THE FEDERAL DEMOCRATIC REPUBLIC OF ETHIOPIA

Security Management Plan (SMP)

Response – Recovery – Resilience for Conflict Affected Communities in Ethiopia (3R-4-CACE)

August 2022

Table of Contents

List of Tables

Acronyms & Abbreviations

3R-4-CACE	Response – Recovery – Resilience for Conflict Affected Communities in Ethiopia
ACLED	Armed Conflict Location & Event Data
C-IED	Counter Improvised Explosive Device
CMT	Crisis Management Team
EDF	Ethiopian Defence Forces
EOD	Explosive Ordinance Disposal
ERW	Explosive Remnants of War
ESCP	Environment and Social Commitment Plan
ESSF	Environmental and Social Standards Framework
GBV	Gender Based Violence
GoE	Government of Ethiopia
HROC	High Risk of Ongoing Conflict

ICT	Information and Communication Technology
IDF	Indirect Fire
IED	Improvised Explosive Device
MoF	Ministry of Finance
NROC	Non-High Risk of Ongoing Conflict
PCP	Project Continuity Plan
SEA	Sexual Exploitation and Abuse
SMP	Security Management Plan
SOP	Standard Operating Procedure
SRA	Security Risk Assessment
UAG	Unknown Armed Groups
UNICEF	United Nations International Children's Emergency Fund
UNOPS	United Nations Office for Project Services
UXO	Unexploded Ordnance
PCU	Project Coordination Unit
PIU	Project Implementation Unit
RTA	Road Traffic Accident
WASH	Water, Sanitation and Hygiene
WBG	World Bank Group
WNCCA	Woreda Needs, Conflict, and Capacity Assessments

1. Objective

The purpose of this plan is to provide an overview of the security threat and safety and health hazards that may impact the Response – Recovery – Resilience for Conflict Affected Communities in Ethiopia (3R-4-CACE) Project and to explain the means by which these are threats and hazards are managed and mitigated.

This security management is concerned with reducing risk, and it does not guarantee that incidents will not occur. It is also subject to adaptation and adjustment in line with situational judgement.

Overall responsibility for the safety and security of the project is held by: Project Coordinator

Responsibility for the safety and security management will be held by: Project Security Manager

The Security Management Plan (SMP), aside from operational good practice, is a required by the World Bank Group (WBG) as part of its Environmental and Social Standards Framework (ESSF). It is intended to be a practical document that can be implemented by a range of personnel.

This SMP aims to provide an overview of the current security situation in Ethiopia and the operational backdrop against which the 3R-4-CACE Project will be carried out. It will then identify key threats and hazards that emerge out of that context and analyse them in terms of their likelihood of occurrence and forecasted impact on the 3R-4-CACE Project. An overview of mitigation and management methods will then follow, with the intent that these will provide a baseline of measures to be implemented in the field, with adjustments as necessary to reflect conditions on the ground.

Part of this plan:

- Annex 1: Security Risk Assessment (SRA)
- Annex 2: Standard Operating Procedures (SOPs)
- Annex 3: Project Continuity Plan (PCP) and PCP Tool

2. Scope of Security Management Plan

This plan is to cover all aspects of the 3R-4-CACE project. Project spending comes with an associated duty of care responsibility by the Project Coordination Unit (PCU) of the Ministry of Finance, and the World Bank Group.

The Project objectives are twofold:

(i) To rebuild and improve access to basic services and climate-resilient community infrastructure

(ii) To improve access to multi-sectoral response services for Gender-Based Violence (GBV) survivors; in selected conflict-affected communities in Ethiopia.

2.1 Activities

The activities forecasted for project implementation are varied and will depend on the requirements of each location. However, broadly speaking, the following activities may reasonably be expected to be carried out, and will be considered for the purposes of this SMP:

- Mobile health services
- Provision of essential medicines
- Rapid renovation of health, education, and WASH facilities
- Speed learning activities (read@home)
- Water trucking
- Community care centres
- Rapid need assessments
- Capacity building activities
- Renovating, reconstruction and building new social services
- Provision of hygiene materials
- Hygiene education
- One-Stop-Centres and other GBV activities, including shelters
- Small-scale infrastructure investments

2.2 Covered Persons

See Labour Plan for additional information on labour considerations.

Largely, personnel covered by this SMP fall into one of four categories:

1) Personnel employed by the Government of Ethiopia to implement the project and its activities
2) Staff of partner organisations, such as UNICEF and UNOPS
3) Personnel of their subcontracts or implementing partners
4) Beneficiaries of the project and local communities

2.3 Locations

The 3R-4-CACE will be implemented in a range of locations and contexts. The proposed Regions in which the project will be initially implemented are the Tigray, Afar, Amhara, Benishangul Gumuz and Oromia Regions, with target woredas and kebeles pending the damage assessment report (anticipated in June 2022).

Each region presents its own unique context and history, as well as massive variation of operating environments within the Regions. These include but are not limited to:

- Urban areas
- Remote rural areas
- Non-Government controlled areas
- Volatile regional border areas
- Areas in which insurgencies and counter-insurgency military operations are ongoing
- IDP camps, including of mixed ethnicities
- Sudanese border areas

For the purposes of the project, woredas will be divided between High Risk of Ongoing Conflict (HROC) and Non-High Risk of Ongoing Conflict (NROC) areas, as determined by the Woreda Needs, Conflict, and Capacity Assessments (WNCCA). In the case of HROC areas, third-party organisations (including UNOPS and UNICEF) will be responsible for implementation. This plan describes the *minimum* Safety & Security requirements to be implemented, and may be superseded by the arrangements of partner organisations, and a gap analysis may be required for partners who do not meet these requirements. However, given the nature of the situation in all targeted Regions, this designation between HROC and NROC may be subject to rapid change with little or no notice, as conflict lines are fluid and in most cases of an insurgency type.

2.4 Assets

Listed below are the assets required for project implementation, the security of which this SMP will seek to maintain.

- Vehicles (either rented or purchased)
- ICT equipment (including mobile phones and laptops)
- Construction materials
- Buildings and property (rented or purchased)
- Beneficiary Data
- Project Personnel Data
- Cash

The Use of use/storage of weapons shall be based on the national military rules/guidelines. Use of force, however, should be aligned with ESS4 and UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials.

3. Institutional Arrangements and Decision-Making Processes

The 3R-4-CACE Project is implemented by the Ministry of Finance (Project Coordination Unit - PCU) of the Government of Ethiopia, along with the Ministry of Women's and Social Affairs (Project Implementation Unit - PIU).

Responsibility for the security risk management of the project, its personnel, activities, assets and reputation lie with the PCU, Ministry of Finance. Safety and security incidents must be reported to the World Bank Group within 48 hours as indicated in the 3R-4-CACE Project Environment and Social Commitment Plan (ESCP) and detailed full report should be prepared then afterwards

Decisions regarding contingency, emergency, and crisis decision making will be made by the PCU in the first instance, in consultation with the WBG

4. Security Management Approach

The safety and security of the Project will rely heavily on community **acceptance** and buy-in of Project activities, as stated in the Project Appraisal Document, "Close engagement with local communities will be favoured over a militarized approach to security". It will rely on almost continuous assessment of the situation, and draw heavily on a wide range of information sources and contact networks in order to **avoid** as much as possible exposure to threats and hazards, with mitigation measures in place to **control** risks, where avoidance is not possible. Deterrence approaches – including the use of armed security forces - where an option, should be carefully considered in light of the threat (be that criminal or armed conflict in nature), nature of program activities involving vulnerable persons and conflict-affected communities, the optics and reputational impact, and tactical advantage provided should armed force be necessary.

The security management approach might differ between HROC and NROC regions, given that HROC implementation is likely to be conducted by a third-party (likely UNICEF). In HROC regions, the use of use/storage of weapons shall be based on aligned with ESS4 and UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials. In addition to the aligning with ESS4 and UN Basic Principles, the use and storage of weapon in NROC shall be based on the national military rules/guidelines.

The Project Coordinator ultimately holds responsibility for the security management of the Project.

The Security Focal Point is to ensure that security procedures are designed, updated, and disseminated amongst relevant Project staff, and captured as necessary in external party agreements, such as with partners, service providers or contractors. Additional responsibilities include:

- Tracking the safety and security situation and providing this information to PCU staff in the field/ at all levels.
- Provide technical advice, assessments and support to Project staff in the field on subjects such as building security measures and journey management.
- Lead and coordinate incident response and management
- Build and maintain a network of contacts across sectors and operating areas for support, information gathering, and stakeholder engagement purposes
- Brief staff on a regular basis on the security situation
- Update the existing SRA, and conduct location specific SRAs as necessary
- Supervision and monitoring of guarding and other security personnel as applicable

4.1 Existing Standards and References

This Security Management Plan will be based on and refer to the following literature:

- WBG Environmental and Social Standard 1
- WBG Environmental and Social Standard 4
- 3R-4-CACE Project Appraisal Document
- 3R-4-CACE Project Social Assessment
- 3R-4-CACE Project Environment and Social Commitment Plan (ESCP)
- HPN Operational Security Management in Violent Environments, December 2010
- UN Minimum Operating Security Standards, 2009
- UNSMS Security Policy Manual, 2016
- UNDSS DO and SMT Handbook, 2020
- IFC & WBG Environmental, Health, and Safety (EHS) Guidelines
- IFC Good Practice Handbook on Use of Security Forces: Assessing and Managing Risks and Impacts
  ISO 31000:2018 Risk management — Guidelines
  WBG Good Practice Note: Assessing and Managing the Risks and Impacts of the Use of Security Personnel.

4.2 Security Situation Overview

Though the security risk situation has improved in the last six months, significant operational challenges remain. According to the Armed Conflict Location & Event Data (ACLED), the five targeted regions have seen the highest numbers of conflict and security incidents in the last six months (November 2021 – April 2022), with Oromia, Amhara and Afar having incident numbers well into the hundreds. The majority of these have been conflict in nature, and whilst direct targeting of aid and development staff has reportedly been minimal, direct targeting of government staff has been reported, and such conflict activity suggests a considerable threat of collateral damage to reconstruction operations in these Regions.

Further, the broad scope of the project will likely take implementation into a range of operating environments, including:

- Urban areas
- Rural areas
- Non-Government controlled areas
- Volatile regional border areas as areas of control fluctuate
- Areas in which insurgencies and counter-insurgency military operations are ongoing
- IDP camps, including of mixed ethnicities
- Sudanese border areas

4.3 Security Risk Assessment (SRA)

At the heart of security management planning is the identification and understanding of possible events or developments that could cause harm to personnel, assets, activities and the reputation of the enterprise. Annex 1 of this document contains the full risk assessment report, summarised here.

A Project Security Risk Assessment process should be carried out on annual basis, following significant change in the threat or operating environment, or significant change in project modality. This is including but not limited to:

- Expansion to other Regions
- New project activities
- Engagement of additional/ new implementing partners

Before starting activities in a new location, an SRA should be carried out to identify the threats and hazards specific to those areas. It is the responsibility of the PCU to ensure such assessments are carried out.

Table 1: Risk Analysis Matrix and Impact Rating

Likelihood	VERY Likely	LOW	MEDIUM	HIGH	VERY HIGH	UNACCEPTABLE
	Likely	LOW	MEDIM	HIGH	HIGH	VERY HIGH
	Moderately Likely	LOW	LOW	MEDIUM	HIGH	HIGH
	Unlikely	LOW	LOW	LOW	MEDIUM	MEDIUM
	Very Unlikely	LOW	LOW	LOW	LOW	LOW
Risk Analysis Matrix		Negligible	Minor	Moderate	Severe	Critical
		Impact				

Impact rating	
Negligible	Little disruption to activities, no injuries to personnel, and no damage to assets
Minor	Delays to activities OR injuries/ possible stress to personnel (no medical attention required) OR possible damage or loss of assets
Moderate	Delays to activities (<7 days) OR non-life-threatening injuries/ high stress OR some loss of damage to assets
Severe	Significant disruption to activities (7 days +) OR severe injuries to personnel requiring emergency medical attention OR significant loss of assets
Critical	Cancellation of activities OR death/ severe injuries to project personnel OR major/ total loss of assets

Table 2: SRA and Proposed Mitigation Summary

Security Threats	Details	3R-4-CACE Project Exposure	Unmitigated Risk Rating	Proposed Mitigation Measures	Residual Risk Rating
Criminal targeting of Project assets (robbery/ theft)	Opportunistic and organised criminal activity amidst increasing prices and cost of living, possible resulting in the injury of personnel	The project will require vehicles, equipment, and cash for implementation, as well as use of building materials, all of which may be attractive to criminal actors Further, given the high-profile nature of the project and associated funding, could increase attractiveness to adversaries	High	▪ Access control in place at all sites, as far as reasonably practicable ▪ Use of unarmed guards/ watch people at project sites ▪ Asset management procedures, including inventories ▪ Secure storage of assets, such as warehousing, as outlined in the SOPs ▪ Seek insurance for high value items ▪ Recruit dedicated security coordinator to oversee mitigation measures and incident management ▪ Cultivate strong culture of incident reporting and follow-up	Medium
Sexual Exploitation & Abuse (SEA) of project personnel/ beneficiaries	Sexual violence – including verbal and physical assault and harassment affecting Project personnel and/or beneficiaries	Although SEA concerns can affect all genders, women are disproportionately impacted and women employees, partners and service providers will be pivotal for project implementation.	High	▪ SEA briefings for all staff as part of safeguarding measures ▪ Incident reporting structures formalised and communicated, both to staff and beneficiaries ▪ Pre-identify possible sources of psychosocial, medical and other support for survivors in all areas of implementation	Medium
Unexploded Ordnance (UXO) / Explosive Remnants of War (ERW) contamination	As the result of both current and historical conflicts, devices (projectiles, mines, IEDs, ammunition) that have not detonated on impact, which could explode if disturbed Potential for death or injury to people and	Possibility of encountering UXO/ ERW during construction activities, causing significant damage, injury or death to project personnel and assets. Schools and health facilities have been identified as sites of particular concern due to their use during conflict activities.	Unacceptable	▪ Identify key contacts in UNMAS and other demining agencies, as well as C-IED/ Search military units ▪ Ensure all staff are trained on UXO/ERW Awareness, and contracted labour are briefed on the UXO/ERW threat ▪ Pre-identify medical facilities in all areas of operations, investigate and test their facilities ahead of implementation ▪ Ensure at least one staff member on site is first aid	Medium

	animals in the vicinity			trained, with a first aid kit available	
Collateral harm to project personnel/ damage to project assets	Conflict activity - e.g., airstrikes, armed clashes, inter-communal violence, IDF - is ongoing in all proposed Regions of operation and may result in non-deliberate harm to personnel or damage to assets/ sites.	Project implementation will be widespread, and given the sporadic nature of the conflict, situations can be volatile and subject to rapid change. Exposure to 'wrong place, wrong time' type incidents are thus a key concern.	Very High	▪ Cultivate strong community relationships and information sources ▪ Coordination and deconfliction with Ethiopian Defence Forces and regional armed forces ▪ Ensure pre-departure checks are carried out ahead of all journeys ▪ Recruit dedicated security coordinator to oversee mitigation measures and incident management	Medium
Abduction/ illegal detention of project staff	The detention by personnel by non-state actors against their will. This may be followed by a ransom demand, creating a kidnapping situation driven by criminal rather than political intent.	Given the high-profile nature of the project, personnel may be seen as valuable in pursuing interests of certain groups. Similarly, personnel may be of interest for criminals hoping to extract a ransom. Given the widespread implementation of the project, and likely time spent in transit, abduction is a possibility for project staff in the field.	High	▪ Recruit dedicated security coordinator to oversee mitigation measures and incident management ▪ Train a crisis management from senior project leadership ▪ Cultivate strong community relationships and information sources ▪ Employ journey management procedures, including route and destination checks prior to departure ▪ Use of armed escorts when specifically recommended as absolutely necessary	Medium
Harassment of project staff	Disgruntled beneficiaries, host communities or other stakeholders may target Project staff. Harassment may be verbal, with the potential to escalate into physical assault.	Inevitably some communities or groups may receive assistance over others, or perceive unfairness in the assistance provided. Delays, changes of plan, and miscommunication may also lead to a deterioration in community relations.	High	▪ Recruit dedicated security coordinator to oversee mitigation measures and incident management ▪ Prioritise community engagement and communications ▪ Cultivate strong culture of incident reporting and follow-up ▪ Identify 'Red Lines' that will lead to a cessation of activities, and discuss these with communities	Medium
Demonstration/ civil unrest in project areas	Disgruntled beneficiaries, host communities or other stakeholders may mobilise.	Inevitably some communities or groups may receive assistance over others, or perceive unfairness in the assistance provided.	Medium	▪ Recruit dedicated security coordinator to oversee mitigation measures and incident management ▪ Develop headcount and staff check-in procedures, as well as activity suspension and hibernation protocols	Low

	Demonstrations may occur for other, non-project related reasons that may disrupt activities, e.g. causing roadblocks. Possible to also escalate to harassment or assault of staff, or damage to project assets or sites (see below)	The scale of the project may take it into areas where there are social tensions that could ignite.			
Vandalism/ deliberate destruction of project assets or sites	Criminals, disgruntled personnel, or unknown armed groups may deliberately target project assets or sites, possibly to express grievance or issue a warning/ threat.	Operations in a range of settings, including those where there are competing interests between groups and possible grievance with the project.	Low		
Direct targeting of project staff	Deliberate killing or injury of personnel involved in government reconstruction and recovery activities by unknown armed groups. Escalation of harassment by or tensions with beneficiaries or host communities, resulting in violence.	Project implementation will be widespread, with those in most need possibly in the most remote places within the reach of UAG actors. Fluctuating presence and areas of control may create a challenging stakeholder engagement/ access negotiation environment Inevitably some communities or groups may receive assistance over others, or perceive unfairness in the assistance provided.	Very High	▪ Recruit dedicated security coordinator to oversee mitigation measures and incident management ▪ Engage local communities and other stakeholders for investment in project success, including deployment of confidential grievance redress mechanisms and consequences for when security guarantees are not met (Red Lines) ▪ Pre-departure checks on field travel ▪ Encourage staff to report on context dynamics and cultivate informal information gathering mechanisms ▪ All staff must report safety and security incidents, no matter how minor, as possible indicators of more significant problems	Medium

Operational & Safety Hazards	**Details**	**3R-4-CACE Project Exposure**	**Untreated Risk Rating**	**Proposed Mitigation Measures**	**Residual Risk Rating**
Covid-19 and other medical	Malaria, food poisoning, Covid-19, HIV/AIDS,	Project personnel will be in close proximity to others, particularly in	Medium	▪ Brief all staff on possible medical concerns ▪ Pre-identify medical facilities in areas of project	Low

concerns	Tuberculosis (TB) and dengue fever are among the medical conditions that can effect personnel, causing a risk of death or serious illness.	large numbers. Medical attention may be inaccessible in some areas where activities are planned, making treatment difficult and raising the possibility of serious illness.	🟨	implementation	🟩
Dangerous wildlife in project areas	Biting and venomous insects, wild dogs, hyenas, snakes and other hazardous fauna present a risk to personnel.	Project activities in rural areas have a heightened risk of encountering dangerous animals.	Low		
Road traffic accidents (RTA)	Collisions involving vehicles and in some cases pedestrians.	As the project will involve travel by road for some activities, the exposure to RTA is significant.	High	▪ Train and monitor the performance of drivers, with disciplinary action linked with incidents where the driver is at fault (e.g. speeding) ▪ Vehicles equipped with emergency kit, including first aid kits ▪ Communications PACE planning ▪ Consider insurance for vehicles ▪ Set and brief staff on procedures, for instance, should a project vehicle hit a child	Low
Safety hazards at project sites	Hazards such as falling objects, trip hazards, accidental fire, sharp objects, falls, misuse of construction tools.	Project activities include reconstruction and renovation of health, education, and other facilities. WASH programming may also include construction activities and excavation.	High	▪ Employ and encourage good practices on site, such as fencing off excavations, keeping the site tidy and proper training on the use of tools ▪ Ensure project staff are equipped with adequate PPE ▪ When working with contractors, ensure safety obligations are captured at contracting stage ▪ Ensure fire safety equipment and procedures are in place at all sites ▪ Least hazardous materials should be preferred, and where necessary to use, hazardous materials must be handled and stored correctly ▪ Safety hazards must be managed in line with WBG EHS	Low

				Guidelines.	
Flooding	The Ethiopian rainy season can lead to extensive flooding, even in urban areas where there is continuous attention to infrastructure. In rural areas, roads and other infrastructure may become unusable by vehicles or damaged. Deterioration in road conditions may also lead to increased risk of RTA.	Construction activities rely on weather conditions to some extent, including delivery of materials. Road travel will be integral to project activities, and may be disrupted by flooded routes and increased RTA numbers.	High	▪ Pre-departure route checks as part of journey management ▪ Stock vehicles with appropriate emergency kit and communications ▪ Identify alternative routes to destinations ahead of travel	Low

4.4 Mitigation Measures

Having identified the key safety and security threats and hazards to personnel involved in the Project, appropriate security risk mitigation measures must be identified, and their implementation planned for. The mitigation measure here should be treated as a baseline guide, to be adapted to operational reality as necessary, but never entirely abandoned.

Security risk mitigation usually falls into one of the following categories:

- **Transfer**
  Shifting the forecasted damage from one party to another. This might include the use of insurance to transfer possible financial losses to an insurance provider, or the use of an implementing partner better equipped to deal with the security risks expected to be encountered.
- **Control**
  Achieved through the use of procedures and other means, resulting in lowering either the impact of an undesirable event occurring, or reducing the likelihood of it happening in the first place. Note that even in the face of strict controls, risk can never be fully removed from an operational undertaking, and some degree of risk is inevitable.
- **Accept**
  Nothing is done, with the potential damage being considered acceptable.
- **Avoid**
  The circumstances in which the risk is assessed as being more likely are avoided. For instance, if RTA is identified as a key hazard, then road travel will not be undertaken.

5. Use of Public/Private Security Force

In Ethiopia, public properties are protected by the government security forces either by federal police forces or regional security personnel. Similarly, based on the agreement with the regional and federal governments, the public security forces will protect the project resources and staffs depending on the local context. The PCU under the MoF and PIU in the MOWSA will discussed and contract with federal or regional police commissioners on these requirements. All the engagement process and discussion outcomes with the police will be recorded. A log of all relevant meetings will be kept for the project.

5.1 Public Security Personnel Role

The followings are the security personnel roles:

Interruption: this refers to the deployment of response force personnel to disrupt an attack by making their presence known to the adversaries in an attempt to disrupt their attack and encourage them to give up on their objective and exit the site before they are detained. This could also include verbal commands or instructions, either in person or via a Personal Address system. Since the Disruption strategy does not require physical confrontation with adversaries, it is appropriate where security personnel have limited capability or are constrained in their actions by regulatory issues. However, it is only likely to be effective against opportunistic attackers since those with any real determination can chose to ignore the presence of the response force or their verbal instructions

Counteraction: this refers to physical intervention by security personnel and actions to counter an attack by an adversary. Examples of Counteraction include physically blocking the adversary's path, the use of reasonable force to prevent them from executing their attack and/or detaining them for subsequent arrest by Police. To be effective against some forms of threat, it may also require the use of armed security personnel. It is vital that the type of actions permissible by security personnel is clearly defined within their assignment instructions and training and does not contradict any laws or regulations of the locality.

Containment: the third main response strategy that can be adopted is containment, which attempts to contain the incident, usually until such a time. Actions could range from simply monitoring adversary actions to allow External Response Forces to be effectively briefed on arrival and recording these actions in support of post-incident investigation and evidential proceedings through to shutdown of vulnerable processes and partial or full evacuation of the site to mitigate the potential consequences of the event that is about to occur.

5.2 Agreement between the PCU/PIU and Police Commission

An agreement will be made between the PCU/PIU and police commission regarding the project site security issues. The project will provide the financial or resourcing issues (such as housing, vehicles, office phone/Airtime card for key personnel, and food allowance accommodation) for all the deployed security staff. The project coordinator and security specialist will approve the identified costs. If required, the PCU will construct security posts and will provide necessary facilities at each post. The security forces will dwell in the existing camp (commonly named satellite camp) arranged for this purpose only. In this regard, to secure the site, the deployed security personnel will cooperate with the local security forces.

5.3 Monitoring

The project will monitor and understand the type of response public security forces are likely to use. Some public security forces are well trained and will respond professionally and proportionately to a threat; others may present a risk of unprofessional conduct or excessive force, which can be exacerbated if the forces include new recruits with limited training and experience. The security personnel must perform professionally and appropriately to the threat. The federal or regional police will check to confirm that policies and procedures remain relevant, and that the forces are aware of and following them. The police commission is required to consider taking appropriate discipline measures (warning, salary cut, firing or other penalties) against the offender to maintain leverage when the member/s deployed security forces do not meet the code of conduct stated in this plan.

5.4 Security Personnel Background Screening

The project will attempt to understand the background and reputation of public security forces to be deployed as part of their assessment of security risks and will monitor the situation so they can respond if any issues arise with certain individuals or units. The police commission must address potential problems by filling gaps through training or equipment, or but should avoid deploying security staff that have a record of any kind of abuse.

5.5 Security Personnel Equipment

The security personnel will be equipped with the required equipment to do their jobs properly and safely. This usually means a uniform and identification, and some type of communication device (typically a radio). In some cases, it includes non-lethal weapons, such as pepper spray. The decision to use lethal force, such as a gun is a serious one that needs to be decided by the security manager.

5.6 Use of Force by Security Staff

Use of force by security personnel shall be for preventive and defensive purposes proportionate to the nature and extent of the threat. It must follow the Principle of Proportionality in Security Responses. The principle of proportionality means that the intensity of any security response should correspond to the nature and gravity of the threat or offense. The security personnel must know what is expected of them. They will be prepared to react with appropriate and proportional force in any situation. The project will use their policies and procedures, reinforced by training to provide clear instructions to directly employed guards. This can be as simple as including a clause in the employment contract setting out expectations and following up with training.

5.7 Allegations of Misconduct

Allegations of abuse by deployed security forces will be conducted by the police commissioner together with security specialist. They must follow up whether the security personnel comply with the national security forces code of conduct on allegations of abuse and must take appropriate measures immediately. The PCU after receiving allegations of unlawful or abusive acts by the security personnel deployed at the project site are advised to record and report these to the pertinent authorities including the World Bank. The Police commissioner will actively monitor the status of any ongoing criminal investigations or allegation of misconduct by the deployed security forces as the commission should ensure principles of Ethiopian security forces and take immediate corrective actions for negligence.

6. Stakeholder Engagement

The SRA has been conducted as peart the Project's compressive social assessment. Stakeholders are consulted at the federal, Woreda/district and community levels. The team members in selected implementation sites/districts in the intervention regions conducted a physical observational visit. At federal level, the consultations were conducted with representative at MOF and MOWSA. Amhara and Afar regions and selected Woredas were consulted. For details on the stakeholder engagement, please refer the projects Comprehensive Social Assessment Instrument. Community members who have complaints and grievances on the security personnel including sexual exploitation and abuse cases would report to the project grievance redress mechanism (GRM). If the GRM do not able to address the cases, committee members will refer it to the security specialist/ focal person to manage the case together with the responsible police team leader or the police commissionaire.

7. Security Operating Procedures

To mitigate the risks identified in the area security risk assessments, the following procedures should be implemented by the PCU, PIU, and other third-party implementing actors. All project personnel must be aware of and familiarised with these procedures.

Procedures are detailed in Annex 2 of this document.

- SOP 01: Incident Reporting
- SOP 02: Site Security
- SOP 03: Communications
- SOP 04: Project Activities
- SOP 05: Travel Security Arrangements
- SOP 06: Security Forces & Civil-Military Liaison
- SOP 07: General Incident Management
- SOP 08: Fire Safety
- SOP 09: Abduction and Illegal Detention

8. Training

Training of personnel is a key security risk mitigation measure, as it can impart the knowledge and create the behaviours required to help keep people safe and lessen the impact and/or likelihood of security incidents taking place.

Table 3: Taring Courses and Intended Attendees

Course	Course Content	Intended Attendees
First Aid Training	Basic first aid training for use during medical situations at the workplace.	Delivered to a pool of Project staff who will be present at Project sites
Personal Security Awareness Training	Raise awareness of threats in the operating environment, SOPs (Annex 2) to mitigate and respond, communicate incident reporting practices, and provide a safe space to express concerns and thoughts on safety and security	All Project staff
Operational/ Information Security Awareness Training	Raise awareness of data protection and IT good practice to protect project data assets	All Project staff
Crisis Management Training	Scenario-based training for members of the CMT with the aim to familiarise themselves with working together, and any crisis management plans that may be in place.	CMT and backups
UXO/ ERW Awareness Training	UNMAS delivered, information on recognition of UXO/ERW and actions to take in the event of a find	All project staff, select project staff to receive Training of Trainers
Safeguarding and SEA Awareness Training	Mitigation measures and actions to take in the event of safeguarding concerns or incidents of SEA	All project staff

9. Security Management Budgeting

Dedicated funding must be made available for the implementation of security risk management measures. Total costs will vary depending on the number of sites and personnel employed on the Project.

Table 4: Security Management Budget

Item	Cost (USD)	Frequency
Project Security Manager	60,000	Annual
Training	300	Per Person
Fire Safety Equipment	250	Per Site
Guarding Services including guard equipment (if applicable)	3000	Monthly/ Per Site
First Aid Kits	100	Per Site
Hibernation kits	300	Per Office Site
Physical security measures (e.g. locks, doors, safes, window grills)	5000	Per Office Site

10. Incident Management

10.1 Reporting

Safety and security incidents – including near misses – must be reported to management as soon as possible (at least within 48hrs) and addressed appropriately according to severity and impact on personnel, assets, activities, or reputation.

Any and all incidents impacting on 3R-4-CACE assets, activities, personnel, or reputation must be reported to the MoF and WBG, including those impacting on UNOPS, UNICEF, their partners engaged in project implementation and beneficiaries during project activities.

The federal police operate under federal government, while the local security operates under regional government. The federal police directly report the federal police commission and the commissionaire reports to Ministry of Justice. Nevertheless, the local government chain of reporting system is that the kebele report to the Woreda, that Woreda to Zone, and the Zone to the regions and finally the region to federal government. The security socialist and the PCU will cooperate and work with the security force assigned to protect the project. The implementation of the SMP will be reported quarterly and annually together with the Project reporting system.

10.2 Management

Security incidents are of many types, and 'actions on' to many are detailed in Annex 2: SOPs. However, there are several good practices can be important first steps in the management of the majority of security incidents:

- Accounting for staff. This may be as simple as checking in with a staff member who experienced a theft, or a larger scale, more complex headcount operation of all staff in an area following civil unrest.
- Alerting management that an incident has taken place
- Stopping further movements in an affected area
- Considering information and data risks, for instance, in the case of a stolen laptop
- Identifying emergency contacts or next of kin for affected staff
- In cases of sexual exploitation and abuse (SEA), ensuring a survivor-centred approach at all times
- Initiating a Crisis Management Team (see below)
- Documentation of key decisions and capture of evidence for post-incident investigation and after action review purposes
- Relocation of staff and assets out of the affected area (see SMP Annex 3: Project Continuity Plan)
- During more severe and public incidents, communication both internal and external may be considered

At all times, ensuring that no further harm or damage takes place should be a priority in incident management.

10.3 Follow up

Once an incident has been managed and declared closed, follow up is vital. This includes:

- Support to victims and survivors, including possible leave requirements, medical care, or psychosocial support
- Conducting an After-Action Review of the incident, to identify lessons learnt and opportunities to improve risk management practices

11. Project Continuity and Contingency Planning

Contingency Planning and Project Continuity is discussed in greater detail in Annex 3: Project Continuity Plan, with an additional PCP Tool for quick and easy use.

11.1 Critical Security Incidents

Critical security incidents are any incidents which may have a critical impact on 3R-4-CACE personnel, assets, activities, or reputation. They may involve or effect any of the personnel covered in this plan, and include but are not limited to:

- Kidnapping or abduction
- Fatal road traffic accident
- Arrest or detention of Project personnel.
- Loss of life as a result of Project activities.
- Medical emergency affecting Project personnel.
- Reputational crisis related to Project personnel or activities.
- Cases or allegations of SEA.
- Armed attack

11.2 Crisis Management Team (CMT)

The 3R-4-CACE CMT comprises senior members of the PCU and PIU and will be assembled to address critical incidents or crises of other nature. Region-level and Woreda-level personnel will generally stay in their Area of Responsibility (AOR) to manage the crisis at that level, either as the interface between the Project CMT and the incident management team (IMT) at the point of incident, or part of the IMT itself.

Neither team should be made up of more than six people.

Table 5: Crises Management Team

CMT Role	**Team Member**	**Position**	**Backup**
CMT Leader			
Security Focal Point			
Support Manager			
HR Manager			
Media and Comms Manager			

11.3 Suspension of Activities, Hibernation, and Relocation

In the event of a critical security incident, or a significant deterioration in the security environment, it may be necessary to take significant steps in order to safeguard the wellbeing of personnel, and prevent (further) harm or damage.

For additional information on security responses and relevant key indicators, see the Risk Level Indicator Matrix (below).

- **SUSPENSION OF ACTIVITIES**
  Should the security situation deteriorate in a specific location, it may be necessary to pause or postpone planned Project activities until the threat has passed. If there is no forecasted change in circumstances, then a resumption based on an assessment of the situation may be required.

  In extreme cases, a suspension of the entire Project may be in order.

  Authority to suspend activities: Project Coordinator in consultation with the PCU

- **HIBERNATION**
  Hibernation – or shelter in place – refers to personnel seeking refuge in a safe location, and not leaving that location until the danger has passed. This time can range from a matter of hours, to weeks depending on the situation, and hibernation may take place at people's homes, at offices, or a designated Safe Haven.

  Authority to order hibernation: Project Coordinator in consultation with the PCU team

- **RELOCATION**
  In some cases, withdrawing from the area may be necessary, for instance if there are no locations deemed safe enough to spend prolonged periods of time, of if failure to relocate at a given time would mean a lack of options to leave later on.

  Authority to order a relocation of personnel: Project Coordinator in consultation with the PCU team

In all of the above cases, it is vital to carefully assess any return to normal functioning. There is a danger either of returning to operations prematurely, and before the security threat has passed or adequate mitigation measures put in place, or not returning to operations at all due to concerns of irresponsible exposure to security risks. Both of these dangers are solved through thorough assessment of security threats and mitigation measures, as well as honest risk vs. benefit analysis.

Authority to resume activities and/or redeploy staff: Project Coordinator in consultation with the PCU team

11.4 Medical Emergency

In the case of a medical emergency, such as sickness or injury, affecting project staff, they are to be immediately evacuated to the nearest medical facility capable of delivering the appropriate life-saving care. In the case of a beneficiary sick or injured as a result of project activities (for example, is injured at a construction site) then it is the responsibility of project staff to support the individual in obtaining the appropriate assistance.

All staff – contracted or employed – should have adequate insurance coverage to cover the cost of medical treatment.

As part of project planning, medical facilities in the vicinity of project locations should be mapped, including capturing key contact numbers, precise location, and medical capabilities to help expedite any response to a medical emergency.

Table 6: Risk Level Indicator Matrix

For Guidance Purposes Only – to be considered at a kebele level as part of Go/No-Go decision making. See Annex 3: PCP Tool for additional guidance.

Risk Level	Key Indicators	Additional Security Measures Required	Key Indicators for Increased Risk to the Project
Low	▪ Community leadership is unified and accessible, with different groups and communities co-existing peacefully. ▪ Security forces (both formal and informal) are well-manned, equipped and with an effective chain of command, and have a good relationship with the local population. ▪ Basic goods and services are available to the majority of the population. ▪ Medical services are easily reachable and offer the majority services. ▪ Security incidents related to serious crime or conflict are rare.	▪ None.	▪ Breakdown in communications with one or more stakeholder. ▪ Information received of tensions or escalations in conflict-related areas. ▪ Increase in the frequency of security incidents. ▪ Increase in the severity of security incidents, and effecting targets of relevance to the Project (e.g. government assets, banks, gatherings of people). ▪ Access limitations to Project locations e.g. combination of flooded roads, halted air travel, and increase in conflict activity. ▪ Direct targeting of Project assets, locations, personnel or affiliated personnel e.g. armed robbery, looting of project site, serious assault of personnel. ▪ Demonstrations or other public
Medium	▪ Community leadership is largely unified, though with differences that are usually resolved constructively. ▪ Different groups and communities are able to resolve any disputes peacefully. ▪ Security forces are generally able to respond to safety and security incidents and have the trust of the majority of the local populace. ▪ There is some scarcity of certain resources, but basic goods and services are largely available. ▪ Medical services are basic and more complex treatment may be unavailable. ▪ Security incidents related to serious crime or conflict are known to take place.	▪ Security Focal Point consulted for additional analysis and advice.	

High	▪ There is active and unresolved contention amongst stakeholders and community leadership. ▪ Inter-community tensions are substantial with sporadic escalations to isolated incidents of violence. ▪ Security forces (both formal and informal) are effective and are able to response adequately to incidents, though acceptance by different groups/ communities may vary. ▪ Basic goods and services are sporadic, with competition for resources commonplace. ▪ Medical services are distant with limited life-saving care available at the location. ▪ Security incidents are frequent, with widespread and indiscriminate targeting and collateral damage	▪ Detailed security risk assessment of the implementing area and access routes is required ▪ Vulnerabilities identified, and additional measures implemented in line with assessment	displays of hostility towards the Project by stakeholders. ▪ Armed conflict in the vicinity of Project locations. ▪ Credible intelligence of an impending attack on a Project location. ▪ Reputational crisis such as high-profile allegations of corruption. ▪ Death of Project staff due to security incident.
Very High	▪ Inter-community tensions are high, and violence is commonplace and prone to escalation. ▪ Active military operations are ongoing causing road closures and service disruptions ▪ Tensions are significant between security forces and one or more community/ group, and are unable to respond adequately to the security situation ▪ Medical services are unavailable and require travel by vehicle to access. ▪ Security incidents are frequent, with widespread and indiscriminate targeting and collateral damage. ▪ Competition for resources is high, resulting in common criminality.	▪ Project activities are carried out on a case-by-case basis, subject to security risk assessment of each activity.	
Unacceptable	▪ Inter-communal tensions are extreme, with little communication, negotiation or mediation. ▪ Security forces (both formal and informal) are non-existent, incapable of intervention, and/or an exacerbating factor in the conflict. ▪ Medical services are unavailable and cannot be reached within a days drive. ▪ Security incidents are continuous, random, and prone to significant escalation and collateral damage. ▪ Basic goods and services are scarce and competition for resources is fierce.	▪ Project activity is suspended until conditions are more conducive and a return to a lower risk level	

Table 7: Sample Table for Key 3R-4CACE Project Locations

Addis Ababa	
Ministry of Finance	
Ministry of Women’s and Social Affairs	
World Bank Group HQ	
Oromia Region	
Benishangul Gumuz Region	
Afar Region	
Amhara Region	
Tigray Region	

Annexes

Annex 1: Security Risk Assessment (separately attached)

Annex 2: Standard Operation Procedure (separately attached)

Annex 3: Project Continuity Plan (PCP) (separately attached)