP encompasses Components 1, 2, 3, and 4 of the project activities. It identifies security-related risks anticipated in the execution of subprojects or site-specific activities. The SMP proposes general risk mitigation measures that will necessitate more detailed examination through Security Risk Assessments (SRA) and the formulation of specific Security Management Plans (SMP) for the Project and its activity locations. The identification of threat sources associated security risks, their potential consequences, and their mitigation via the SMP aim to ensure adequate security levels for project personnel, assets, affected communities, Implementing Partners (IPs)/Contractors, and overall operations.

Building on the SRA, it details how security will be managed, the responsible parties, required resources, expected behavior from security personnel, equipment, responsibilities, and risks related to their conduct and impact on communities. While the SMP is practical and actionable, it cannot cover every scenario in detail but should present the project's general security approach, risk mitigation strategies, and compliance with international standards such as the UN Basic Principles on the Use of Force or the International Code of Conduct for Private Security Providers. Key commitments from the SMP should align with the Environmental and Social Commitment Plan (ESCP). In projects with lower security risks, these commitments are directly integrated into the ESCP, highlighting major security risks and mitigation measures.

1.3 Integration of SecMF and SMP:

1. *Alignment of Objectives:*
   The SecMF provides the overall strategy for security, while the SMP focuses on applying these strategies at a detailed level to ensure effective security management throughout the SESRP.
2. *SecMF Guidance for SMP:*
   The SecMF offers guidelines on security management, including risk assessment and emergency protocols. The SMP follows these guidelines to implement specific security procedures and solutions tailored to the project's needs.
3. *Risk Assessment Linkage:*
   Security risks identified in the SecMF's Security Risk Assessments (SRAs) are used to develop detailed security plans (SMP) for the project, helping address the risks with targeted actions.
4. *Development Continuum:*
   The SecMF informs the creation of security risk assessments and management plans for different project components and locations, outlining necessary actions, responsibilities, and resources.
5. *Compliance and Alignment:*
   The SMP aligns with the Environmental and Social Commitment Plan (ESCP), ensuring that security measures comply with both project needs and international standards.
6. *Continuous Improvement:*
   The SecMF and SMP are interconnected in a feedback loop, where the implementation of security measures in the SMP informs updates and adjustments to the SecMF, ensuring that security strategies remain adaptable and responsive to changing risks.

By integrating the strategic direction of the SecMF with the detailed security measures of the SMP, the SESRP project can effectively manage security risks, protect stakeholders, and enhance overall project resilience.

1.4 Security Governance and Responsibilities in SESRP:

Security Governance:

In the intricate landscape of the Somali Electricity Sector Recovery Project (SESRP), solid security governance structures are fundamental for effective risk management. This includes undertaking periodic security monitoring from the contractors to the security Advisor at the PIU. The security management protocols must be followed successfully.

Responsibilities:

Designating clear responsibilities is essential for effective security management within SESRP. Responsibilities should include community engagement to address security concerns, capacity-building through training initiatives, compliance monitoring to enforce security protocols, and mechanisms for continuous improvement to adapt to emerging threats. By delineating roles and fostering accountability, SESRP can navigate its dynamic environment with enhanced security measures that safeguard project personnel, assets, and neighboring communities effectively.

2. Security Management Pillars for SESRP Operations:

In ensuring the security of the Somali Electricity Sector Recovery Project (SESRP), adherence to the fundamental pillars of security management is paramount. These four pillars serve as guiding principles for mitigating risks, protecting assets, and safeguarding personnel within the project environment.

- *Detect an adversary.*
- *Deter an adversary.*
- *Delay the adversary until appropriate authorities can intervene.*
- *Respond to the adversary's actions.*

1. DETECT:

Detecting potential threats and adversaries is the initial step in effective security management for SESRP operations. This pillar emphasizes the importance of implementing surveillance systems, monitoring tools, and threat intelligence mechanisms to identify any suspicious activities or security breaches promptly. By proactively detecting threats, security personnel can initiate timely responses and preventive measures to mitigate risks and enhance overall situational awareness.

2. *DETER:*

The deterrence of adversaries forms a critical component of SESRP's security strategy. By implementing visible security measures, access controls, and security protocols, the project aims to dissuade potential threats from engaging in harmful activities. Deterrence mechanisms such as security patrols, presence of security personnel, and clearly defined security perimeters communicate a strong message that unauthorized actions will not be tolerated, thereby discouraging adversarial activities.

3. DELAY:

In instances where detection and deterrence measures may not prevent an adversary's intrusion, the ability to delay their progress is crucial. Delay tactics involve implementing physical barriers, access controls, and response plans to impede the adversary's advancement and buy time for appropriate authorities to intervene. By delaying the adversary's actions, security personnel can prevent immediate harm and facilitate a coordinated response to the unfolding situation.

4. RESPOND:

The final pillar of security management entails a swift and well-coordinated response to adversary actions. In the event of a security breach or threat escalation, SESRP's response protocols come into play. These protocols outline clear procedures for alerting authorities, initiating emergency responses, evacuating personnel if necessary, and implementing crisis management strategies to mitigate the impact of the adversary's actions. A robust response capability ensures that security incidents are managed effectively, minimizing potential damage and ensuring the safety of project personnel and assets.

By adhering to these four pillars of security management—Detect, Deter, Delay, and Respond—SESRP can establish a comprehensive security framework that effectively addresses potential threats, safeguards project operations, and maintains a secure environment for all stakeholders involved in the project.

2.1. Security Approach for SESRP:

Within the Somali Electricity Sector Recovery Project (SESRP), the Project Coordinator, in collaboration with the security advisor within the Project Implementation Unit (PIU), is tasked with ensuring a robust security framework that safeguards project operations. This entails the continuous design and updating of security procedures and criteria, ensuring that the necessary resources are readily available to maintain the security of project activities.

This security management plan (SMP) outlines how security measures are structured to address identified threats and how security protocols are regularly reassessed and adjusted in response to evolving security situations and operational requirements. The Project Security Advisor, working closely with the PIU Coordinator, will harness existing national and local security infrastructure to access and share conflict-related information. This collaboration aims to engage local police leaders in addressing conflict risks during community interactions promptly.

Given that many security risks stem from inherent local social issues, the security approach integrates project operations, government relations, and community engagement activities. Staff members actively participate in security processes to promote a comprehensive security culture within SESRP. Importantly, proactive measures are outlined to address physical security at project sites, safeguard project assets, and ensure the safety of workers during travel.

To mitigate and manage project security risks effectively, the security approach emphasizes preventive strategies, early detection measures, and rapid response protocols. This includes implementing access controls, surveillance systems, and emergency response plans to minimize vulnerabilities and respond swiftly to security incidents. Additionally, the potential deployment of security personnel, including police officers, is considered to enhance on-the-ground security measures.

Furthermore, close coordination and cooperation with law enforcement agencies are essential components of the security strategy. Establishing relationships with local authorities and fostering collaboration with law enforcement entities enable SESRP to leverage external support, enhance security intelligence sharing, and facilitate a coordinated response to security threats. By integrating these elements into the security approach, SESRP aims to create a secure operational environment,

protect project assets, and ensure the well-being of project personnel amidst dynamic security challenges.

2.2 Enhancing Security Governance: Compliance with World Bank's Environmental and Social Framework.

The security management plan (SMP) for the SESRP project is crucial for addressing and mitigating potential risks identified in the Security Risk Assessment. The World Bank's Environmental and Social Framework outlines specific requirements and standards that borrowers like the Somaliland Government must adhere to when implementing projects supported by the Bank. In this case, the following ESS and GPN are particularly relevant for security governance in SESRP:

ESS1: Assessment and Management of Environmental and Social Risks and Impacts: This standard requires assessment, management, and monitoring of environmental and social risks and impacts throughout the project lifecycle to ensure outcomes align with Environmental and Social Standards.

ESS4: Community Health and Safety: This standard emphasizes the importance of considering community health and safety impacts resulting from project activities, equipment, and infrastructure, especially in areas already vulnerable to climate change effects.

ESS10: Stakeholder Engagement and Information Disclosure: Encourages open and transparent engagement with project stakeholders to enhance project sustainability, acceptance, and successful implementation.

GPN: Addressing Sexual Exploitation and Abuse and Sexual Harassment (SEA/SH): Provides guidelines for assessing and addressing risks of sexual and gender-based violence, crucial for meeting the requirements of ESS1 and ESS4.

GPN: Assessing and Managing the Risks and Impacts of the Use of Security Personnel: Offers expectations for evaluating and managing risks associated with security personnel to prevent harm to communities where project activities are conducted.

GPN: Road Safety: Outlines expectations for assessing and managing the risks of road traffic accidents involving project personnel and local communities.

Relevant laws that should be considered for the security management plan of the SESRP project in Somaliland include:

1. *Law No. 5/2012 - The New Somaliland Maintenance of the Police Order and Security Law:* This law likely addresses the maintenance of public order and security within Somaliland.
2. *Somaliland Public Order and Security Law No. 21, Articles 7, 18, 19:* Specific articles within this law may provide guidance on security measures, law enforcement, and public safety.
3. *Somaliland Constitution, Articles 18, 19, 24:* These constitutional articles may relate to fundamental rights, security provisions, and governance structures relevant to the project's security management.

2.3. Project Documents

To implement the World Bank ESF requirements outlined above, the PIU has in place key documents that also play a significant role in the governance of security in SESRP and support the Security Management Framework, these are listed below;

- *Environmental and Social Management Framework (ESMF)* – This document guides the environmental and social screening and assessment of the potential impacts from SESRP and proposes broad mitigation measures. It also ensures that SESRP activities are compliant with the relevant requirements of Federal and State-level policies, regulations and legislation as well as the World Bank ESF.
- *Stakeholder Engagement Plan (SEP) –* This document provides a structured, purposeful, genuine and culturally appropriate approach to consultation and information disclosure. The aim is to create an atmosphere of understanding that actively involves project-affected people and other stakeholders leading to improved decision-making.
- *Grievance Redress Mechanism* – This document provides guidance for the management of complaints and grievances that arise during SESRP delivery and provides a suitable, centralized grievance mechanism that allows the reporting of grievances, assessing issues raised and how these will be investigated and resolved.

2.4 Brief overview of the security situation in the project areas:

The security overview for the project areas, excluding the Sool region, portrays a stable environment with a prevailing positive sentiment towards the SESRP project within local communities. While this positive outlook sets a firm foundation for the project's advancement, several critical security concerns merit attention to safeguarding its seamless progression and enduring success.

One paramount area necessitating scrutiny involves the potential presence of criminal activities, albeit at minimal levels, such as sporadic incidents of theft and vandalism posing risks to project assets and personnel. Additionally, although instances of violence are infrequent, addressing emerging patterns and reinforcing preventive measures against potential escalations remain imperative. Moreover, the region's susceptibility to external threats, including the looming specter of insurgencies or extremist activities, underscores the necessity for constant vigilance and strategic security planning.

An essential facet entails proactive engagement with law enforcement agencies and the establishment of robust communication channels to swiftly address any security breaches. By proactively tackling these security concerns, cultivating community partnerships, and bolstering security protocols, the SESRP project can adeptly navigate potential challenges, ensuring the safety of all involved while advancing its objectives across Somaliland.

Incorporating measures to address clan conflicts, potential terrorism risks, and historical tensions within the security framework will fortify the project's resilience and contribute significantly to its sustainable development goals in the region.

2.5 Security Responsibilities within SESRP

This table outlines the security responsibilities within the SESRP project at different organizational levels and how these entities should interact with each other to ensure effective security management.

Energy Sector Working Group (ESWG)	PIU	IPs/Construction Contractors
• Provides guidance for project implementation. • Provides a forum for sector dialogue, ownership, and accountability between government, development partners, and other sector stakeholders. • Supports coordination and harmonisation of processes, procedures, implementation, and monitoring of government programs, development partner support, and private sector initiatives.	• Engage a PIU Security Advisor. • Ensure the development of Project-wide and District SRA in line with the requirements of the SecMF and ISO31000 • Ensure the development of a Project-wide SMP and project SRAs and SMPs for Proposed (specific) sites, and project-level ASPs (as applicable). • Ensure the integration of the Region and District stakeholders in SRM in line with the Project SEP. • Ensures training is provided to stakeholders and Contractors related to SMP. • Seek WB no objections on SMPs. • Ensure the integration of local SMP requirements and adequate budgeting of security measures into bidding processes during procurement of IPs/Contractors • Monitor the implementation of SMPs by Contractors • Report on the implementation of SMPs as part of the reporting on environmental and social standards.	• Present appropriate budget for security risk mitigation. • Implement security risk mitigation measures for the activity. • Exercise right to suspend activities due to security threats. • Act in accordance with social and environmental framework directives.

Table 1: Security Responsibilities within SESRP

3. Security Management Measures

3.1 Overview

This section outlines measures to mitigate threats identified in Section 2. Each threat category includes a risk level and proposed mitigation measures for SESRP partners to implement. The threats are categorized as follows:

- *Threat to Worksites*
- *Threat to Movement*
- *Threat to Local Population*

All threats apply across the categories of workers, movement, and local population. The following table organizes the relevant information into three columns: **Threat/Risk Category**, **Proposed Mitigation Measures**, and **Responsible Party**.

Risk Category	Threats to Work Sites	Threats to Movement	Threats to Population
Political	-Political risks could impact the delivery of SESRP activities or could escalate into violence, which could impact workers. - Political instability disrupting operations, - Protests causing safety concerns, - Changes in regulations impacting work	- Civil unrest affecting transportation- Political tensions at borders- Embargoes restricting movement- Diplomatic crises causing border closures- Political attacks on personnel	- Community tensions leading to violence- Election-related conflicts- Government overthrows- Persecution of minority groups- Forced relocations due to projects
Safety	-Project personnel will be exposed to safety risks, while at the SESRP worksites. - Accidents due to poor working conditions, - Equipment failures causing injuries, - Exposure to hazardous materials, - Falls and electrical hazards	-Project personnel will be exposed to safety risks while moving SESRP equipment, - Road accidents from poor conditions, - Vehicle breakdowns, - Driver fatigue, and adverse weather	- Public health crises (e.g., pandemics), - Industrial accidents impacting communities, - Natural disasters affecting safety, - Environmental contamination

Extremism	- Terrorist attacks on worksites, - Kidnapping of personnel, - Radical ideologies influencing the workforce, - Sabotage of infrastructure Personnel, - Radical ideologies influencing the workforce, - Sabotage of infrastructure	- Travel restrictions due to threats, - Violence impacting movement, - Displacement of individuals	- Injury and loss of life from extremist actions, - Psychological trauma within communities
Criminality	- Property damage and theft, Interference with daily operations	- Physical harm from criminal activities, - Disruption of operations due to crime	- Theft of valuables affecting safety, Loss of community trust
Theft	- Property damage and loss of assets, - Interference with operations	- Physical harm during theft incidents, - Disruption of movement due to theft	- Loss of community resources, - Increased fear in public spaces
Vandalism	- Damage to property leading to loss of assets, - Interference with daily operations	- Physical harm from vandalism-related incidents, - Disruption of community events	- Damage to community infrastructure, - Loss of cultural heritage
Civil Unrest	- Disruption of operations and damage to property, - Increased risk of violence at worksites	- Travel restrictions due to protests, Safety concerns affecting transportation	- Physical harm to community members- Disruption of social cohesion
Communal Violence	- Damage to community infrastructure and work sites, - Interruption of community events	- Disruption of movement due to violence, Safety threats affecting transportation	- Threats to community safety leading to displacement
Vested Interests	- Disruption of operations due to external influences, Damage to reputation impacting business	- Interference with operations causing financial loss, Threats to business continuity	- Financial loss affecting community resources, - Erosion of trust in local businesses

3.2 Supporting security procedures

The Use of Armed Guards

While the security situation in the SESRP area of focus necessitates the use of Armed Guards at worksites, we must be mindful of the risks presented by untrained, ill-disciplined, or ill-equipped security guards.

Guards should, therefore, be hired from local security providers that are appropriately licensed and registered with Somaliland's Ministry of Interior.

The use of Armed Guards can potentially increase some risks in that;

- Guards may react inappropriately to situations, posing a risk to others or themselves;
- Guards may fail to perform their duties adequately, allowing threat actors to target SESRP;
- Guards lead to situations of misconduct against the wider community or colleagues.

The risks of using Armed Guards are to be addressed through four channels, outlined below.

Selection of Guards and Suppliers

Prior to being contracted to supply guards, a guard supplier should be screened by the PIU, to ensure that they meet expected standards.

The screening process will check;

- Licence and registration of the company and the weapons they are supplying;
- Management processes;
- Guard training syllabus;
- The company's existing Code of Conduct and Rules for the Use of Force;
- The backgrounds, where possible, of the Guards proposed for the worksite.

It is, unfortunately, expected that not all local suppliers will be able to meet these criteria. While elements such as licencing and registration cannot be ignored, if a company does not have a documented Guard Training syllabus, Code of Conduct or Rules for the Use of Force, standardised versions created by the PIU security advisor can be supplied, along with support for the supplier to operationalise these.

The intention of ensuring Guard suppliers have existing Codes of Conduct, Rules for the Use of Force, Management processes, and training syllabus is to ensure a basic level of management control exists.

Sample Code of Conduct

Where a security provider does not have an existing Code of Conduct, or the Code of Conduct does not meet SESRP requirements, they will be expected to comply with the sample Code included at Annex A.

Procedures

Guards working on SESRP sites will be expected to follow the security measures specific to the site as outlined in this Management Plan. This includes measures such as Access Control, Patrolling, Incident Response, including the Code of Conduct and Rules for the Use of Force created for SESRP.

It is recommended that during the process to contract armed guards and deploy them to SESRP sites the supplier is requested to provide their procedures for review and approval by the PIU Security Advisor.

Trainings

Training Overview

Training for guards at SESRP sites will be provided by the Security Advisor with the assistance of Security Focal Points appointed by contractors upon contract award. The training aims to ensure guards are familiar with SESRP controls related to Armed Guards and their duties. Security Focal Points will also participate in the Community of Practice (CoP) directed by the Security Advisor. The training will be conducted periodically at intervals to be determined by the need.

Training Structure:

1. *Initial Training:*
    - Provided by the Security Advisor in collaboration with Security Focal Points to familiarize guards with SESRP controls and responsibilities post-contract award.
2. *Ongoing Training:*
    - Regular refresher sessions conducted periodically to reinforce security protocols and keep guards updated on any changes.
3. Incident-Specific Training:
    - Conducted in response to specific incidents or as necessary based on security assessments.
4. *Annual Training:*
    - Yearly sessions to review procedures, address gaps, and ensure ongoing compliance with security measures.

Training Content:

- *Code of Conduct and Rules for Use of Force:* Emphasis on adherence to specific SESRP guidelines.

- *Security Measures:* Training on access control procedures, patrolling techniques, and incident response protocols.
- *Emergency Response:* Guidance on effective handling of emergencies and security incidents.
- Risk Awareness: Education on identifying and mitigating potential risks at the site.
- *Communication Protocols:* Awareness of communication channels and reporting procedures.

Training Providers:

- *Initial Training:* Conducted by the Security Advisor with the support of Security Focal Points nominated by contractors.
- *Ongoing Training:* Led by the Security Advisor or designated trainers with expertise in security management.
- *Incident-Specific Training:* Carried out by experienced security professionals.
- *Annual Training:* Organized by the Security Advisor or external security training providers with relevant experience.

Monitoring Security Guards

During the deployment of security personnel, performance should be monitored throughout by the security provider to ensure professional and appropriate conduct. Any operation which may require the use of force should be closely supervised and monitored by management to ensure that the use of force, if required, is permissible and appropriate in the circumstances. The role of management monitoring the operation is to ensure that the operational plan is followed correctly, that all reasonable steps to avoid the use of force are taken by the deployed personnel, and that the use of force continuum is applied wherever required.

Supervision and monitoring also serve to reprimand and reorient the security personnel who might diverge from the operational plan, those who may be tempted to resort to the use of force when not necessary, or those who have been accused of misconduct. Throughout the operation, the responsibility of the management is to ensure the respect of the principles of necessity, proportionality and precaution and to adopt means and measures to ensure that those principles are upheld.

In cases where this fails, managers are responsible for ensuring accountability. Proper supervision and monitoring will play a crucial role after the operation, whenever an incident involving the use of force might require reporting, investigation or disciplinary sanctions.

Failure to adequately supervise or monitor PSP personnel during an operation that involves or potentially requires the use of force might engage the responsibility and accountability of those in management positions.

Security providers should:

- Establish and maintain a clearly defined management structure. Responsibilities should be clearly defined, documented and communicated. Roles should include tasks such as monitoring, coordination and supervisory responsibilities, as well as planning, security, incident management, response and/or recovery. Roles should be paired with appropriate authority, adequate resources and rehearsed operational plans and procedures to effectively deal with disruptive and undesirable events;
- Establish communication procedures to share information about the security team activity, its regulations on the Use of Force, its operational and logistical status, the relevant threat information and incident reporting to company management, clients, other private security teams and relevant authorities;
- Establish and implement procedures to support the protection of people, assets and other security related functions, including managing risks;
- Establish and implement procedures to 1) identify undesirable or disruptive events, 2) define how the PSP prevents, mitigates, and responds to undesirable or disruptive events, and 3) document how the PSP will proactively prevent, mitigate, and respond to such events.

Security grievance reporting mechanism

the SMP adopts the Project Grievance Mechanism for security complaints, integrated with SESRP and Stakeholder Engagement. Collaboration with security leaders aligns with internal procedures. Key steps include publicizing procedures, receiving, and tracking grievances, reviewing, and investigating, developing resolutions, and monitoring. Security personnel grievances follow Somaliland National Police Force and Independent Policing Oversight Authority protocols for resolution. Key Steps in the Security-Related GRM Process

Key Steps:

- Record the incident or allegation.
- Monitor and communicate outcomes.
- Take corrective action to avoid recurrence.
- Collect information promptly.
- Report any unlawful act.
- Protect confidentiality.
- Document the process.
- Assess the allegation or incident.
- Conduct further inquiry, if warranted

The monitoring of security, and security suppliers, performance will be an ongoing process and should be driven by inputs from within the SESRP PIU and the wider community.

Project Personnel will have the right to report concerns over security and risks internally to their employer or PIU representative. These risks will be addressed either locally or at PIU level.

If issues are not resolved, workers will be able to escalate concerns in line with the Workers Grievance Redress Mechanism which is in place. Where feasible, such issues should be dealt with a Tier 1 Community OR Contract/ Activity level, however security issues relating to the performance of Armed Guards may need to be addressed at Tier 2 PIU level.

Communities may follow a similar process for addressing security concerns and concerns regarding the performance of Armed Guards at a SESRP site as per the project SEP.

Grievances against Armed Guards should be handled discretely with a view to preventing further misconduct. Where Armed Guards are to be investigated, they should be removed from the site as soon as the grievance is reported. Depending on the nature of the grievance, local security authorities may also need to be informed, particularly if the accusation relates to a serious crime.

Where an investigation demonstrates misconduct was the result of a lack of supervision and leadership by the relevant security supplier, the supplier should be removed from the site and a new supplier hired, or punitive clauses in contracts should be invoked.

Project affected persons (PAPs) may also make complaints directly to the project wide GRM through the key contact persons (Grievance officer).

- **Hotline number: 999**
- **Contact numbers-:** + 252637666625
- **Email address**: grm.sesrp@gmail.com
- **WhatsApp numbers:** +252637666625

4. SMP Monitoring, Evaluation, and Reporting

4.1 Monitoring

Overview

To ensure that the measures outlined in the SMP are implemented and continue to manage the risks to the project and affected communities, ongoing performance monitoring will be conducted across the project.

In keeping with ISO31000, the Security Risk Assessment process is an ongoing activity. During project delivery, the operational environment and implemented controls will be assessed in accordance with the methodology outlined in the Project Security Risk Assessment document.

The ongoing security risk assessment will utilise information from the context monitoring process, which looks externally to the project, and the performance monitoring process which looks internally.

Monitoring Methods

- *Site Visits:* Regular site visits are a crucial component of the monitoring process. During these visits, security protocols are evaluated on the ground, allowing for a direct assessment of their implementation. Potential vulnerabilities are identified, and the effectiveness of security measures is observed firsthand. Site visits provide a tangible understanding of the security landscape and offer insights into areas that require immediate attention or improvement.
- *Stakeholder Engagement:* Active engagement with key project security stakeholders is paramount for maintaining an effective security management plan. By conducting regular meetings, surveys, and consultations, valuable feedback is gathered on the plan's effectiveness. This engagement fosters a collaborative environment where stakeholders, including employees, contractors, and partners, can voice their concerns, suggest improvements, and contribute to shaping a robust security framework. Involving stakeholders at various levels ensures a holistic approach to security management and enhances overall buy-in and compliance.
- *Incident Response Reviews:* Reviewing past incident responses is a critical aspect of monitoring. By analyzing previous incidents, valuable lessons can be learned, and areas for improvement can be identified. This process allows for the refinement of security response protocols, the identification of recurring issues, and the implementation of corrective measures to enhance the overall effectiveness of the security management plan.
- *Performance Metrics:* Establishing key performance indicators (KPIs) is essential for quantitatively measuring the effectiveness of the security management plan. These metrics serve as benchmarks for evaluating security performance and can include parameters such as incident response times, security incident rates, and employee training compliance levels. By tracking and analyzing these metrics, security stakeholders can gauge the plan's efficiency, identify trends, and make informed decisions to enhance security measures proactively.

Context Monitoring

- *Information Collection:* The Security Advisor within the Project Implementation Unit (PIU) collects information from various sources to support ongoing risk assessment. This data enhances the understanding of the project's context and informs security measures.
- Detailed Understanding: Context monitoring involves continuous assessments of the operational environment and controls. This process ensures alignment with ISO31000 standards and facilitates a comprehensive evaluation of security measures and risk management strategies.

Performance Monitoring

In addition to context monitoring during the project the performance of the SMP will also be monitored. Contractors will be expected, as part of their delivery to implement appropriate security measures to ensure the safety of project personnel, project affected communities and project assets. The goal of the performance monitoring process is to ensure that contractors are complying with these contractual requirements and that the measures undertaken are performing adequately.

Performance monitoring involves several elements;

- *Security Community of Practice* – input from an extended community of practice as to the effectiveness of the security system will be sought.
- *Contractor self-certification* – contractors will be required to submit proof of SMP implementation at sites. They will be required to provide a copy of their Site or Activity Security Plan, contracts with private security providers (if applicable) and evidence where physical security measures are put in place (plans and photographs).
- *PIU audit and inspection –* the PIU Security Advisor will conduct site inspection activities during project delivery to provide verification that the contractor has properly implemented the measures outlined in the SMP and that the self-certification evidence provided is accurate.

4.2 Evaluation

The results of the ongoing monitoring activities will be reviewed and evaluated against the security management framework as well as the project's underlying principles, including the measures outlined in *Environmental and Social Standard 2: Labour and Working Conditions*, *Environmental and Social Standard 4: Community Health and Safety* and *Good Practice Note: Assessing and Managing the Risks and Impacts of the Use of Security Personnel*.

By comparing the results of the monitoring with the evaluation framework, we will identify areas where the security management framework is either not working or can be improved. This information will then be used to improve the security management framework.

4.3 Reporting

The project will see several levels of reporting conducted. In addition to the documents created as part of the security management framework, namely the Project SRA and SMP, the specific site SRAs and

SMPs and the Activity/Site SRA and SMP, other documents will be created and shared with the PIU project manager /MoEM.

- *Incident reporting-* as per the Security Management Framework (SecMF), and Environmental Social Framework (ESF) all incidents that have or result impact to the project personnel, workers, activities, communities, contractors and WB/MoEM will be reported within 24 hours of their occurrence, typical or same WB ESIRT will be applied by the SESRP. This tool will be confidential, owned and managed by the SA/SF while its utilization orientation/training will be conducted through the Bank's technical person/unit. WB will include the recipients of those incidents reported.

- *GBV incidents reporting –* all GBV incidents will be reported through a specific GBV incident reporting tool that is managed by the GBV specialist and her GBV focal points at project activities sites/areas.

- *Risk Registers* - will be created and hosted online and available for review at any time. These Risk Registers will combine the outcomes of the Security Risk Assessment and Security Management Plans. The purpose of the Risk Registers will be to ensure that the PMU are able to track the overall Security and Safety Risk levels. They will be reviewed and updated following the monitoring and evaluation activities as outlined above.
- *Weekly Security Reports –* these will provide updates to the PMU on the overall security and conflict context;

- Regular Security Community of Practice meetings on a weekly/monthly basis. These meetings will include discussions on incidents and events, review system performance, assess changes to the Security Management Plan, identify new risks, and lessons learnt. Meetings will include;

    a. PIU Security Advisor and Security Focal Point calls;

    b. Monthly Safeguarding team meetings;

    c. Wider community of practice (CoP) meetings on a monthly basis (or as called for by the PIU Security Advisor).

- Incident Reports – in the event of an incident, we will work with key stakeholders to review and identify the incident, the root cause, and lessons learnt, and supply this to the PIU.

5. Project Critical Incident Management Framework Overview

While the Security and Safety procedures detailed in the previous section are in place to reduce the likelihood of incidents occurring or ensure they are managed at the operational level, exceptional situations can arise that fall outside typical management arrangements due to their nature and severity.

Successfully resolving and managing any critical incident depends on our ability to make appropriate decisions quickly, which requires preparation, a good flow of information, and clear channels of communication that all staff understand. The objectives of Critical Incident Management are;

- *Prevent (further) harm and ensure the health and/or safety of the victim(s) and other personnel affected by the incident* – The first hours following (the onset of) a Critical Incident are often the most crucial, rendering instant reporting, a clear division of roles and responsibilities, and fast decision-making an absolute necessity;
- *Assure families of victims of a responsible and effective response –* Maintaining the confidence of victims' families is essential in establishing good relations and ensuring all stakeholders are "on board" during and after the incident.
- *Ensure continued organisational management and output during the incident* – Critical Incident Management is resource-intensive, especially for enduring incidents (for example, abductions). Planning and preparedness will mitigate the risk of the unnecessary distraction of senior management, thus contributing to the ability of SESRP to continue functioning:
- *Ensure project continuity* – In addition to mitigating the impact of a Critical Incident on organisational management, good Critical Incident preparedness contributes to our ability to continue project activities during a Critical Incident and/or restart operations in its aftermath;
- *Fulfil organisational responsibilities and reduce the risk of litigation/liability claims* – Contractual obligations and related litigation risks vary by country since we are subject to national legislation. We must ensure that we are fully aware of relevant legal labour frameworks, including those for national staff in each country of operation;
- *Safeguard organisational image and reputation* – Inadequate Critical Incident response, or perceived mishandling of a Critical Incident (in the eyes of media and/or family), can negatively affect the image of SESRP, with myriad consequences in countries of operation and at the international level (fundraising, recruitment, etc.). Again, a solid and professional Critical Incident response will help to mitigate this risk.

A small caveat, safeguarding reputation, while an important consideration, should never take precedence over the safety and well-being of staff, which remains the primary objective of Critical Incident Management within SESRP.

5.1 Critical Incident Management Team

SESRP has established a Critical Incident Management Team (CIMT) to respond to critical incidents. The CIMT has the following responsibilities. On receiving an incident report, the CIMT must decide the following;

- *Project Activities* – should these be suspended, or personnel withdrawn to a more secure location;
- *Support* – should additional personnel be deployed to assist;
- Information – what should be circulated internally and externally, and any limitations or confidentiality issues;
- *Objective* – how should the Critical Incident be resolved.

The CIMT is comprised of the following;

- The SESRP PIU Coordinator;
- SESRP PIU Project Security Advisor;
- The SESRP PIU Environmental and Social Safeguards Advisor;
- Project partner management, including those with safety and security responsibilities.

Critical Incident Management Procedures

Scenario	Project Team	Critical Incident Management Team
Relocation and evacuation	**Preventative** • Recommends evacuation to the Senior Management. • Will manage evacuation if authorized. **Emergency** • Alert CIMT of need to evacuate and how many personnel. • Identify how to evacuate and inform CIMT	**Preventative** • CIMT alerted and monitors to support if Project Team needs assistance. • Media Management **Emergency** • Assess the situation with personnel, partners and other stakeholders. • CIMT decides on evacuation. • CIMT to manage evacuation with input from Project Team. • Media Management
Medical response	• Provide 1st Aid and get to hospital. • Alert CIMT. • Support CIMT and Incident response.	• Implement Medical Incident Response Plan • Inform family/next of kin through family liaison. • Communicate with personnel and relevant parties. • Provide Psychosocial support.
Injury of personnel	• Alert CIMT. • Support CIMT and Incident response.	• Implement Medical Incident Response Plan • Inform family/next of kin through family liaison. • Communicate with personnel

		and relevant parties. • Media Management. • Provide Psychosocial support.
Death of personnel	• Alert CIMT. • Support CIMT and Incident response.	• Immediately notify SESRP Project Management Committee and Project Steering Committee. • Inform World Bank team. • Inform family/next of kin through family liaison. • Communicate with project personnel and other relevant parties. • Media Management. • Provide Psychosocial support.
Staff disappearance, Abduction, detention or kidnap	• Alert CIMT. • Continue to try and contact missing personnel. • Liaise with local partners to understand if Abduction/ Detention/ Kidnap. • Support CIMT and Incident response.	• Immediately notify SESRP Project Management Committee and Project Steering Committee. • Inform World Bank team. • Implement Hostage Incident Management Plan. • Inform family/next of kin through family liaison. • Communicate with project personnel and other relevant parties. • Media management. • Provide Psychosocial support.
Attack or threat of attack against project activity (worksite/movement)	• Alert CIMT. • Project activities to pause, personnel to shelter in place. • Liaise with authorities and other organisations working in the area	• Assess the situation with personnel, partners and other stakeholders. • Monitor situation and authorize pause or withdrawal of personnel if risk warrants it. • Inform family/next of kin through family liaison. • Communicate with personnel and relevant parties. • Media management. • Provide Psychosocial support.
Attack on a hotel where personnel are staying or at an office	• Alert CIMT and check how many personnel may be involved. • Try and contact personnel to check on status. • Liaise with local partners as necessary.	• Assess the situation with personnel, partners and other stakeholders. • Inform insurance. • Monitor situation and liaise with authorities. • Inform family/next of kin

	• Liaise with the authorities.	through family liaison. • Communicate with personnel and relevant parties. • Media management. • Provide Psychosocial support.
Media or reputation crisis	• Do not respond. • Alert CIMT.	• Do not respond until an assessment has been made and advice has been sought from the media/comms team.
Disease outbreak/pandemic	• Alert CIMT and check how many personnel may be involved. • Liaise with local partners as necessary. • Liaise with the authorities. • Provide PPE and support services to staff.	• Establish safety and wellbeing of personnel. • Restrict travel and activities to limit exposure. • Inform insurance. • Ensure accurate information is passed to personnel. • Update health measures and contingency plans. • Work with Project Team to monitor health of personnel.

Table 2: Critical Incident Management Procedures

5.2 Violent Incident Response Plan

Overview

During project delivery, project personnel may be at risk of armed attacks by criminals, communal militia and extremists. This section outlines how such incidents should be responded to.

It should be noted, though, the descriptions below are to be seen as guidelines as opposed to an exact process as every situation is different and a document cannot account for all possible events.

These procedures work in conjunction with the Critical Incident Management procedures in Table 6 above.

Direct Fire

If during SESRP activities personnel come under direct fire (the firing of a ranged weapon whose projectile is launched directly at a target within the line-of-sight of the user) the following are steps that can be taken.

- *Take cover* – find the closest hard cover and get behind it. Be wary of objects that provide concealment (hide from view) as opposed to cover (prevent projectiles striking).
- *Return fire* – if accompanied by armed security personnel (security forces or private security guards) these should fire on the person/s firing at the party, remembering the relevant Rules of

Engagement (security forces) or Rules for the Use of Force (private security). Fire should be aimed and controlled and not towards civilians (to avoid inflicting casualties).

- *Evacuate –* leave area expeditiously towards a safe location. If with vehicles (and if undamaged) use these to evacuate the area.
- *Rally* – all personnel to go to the same safe location and meet. Ensure all personnel are present and uninjured (respond according to the Medical Incident Response Plan and Hostage Incident Management Plan if someone is injured/ missing).
- *Report* – inform local security forces, PIU, and community stakeholders of the situation and what has happened.

Direct Fire Attack on Office / Hotel – Active Shooter Situation

There is potential that while SESRP personnel are in the building (including Hotels or Offices) the site could come under attack by armed individuals (extremists, communal militia, criminals) who can enter, leading to an Active Shooter situation.

The response is based on, but with differences, to the usual Direct Fire response plan due to differences in environment, availability of cover, restricted movement, etc. The following are steps that can be taken.

- *Run -* If there is an accessible escape path, attempt to evacuate the premises. Be sure to:
    - Have an escape route and plan in mind
    - Evacuate regardless of whether others agree to follow
    - Leave your belongings behind
    - Help others escape, if possible
    - Prevent individuals from entering an area where the active shooter may be
- *Hide –* If evacuation is not possible, find a place to hide where the active shooter is less likely to find you. Your hiding place should:
    - Be out of the active shooter's view
    - Provide protection if shots are fired in your direction (i.e., an office with a closed and locked door)
    - Not trap you or restrict your options for movement
    - To prevent an active shooter from entering your hiding place:
        - Lock the door
        - Blockade the door with heavy furniture
    - If the active shooter is nearby:
        - Lock the door
        - Silence your cell phone and/or pager
        - Turn off any source of noise (i.e., radios, televisions)
        - Hide behind large items (i.e., cabinets, desks)
        - Remain quiet
- *Fight –* As a last resort, and only when your life is in imminent danger, attempt to disrupt and/or incapacitate the active shooter by:
    - Acting as aggressively as possible against him/her
    - Throwing items and improvising weapons
    - Yelling

- Committing to your actions

Throughout the situation if members of the security forces arrive on scene ensure you cooperate with their instructions, remain calm and keep your hands visible.

Indirect Fire

If during SESRP activities personnel come under indirect fire (the firing of a ranged weapon without relying on a direct line of sight between the gun and its target), the following are steps that can be taken.

- *Take cover –* find closest overhead cover and get below it. If there is no overhead cover available, personnel should assume the prone position.
- *Evacuate –* leave area expeditiously towards a safe location. If with vehicles (and if undamaged) use these to evacuate the area.
- *Rally –* all personnel to go to the same safe location and meet. Ensure all personnel are present and uninjured (respond according to the Medical Incident Response Plan and Hostage Incident Management Plan if someone is injured/ missing).
- *Report –* inform local security forces, PIU, and community stakeholders of the situation and what has happened.

5.3 Explosive Hazards

During SESRP activities personnel may observe or trigger an explosive hazard, either an Improvised Explosive Device (IED) planted by extremists or Unexploded Ordnance (UXO) left from previous armed conflict. The following are steps that can be taken.

Observation of an IED/ UXO Threat

If a device IED/ UXO is observed and has not exploded.

- Alert – whoever sees the suspected device must raise the alarm. The alarm should use the 3Ds (Distance; Direction; Description).
- Stop – all movement within 200m of the suspected device must stop immediately.
- Evacuate – leave area expeditiously towards a safe location (at least 200m from the device).
- Rally – all personnel to go to same safe location and meet. Ensure all personnel are present and uninjured (respond according to the Medical Incident Response Plan and Hostage Incident Management Plan if someone is injured/ missing).
- Report – inform local security forces, PIU, and community stakeholders of the situation and what has happened.

IED/ UXO Explosion

If an IED/ UXO explodes near project personnel.

- *Stop –* all movement within 200m of the suspected device must stop immediately.
- *Evacuate –* leave area expeditiously towards a safe location (at least 200m from the device).

- Rally – all personnel to go to same safe location and meet. Ensure all personnel are present and uninjured (respond according to the Medical Incident Response Plan and Hostage Incident Management Plan if someone is injured/ missing).
- *Treat* – Use the measures in the Medical Incident Response Plan.
- *Report* – inform local security forces, PIU, and community stakeholders of the situation and what has happened.

5.4 Medical Incident Response Plan

General Requirements

During project delivery personnel may, unfortunately, be injured during delivery (for example a safety incident) or as the result of a violent incident by a threat actor (criminal activity, extremist violence, communal violence). To ensure medical incidents are responded to in an appropriate manner, project partners should ensure they have sufficient medical support in place. This consists of;

- At least one employee at a worksite or in a convoy must have received emergency medical training (to FPOS-I or similar standard).
- A convoy or worksite must have sufficient medical equipment to address both day-to-day minor injuries, such as cuts and abrasions, expected in a construction project and more significant medical incidents such as gunshot or blast wounds resulting from attacks by threat actors.
- Project contractors must identify the nearest medical facility to a worksite capable of dealing with traumatic injuries and also identify the quickest, safest, route to reach this facility.
- Where no medical facility capable of dealing with traumatic injuries is within 30 minutes drive of a worksite, a contractor should ensure they have provision to treat such injuries at a worksite, at least to the point of stabilising an injured employee to the point where an evacuation to a more distant medical facility is feasible.

Medical Evacuation

Depending on the nature of injury project personnel may require a medical evacuation. There are three levels of medical evacuation considered within the project as outlined below.

Level	Scope	Reason	Requirements
1	Intra-District	• Traumatic injury that cannot be treated at worksite. • Traumatic injury that cannot be treated at nearby medical facility.	• Injured employee must be stabilised at scene for evacuation to be safe. • Contractor supplied vehicles to transport the injured party (ensuring movement security mitigations are employed)
2	Intra-Region or Intra-Somaliland	• Traumatic injury that cannot be treated at medical facility in District.	• Injured employee must be stabilised at local medical facility for evacuation to be

		• Persistent effects of an injury that require specialist care not available in District.	safe. • Evacuation by road or air depending on medical condition of employee and prevailing security situation. • Movement by air requires properly supplied and configured aeromedical transport and flight medic.
3	International	• Persistent effects of an injury that require specialist care not available in Somalia.	• Injured employee must be assessed as being stable enough for evacuation to be safe. • Evacuation by road or air depending on medical condition of employee and prevailing security situation. • Movement by air requires properly supplied and configured aeromedical transport and flight medic.

Table 3: Medical Evacuation Procedures

5.5 Hostage Incident Management Plan

Overview

During project delivery, project personnel may be at risk of kidnapping by criminals, communal militia and extremists. This section outlines how project partners should respond to such incidents.

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 motives 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.

Stage	**Activities**
Prevention	• Operate according to procedures outlined in Section 3: Security Management Plan • Ensure staff accountability and tracking systems are in place • Conduct regular security and awareness briefings with personnel • Avoid routine during movement • Use protection where required by risk levels • Establish a clear policy on payment of ransoms

Initial Response	• When personnel are reported missing, initially try to locate them and report they are missing to local security forces to enlist their support
	• If there is clear evidence of kidnapping, then.
	  ○ Inform PIU immediately
	  ○ Inform local security forces

	○ Halt all activities in District with personnel to shelter in place ○ Limit spread of information • Seek support of specialist advisors on kidnapping resolution
Managing the Incident	• Contact the kidnapped personnel's families, face to face, is best, and brief them • Standby to receive contact from kidnappers • Nominate the communicator (and a backup) who will lead conversation with kidnappers • Consider kidnapping scenarios and possible demands
Communication with Kidnappers	• The communicator or the back up to lead on conversations • Communications to be kept calm, clear, and professional • Understand the kidnappers' demands • Seeking to establish Proof of Life as quickly as possible • Maintain confidentiality and contain the spread of information
Media Management	• Try to minimize the spread of information to reduce chances of leaks to the media • If media/ social media report kidnaps, a no comment response should be provided • Media response is to be aligned with PIU, and the security forces
Ending the Incident	• Kidnapping may take weeks to resolve • Payment of ransoms is not encouraged but may be necessary. Should be aligned with all stakeholders (PIU, District Commission, security forces) • Abduction for political reasons may take longer to resolve • When the victim is released, psychosocial support and counselling is an immediate need

Table 4: Hostage Incident Management Plan

5.6 Region Incident Levels and Responses

During the course of the project, incidents that may affect the project or larger community are likely to occur. While incidents directly targeting SESRP activities should be dealt with by procedures created by project partners operating in the Region, incident levels elsewhere in the region can escalate to the point where they pose a threat to the project, the personnel working on it and the wider community.

During the course of project delivery, the situation in the project footprint should be monitored and appropriate measures, as outlined below be implemented.

Stage 1 Low Risk Level (Normal)			
• No overt political and cultural disputes in District relating to project or partners • No criminal activity or attacks by vested interests targeting project in previous 30 days • No extremist attacks in District • No communal violence in the district affecting the project in the previous 30 days • Discussions with local communities do not indicate discontent			
Stage	**Level of Risk**	**Alert State**	**Actions**
1	Low	Normal	• Business as usual • Weekly review of conditions

			• Quarterly review of staff contacts details, NOK, etc. • Review and rehearsal of procedures

Table 5: Region Incident Levels - Low Risk

Stage 2 Moderate Risk Level (Caution)			
• Increasingly overt political and cultural disputes in the district relating to the project or partners • No criminal activity or attacks by vested interests targeting project in the previous 15 days • Limited extremist attacks in the district with attacks occurring over 20 km of a worksite • No communal violence in the district affecting the project in the previous 15 days • Discussions with local communities indicate a low level of discontent			
Stage	**Level of Risk**	**Alert State**	**Actions**
2	Moderate	Caution	• Daily monitoring of conditions • Review incident response procedures • Review medical evacuation procedure • Review staff personal safety measures • Identity documents and go-bag contents to be carried by all individuals during all routine moves

Table 6: Region Incident Levels - Moderate Risk

Stage 3 High Risk Level (Alert)			
• Increasingly overt political and cultural disputes in District and protests against project or partners • No criminal activity or attacks by vested interests targeting project in previous 7 days • Regular extremist attacks in District with attacks occurring over 5Km of a worksite • Communal violence in District but is not within 5Km of a worksite • Discussions with local communities indicate increasing level of discontent			
Stage	**Level of Risk**	**Alert State**	**Actions**
3	High	Alert	• Daily monitoring of conditions • Consider pause of project activities and discuss with PIU • Be prepared to pause project at short notice • Prepare staff for evacuation at short notice

Table 7: Region Incident Levels - High Risk

Stage 4 Extreme Risk Level (Emergency)			
• Overt political and cultural disputes in the district with protests and armed attacks against the project or partners • Criminal activity or attacks by vested interests target the project • Daily extremist attacks in the district with attacks occurring within 5 km of a worksite OR extremist attacks on project activities • Communal violence in the district affecting the project • Discussions with local communities indicate the widespread level of discontent			
Stage	**Level of Risk**	**Alert State**	**Actions**

4	High	Emergency	• Project paused in District • Personnel to be evacuated or shelter in place • Project worksite to be secured

Table 8: Region Incident Levels - Extreme Risk

5.7 Anticipated Security Risks and Mitigation Measures

Given that the SESRP will be implemented across a diverse and contested geographical space, concrete threat vectors will require in-depth security risks assessments (SRA) to ensure the safety of Project workers, contractors and local communities at the site level. The security threat assessments and mitigation measures will vary considerably depending on the metropolitan and rural Districts worked in urban centres and peri-urban are generally more accessible for development actors and humanitarians.

Rural areas, where Component 3 activities are to occur, are an entirely different proposition and vary considerably in terms of their respective accessibility. The security arrangements for the Project may themselves pose risks and impact on project workers and local communities. It is important to take these risks and their impact into consideration and to determine measures to address them. This will be part of the ongoing stakeholder engagement on the project, as described in ESS10 and the project SEP, which the PIU, will incorporate into a cohesive Project level SMP.

The section of the SecMF lists security related risks that can be anticipated in the implementation of subprojects or site-specific activities – see Annex C. It recommends generic risk mitigation measures that will require more detailed treatment through Security Risk Assessments (SRA) and development of related Security Management Plans (SMP) for the sub projects and its specific activity localities when the feasibility and design reports are prepared. Identification of sources of threat, related security risks, their potential impact and their mitigation through SMP are all designed to ensure adequate levels of security for project personnel, project assets, affected communities, IPs/ Contractors and general operations.

5.8 Risk Treatment

The purpose of risk treatment is to select and implement options for addressing risk. the risk treatment follows a systematic approach to ensure appropriate security measures are developed and implemented. By following these risk treatment measures outlined in the SMP, the project aims to

ensure the safety and security of project personnel, assets, affected communities, and contractors while mitigating potential security risks.

Here are the key elements of risk treatment mentioned in the SMP:

- *Security Risk Assessment (SRA):* The SRA is conducted to identify and assess security-related risks associated with the project's implementation. It helps in understanding potential threats, their impacts, and vulnerabilities. The SRA provides the foundation for developing risk mitigation measures.
- *Generic Risk Mitigation Measures:* The SMP recommends generic risk mitigation measures that serve as initial steps to address identified security risks. These measures require more detailed treatment through Security Risk Assessments (SRA) and the development of specific Security Management Plans (SMP) for the project and its activity localities.
- *Specific Security Management Plans (SMP):* For projects with high security risks, a stand-alone SMP is developed, containing detailed procedures and protocols related to security for the project. The SMP describes how security will be managed and delivered, the required resources, and expected behavior from security personnel. It covers equipment, responsibilities, and security risks associated with personnel behavior and their impacts on communities.
- *Conformity with Standards and Principles:* The SMP ensures conformity with ESS4 (Environmental and Social Standard 4) regarding security personnel. It assesses the risks posed by the security arrangements for individuals within and outside the project sites. The SMP follows the principles of proportionality and Good International Industry Practice (GIIP) and adheres to applicable laws in hiring, training, equipping, and monitoring of security workers.
- *International Standards and Commitments:* The SMP includes references to relevant international standards such as the UN Basic Principles on the Use of Force or the International Code of Conduct for Private Security Providers. These standards provide guidance on the conduct of security personnel and the use of force.
- *Coordination with Other Management Plans:* The SMP is developed in coordination with other management plans, such as the Environmental and Social Management Plan (ESMP) or Stakeholder Engagement Plan (SEP). This ensures that security considerations are integrated into the overall project management framework.
- *Training and Awareness*: The SMP emphasizes the importance of regular training for security personnel, specifying the type, frequency, and completion rates. It also highlights the need for engagement with communities to raise awareness about the project's impacts on community safety and security, the Code of Conduct commitment, and the project's grievance mechanism.
- *Incident Reporting and Grievance Mechanism:* The SMP establishes clear procedures for incident reporting and receiving and following up on incidents and allegations. It includes guidelines for reporting to the Borrower and the Bank as required. The SMP also ensures the presence of a transparent grievance mechanism for project workers and the public, with clear prohibitions against retaliation for raising grievances.
- *Compliance and Audit:* The SMP document should be in a format that can be audited for compliance purposes. It includes provisions for reviewing the implementation of the SMP, including any material changes or incidents. Cost estimates for implementing the SMP are included, and the budget for the SMP may be part of the overall project budget.

Annex A: Sample Code of Conduct for Security Providers

Purpose and Scope

We, at <Insert Security Provider Name>, operate in compliance with national and international laws and corporate standards, emphasizing ethical conduct and respect for human rights. Our mission is to deliver top-tier maritime and land security solutions while upholding legal, moral, and ethical values.

Responsibility

This Code applies to all personnel and third parties representing <Insert Security Provider Name>. Compliance with laws, regulations, and ethical practices is mandatory. Violations may lead to disciplinary action, including termination.

Procedure

- ✓ *Guiding Principles:*

  We operate with professionalism, ethics, and accountability.

- ✓ *Mission and Vision:*

  Provide maritime and land security solutions with high ethical standards.

- ✓ *Conduct Business Legally:*

  Comply with all relevant legislation and avoid discrimination.

- ✓ *Conduct Business Morally:*

  Respect social norms, cultural values, and maintain a positive reputation.

- ✓ *Conduct Business Ethically:*

  Uphold professional conduct, respect all parties, and prevent conflicts of interest.

Management Commitment

Our management ensures compliance with legal and ethical standards. Every individual representing <Insert Security Provider Name> must prioritize adherence to laws, this Code, and company policies.

Compliance Is Everyone's Responsibility

- All personnel are accountable for upholding the Code.
- Reporting violations promptly is crucial.
- Retaliation against whistle-blowers is strictly prohibited.

Enforcement and Investigations

- Misconduct is addressed promptly and fairly.
- Internal investigations are conducted with confidentiality.

- Cooperation with external investigations is mandatory.

Ethical Policies

- *Human Rights:*
  - Uphold human rights and comply with international laws.
- *Human Trafficking and Anti-slavery:*
  - Prohibit trafficking and slavery in all forms.
- *Anti-Sexual Exploitation, Abuse, and Gender-Based Violence:*
  - Maintain a zero-tolerance policy.
- *Child Labor:*
  - Protect children from exploitation and report any violations.

Workplace Practices

- *Discrimination:*
  - Promote diversity and equal opportunities.
- *Harassment:*
  - Prohibit all forms of harassment.
- *Workplace Violence:*
  - Maintain a violence-free environment.

Health and Safety

- Prioritize health and safety in the workplace.
- Comply with all health and safety laws and regulations.

Alcohol and Drugs

- Maintain a drug and alcohol-free workplace.
- Prohibit the use of alcohol and illegal substances during work hours.

Environment

- Commit to environmental sustainability.
- Reduce, recycle, and dispose of resources responsibly.

Personnel

- Ensure fair selection and vetting processes.
- Continuous training and performance evaluation are key.

Annex B: Rules for the Use of Force / Graduated Force Response

Introduction

This sample Rules for the Use of Force is to be used where a Private Security Provider selected to provide security services in support of SESRP does not have an existing Rules for the Use of Force that meets SESRP requirements.

These Rules for the Use of Force set out guidelines for a graduated response by armed security personnel to any actual, perceived, or threatened act of violence against SESRP personnel, locations, assets, or communities in which SESRP operates (and as authorised by the PIU).

No armed personnel shall be deployed in support of SESRP without a detailed Security Risk Assessment being completed that demonstrates a clear need, and that the deployment of armed guards shall not be an alternative to implementing structural, procedural, or other actions to minimise risk.

Scope

The general requirements of any Rules for the Use of Force should be that they are;

- By Federal and State law and regulation;
- Consistent to protect and defend personnel, communities, and project assets;
- Consistent with the use of force only being used when essential, and then using the minimum level necessary;
- Allow a graduated response plan that is reasonable and proportionate;
- Clearly define roles and responsibilities of the PIU, Contractor, and the security personnel;

PMSC and PCASP Obligations

The Rules for the Use of Force should reflect the obligations imposed and agreed upon under any contract/agreement. They should ensure that armed security personnel confirm that they understand these obligations. The RUF should contain guidance for armed security personnel.

- Are trained and qualified to relevant documented standards in the appropriate use of force by Somaliland law.
- If they use force, it is in a manner consistent with applicable law;
- If they use force, it does not exceed what is strictly necessary;
- Use of force is proportionate and appropriate to the situation;
- Have unambiguous instructions and training on when and how force may be used; and
- Take all reasonable steps to avoid the use of lethal force.

Self-Defence and the inherent right to exercise it

The Rules for the Use of Force should reflect that Security Personnel shall always be responsible for any decision to use lethal force, including targeting and weapon discharge, by the Rules for the Use of Force and applicable national law.

Individuals have a right to use reasonable force to prevent a serious crime and the right to use force in their self-defence, and the Rules for the Use of Force reflect these rights as appropriate.

Graduated and Proportional Defence

The Rules for the Use of Force reflect the following guidance on graduated and proportional use of force.

Principles

- To enable the graduated approach and command and control of the situation, the force must be necessary and proportional.
- Respect for human dignity and the human rights of all persons should prevail; and
- Attempts at non-violent means should be applied first.

Non-violent measures

Examples of non-violent means for consideration are:

- Presence – being visible to potential attackers;
- Visual – providing a visible warning to deter attackers;
- Sound – the use of megaphones or shouted warnings;
- Show Intent – showing weapons and raising them to indicate intent to use.

Weapon status

Firearms are to be stored securely when not in use and issued only to security personnel on duty.

The Rules for the Use of Force consider “states of readiness” for the security personnel. It is suggested that there should be three states for consideration:

- Normal – Firearms are issued to on-duty personnel with no magazine attached or rounds chambered
- Heightened – Firearms have a magazine inserted but no round chambered; and
- Stand-to-stand security personnel chamber rounds but ensure safety catches are applied and they are prepared to respond to a threat.

Use of Lethal Force and Opening Fire at a Person

Lethal force should be used only as a last resort and by the abovementioned principles. The circumstances in which deadly force in self-defence can be used will vary. Such circumstances may include an armed attack on SESRP personnel, communities, assets, or sites where the attackers are, for example:

- Firing directly at persons or persons at a site where the attackers have failed to heed warnings or other deterrent measures (assuming there was sufficient time for such measures).
- Preparing to fire or firing at SESRP personnel, communities, assets, or sites whilst demonstrating an intention to draw closer to the site.

If security personnel open fire, they should.

- Fire aimed shots to stop the attack;
- Fire the minimum number of rounds necessary to stop the attack; and
- All precautions should be taken not to injure anyone other than the targeted person.

Incident Reporting and Investigation

Districts/Regions are primarily responsible for investigating, prosecuting, or extraditing for prosecution persons suspected of committing crimes under national and international law.

To implement their obligation to protect human rights, it is necessary to investigate and prosecute potential violations of national laws that aim to protect the right to life. Additionally, the government should ensure that PSPs establish, implement, and maintain procedures for reporting and investigating any incident, as without such reporting, accountability is not possible. In the case of incidents involving the use of force or the use of weapons, any casualties, physical injuries, or allegations of abuse have to be promptly reported to the nearest precinct (District/Region authorities).

The PSP should monitor, investigate, take disciplinary sanctions, and provide remedies where required. Investigations must be conducted expeditiously and impartially, with due consideration to confidentiality and restrictions imposed by national law. The investigation must establish what happened, identify the root causes, and determine the corrective and preventative actions that may be taken, including disciplinary sanctions and vetting as required. All incidents investigated shall be reported to the competent authorities. Companies should:

- Report any crimes or reasonable suspicion of crimes, including international crimes, to competent authorities;
- Prepare incident reports whenever PSP personnel are involved in using a weapon.
- Establish incident monitoring, reporting, investigation, disciplinary arrangements, and remediation procedures, particularly for cases involving the use of force and/or weapons.

Annex C: Security Requirements in Procurement

1. Overview

Security is critical in procurement, particularly for projects involving multiple stakeholders such as contractors, project workers, affected communities, and government bodies. Contractors bidding for and selected to execute project activities must comply with rigorous security measures to mitigate risks and ensure operational continuity.

Security requirements in procurement ensure that:

1. Project workers and affected communities remain safe.
2. Project assets are protected from theft, vandalism, or destruction.
3. Security risks are proactively assessed, managed, and mitigated.
4. Project timelines are not compromised due to security challenges.
5. A structured response mechanism exists for security incidents.

---

2. Duty of Care

The Duty of Care mandates that all parties involved in the project, particularly the Project Implementation Unit (PIU) under the Ministry of Energy and Minerals (MoEM) and contractors, must take reasonable steps to ensure the safety of workers and other stakeholders.

Contractor's Duty of Care Responsibilities

- Align security practices with national labor laws and international best practices (e.g., ISO 31000).
- Implement safety protocols to minimize risks to workers.
- Ensure contract security personnel follow ethical guidelines.
- Provide adequate resources (e.g., protective equipment, emergency response plans).
- Maintain clear communication with the PIU to report and address security concerns.

---

3. Security Risk Assessment (SRA)

Before executing project activities, contractors must conduct a Security Risk Assessment (SRA) to evaluate potential risks in the project area.

Key Elements of the SRA

- Identification of Threats: Evaluate internal and external risks to staff, communities, and assets.
- Risk Categorization (based on ISO 31000):
    1. Political Risks

2. Cultural Risks
3. Safety Risks
4. Criminal Activity
5. Extremist Activity
6. Communal Violence
7. Vested Interests

- Continuous Monitoring: Regularly update the SRA to reflect changing security dynamics.
- Documentation: Maintain records of assessments and mitigation actions.

---

4. Security Management Plan (SMP)

The Security Management Plan (SMP) is a blueprint for managing security risks throughout the project lifecycle.

Implementation of the SMP

- Must align with both the Project SMP and specific site-level SMPs.
- Contractors may propose alternative security measures if original plans are unfeasible, provided the same level of protection is maintained.
- Collaboration with local security authorities is encouraged where necessary.

Key Components of a Contractor's SMP

1. Security Governance: Define roles and responsibilities.
2. Threat Analysis: Identify and assess threats.
3. Preventive Measures: Include patrols, surveillance, and access control.
4. Incident Response Plan: Detail response procedures, including evacuation.
5. Crisis Communication: Establish protocols for reporting incidents.

---

5. Security Requirements in Bidding Documents

During procurement, contractors must demonstrate their capacity to meet security obligations.

Mandatory Security Submissions

Contractors must provide:

1. Demonstration of Security Capability: Show the ability to implement the Project SMP.
2. Nomination of a Security Focal Point (SFP): Include CV with relevant experience.
3. Budget Allocation: Provide a detailed security budget (personnel, equipment, etc.).

Post-Contract Award Obligations

Once a contract is awarded, the contractor must:

- Develop and submit an Activity/Site SMP for PIU review.
- Revise SMP based on PIU feedback (at their own cost).
- Comply with any new security directives from PIU or regulators.

---

6. Suspension of Delivery Activities

Contractors reserve the right to temporarily or permanently suspend operations if:

- Security risks exceed acceptable thresholds.
- Personnel or community safety is compromised.

Conditions for Suspension

- Must align with the Security Management Framework.
- Require consultation with PIU and the World Bank (unless an immediate threat exists).
- Suspension triggers (e.g., violent incidents, curfews) must be outlined in the Activity/Site SMP.

---

7. Additional Security Considerations

Personnel Selection, Vetting, and Training

- Contractors must conduct background checks and interviews.
- Provide training in security awareness, emergency response, and conflict resolution.
- Security staff must act ethically and within legal bounds.

Community Engagement

- Develop engagement strategies to prevent conflict with local populations.
- Implement early warning systems with community involvement.

Use of Technology

- Integrate surveillance, GPS tracking, and secure communications.
- Use digital systems for incident tracking and reporting.

---

8. Conclusion

Security in procurement is vital to the successful and safe execution of project activities. Contractors must demonstrate their ability to assess, mitigate, and manage security risks effectively.

By adhering to these security requirements, contractors contribute to:

- Reduced security risks and operational disruptions.
- Enhanced project credibility and stakeholder confidence.
- Timely and safe project delivery.

Failure to comply with these requirements can result in delays, financial loss, and reputational damage. A proactive, well-structured approach to security is essential for seamless procurement and project implementation.

Annex D: SESRP-related incident and accident reporting procedure.

Purpose

This procedure aims to outline the requirements, methods, and outcomes ofreporting all incidents and accidents.

Scope

The following incidents and accidents will be reported, irrespective of the nature and level of severity:

- Fatality and critical injury/illness, or injury for which an employee receives/seeks medical attention.
- First aid treatment, occupational disease,
- Property damage and fire
- Environmental release (chemical spillages) and social risks (outlined in the project ESMF)
- Explosions
- Exposures to biological, chemical, or physical agents and other related factors.

Roles and Responsibilities

Security advisor, Environmental and Social Safeguard Specialists, and Project Coordinator

- Security Advisor shall regularly monitor and follow up on project-related security incidents and accidents.
- Environmental and Social Safeguard Specialists shall continue to monitor and follow up on project-related environmental, societal, OHS, incidents, and accidents.
- All project-related incidents and accidents shall be reported within 48 hours to the Project Coordinator
- All templates for incident and accident reporting will be provided. Ensure that all templates are completed.
- Ensure injured or ill employees have received the required medical treatment and regularly update their health status to the PIU.

Contractors, security, Environmental and Social Safeguard Focal Persons

- Shall continuously monitor and follow up on project-related incidents and accidents.
- Report the case to local administration entities and relevant bodies.
- Ensure the injured persons have received the required medical treatment.
- Ensure Incident/accident Templates are completed.
- Report the incident/accident within 24 hours to the Project Implementing Unit (PIU) at MoEM

Communication

This procedure shall be communicated to all project PIUs, contractors, subcontractors, and relevant bodies.

Evaluation

Compliance with the accident /incident reporting procedures is monitored regularly by security, environmental, and social safeguard specialists, as well as environmental and social safeguard focal persons.

Annex E: Security incident registration form for sub-projects

Project Name----------*Region* ---------- District----------

Date	
Section **A***: recorder /investigator*	
Name	Position
Section **B*****:*** *Incident description*	
Date and time of incident:	
Location of incident:	
Detailed description of the incident:	
Detailed description of the incident from an eyewitness:	

Section **C:** *Identify the root cause: What caused the incident?*
Section **D:** *Action taken to mitigate incidents:*
Section **E:** *Recommended corrective action to prevent future:*

Annex F: Occupational Health and Safety Incident Registration Form

Project Name----------Region---------- District ----------

Date		
Section **A**: *recorder /investigator*		
Name	Position	
Section **B**: *Incident description /injury information*		
Name of injured employee	Age	Sex
Employee`s job title		
Date and time of incident:		
Location of incident:		
Detailed description of the incident:		
Detailed description of the incident from the eyewitness:		
Section **C:** Identify the root cause: What caused the incident?		
Safety procedures were not followed---------- Machine failed or safety equipment failed ---------- Lack of proper training (use of the PPE, the machine, or other equipment for work) ---------- Other, specify……		
Recommended corrective action to prevent future incidents		

Corrective Action Taken/Root cause addressed.