



# **Regional Climate Resilience Program (RCRP) for Eastern & Southern Africa**

## **ENTRO & NELSAP-CU Social and Environmental (S&E) Risks Management**

### **Security Management Plan for RCRP project**

# CONTENTS

<b>1. PROJECT BACKGROUND</b>	<b>1</b>
<b>2. SECURITY MANAGEMENT APPROACH</b>	<b>1</b>
<b>2.1 Standards and Good International Practice</b>	<b>2</b>
<b>2.2 ENTRO &amp; NELSP-CU RCRP Project Security Management Plan</b>	<b>2</b>
2.2.1 Overview of the Project Implementation Sites' Security Situation	3
2.2.2 Categories of Security Risks	9
2.2.3 The main security risks at the RCRP project implementation sites	10
2.2.4 Potential Impacts of Project Security Personnel on Communities and Workers	18
2.2.5 Security Personnel Risk Management Measures	21
<b>3. ALERT STATES</b>	<b>24</b>
<b>3.1 Alert State Status Information</b>	<b>30</b>
<b>3.2 Journey Management Plan (JMP)</b>	<b>31</b>
<b>3.3 Institutional Arrangements and Decision-Making Processes</b>	<b>32</b>
<b>4. OVERVIEW OF KEY LABOR RISKS ON THE PROJECT</b>	<b>32</b>
<b>4.1 Overview of Labor Use on the Project</b>	<b>32</b>
4.1.1 Direct workers	32
4.1.2 Contracted workers	33
4.1.3 Security Personnel	33
4.1.4 How to address Labor Risks	33
<b>4.2 Security Personnel Related Grievances Redress Mechanism (GRM)</b>	<b>33</b>
<b>5. ANNEXES</b>	<b>35</b>
<b>5.1 Annex I: Adopted ENTRO &amp; NELSAP-CU RCRP Project Security-Related Grievance Redress</b>	<b>35</b>
<b>5.2 Annex II: ENTRO &amp; NELSAP-CU RCRP Project Security Personnel Code of Conduct</b>	<b>37</b>
<b>5.3 Annex III: Definition of Impact Levels</b>	<b>39</b>
<b>5.4 Annex IV: Definition of Risk Levels Rating</b>	<b>39</b>
<b>5.5 Annex V: Journey Management Plan for the RCRP project</b>	<b>40</b>

**List of Tables**

Table 2.1: Risk Assessment Matrix..... 12  
Table 2.2: RCRP Project Security Risks and Mitigation Measures ..... 13  
Table 2.3: Situation Analysis Matrix for security within the project sites ..... 18  
Table 2.4: Summary of key mitigation measures/Management Actions related to Security personnel  
Misconduct during RCRP project implementation ..... 23  
Table 3.1: Alert State - Security Response Level with Crisis Management Plan for RCRP project sites... 25  
Table 3.2: Alert State-Security Response Level with evacuation Plan for RCRP project sites ..... 28

## List of Figures

Figure 2.1: South Sudan displacement into the Gambella Region of Ethiopia because of armed conflict (IOM SLO Ethiopia, January 2017).....	4
Figure 2.3: A map showing part of Uganda – South Sudan Border.....	9
Figure 3.1: Security status map of RCRP project sites (BAS, Yabus and Unyama) in Ethiopia, South Sudan, Sudan and Uganda .....	30

## 1. PROJECT BACKGROUND

The World Bank International Development Association (IDA) has financed the Nile Basin Initiative (NBI) centers through the Eastern Nile Technical Regional Office (ENTRO) and the Nile Equatorial Lakes Subsidiary Action Program Coordination Unit (NELSAP-CU), to implement Phase 1 of the Regional Climate Resilience Program (RCRP) for Eastern and Southern Africa, a program envisioned as a regional multi-phase engagement Series of Projects (SOP). The Program Development Objective (PDO) is to improve the management of water-related climate impacts, with the higher-level aim of strengthening the resilience of populations to climate-related shocks. The target countries are Comoros, Madagascar, Malawi, Mozambique, and South Sudan with the assistance of regional organizations, namely the African Union (AU), Southern Africa Development Community (SADC), and NBI.

Activities to be implemented by ENTRO and NELSAP-CU at the regional/basin level include: 1) Development of Flood Risk Mapping for selected areas in the Baro-Akobo-Sobat (BAS) sub-basin (involving Ethiopia and South Sudan); 2) Feasibility study for flood management interventions in the Yabus catchments and associated riverine (involving Ethiopia, South Sudan and Sudan); 3) Integrated Transboundary flood management at the Elegu-Nimule border between South Sudan and Uganda; 4) Enhancing Community Awareness and Preparedness towards climate change adaptation and resilience; and 5) Strengthen capacities of ENTRO, and NELSAP-CU and their member countries.

The deliverables include 1) prefeasibility & feasibility studies; 2) preparation of Environmental and Social Impact Assessments (ESIAs), Resettlement Action Plans (RAPs), detailed engineering designs, and preparation of tender documents for any identified high priority flood management infrastructure/structures in the involved NBI member states; and 3) promotion of the use of early warning system information from the Nile Cooperation for Climate Resilience (NCCR) Flash Flood Early Warning System (FFEW) for the communities in the target flood prone areas.

The security risk assessment and management plan is prepared with the objective of assessing and identifying the potential security risks that could potentially threaten the safety and security of the project workers and the beneficiary community in the RCRP project intervention sites (BAS, Yabus, and Unyama). Information and data from ENSAPT and TAC leaders' respective countries where the project was implemented were used for the preparation of the plan.

## 2. SECURITY MANAGEMENT APPROACH

Under guidance of both ENTRO & NELSAP-CU managements, and in close collaboration with the member countries, the RCRP Project Lead Technical Specialist, Project Coordinator for the Unyama-Ame and ENTRO Social Development and Environmental Officer will ensure that security procedures and criteria are fully designed and updated, and the means are fully available to ensure the security for project operations.

In consultation with ENSAPT Leaders, the Eastern Nile Subsidiary Action Programme (ENSAP) Technical Team Leaders of the three Eastern Nile Countries (Ethiopia, South Sudan, and Sudan); and the Nile Equatorial Lakes Subsidiary Action Programme (NELSAP) Technical Advisory Committee (TAC) leader of Uganda), the Lead Technical Specialist and Social Development and Environmental Officer will also leverage the existing national and local security infrastructure to access and share security and conflict-related information.

In addition, working with the Grievance Focal Points of the respective project implementation sites, the Lead Technical Specialist, Project Coordinator for the Unyama-Ame and Social Development and Environmental Officer will specifically identify associated risks, including armed conflict that can pose a threat to project staff and communities while implementing activities of the project (including Socio-economic data collection and survey work for staff gauge installation) at BAS, Yabus, and Unyama implementation sites.

## **2.1 Standards and Good International Practice**

This security management plan is anchored on (a) World Bank Environmental and Social Standard 4 (ESS4) that covers Community Health and Safety subsection (b) Personnel Security in line with the World Bank Good Practice Note on Assessing and Managing Risks and impacts of the Use of Security and (c) the Guidelines for Implementation of the UN Basic Principles on the Use of Force and Firearms by law Enforcement Officials.

The standard role of the Public Security Agencies will be to maintain the rule of law, including safeguarding human rights and deterring any actions that will threaten the project personnel and facilities. The Public Security agents to be deployed when needed will be competent, appropriate, and proportional to the threat. ENTRO will adopt the World Bank Good Practice Note on Assessing and Managing Risks and Impacts of the Use of Security to comply with the commitments on human rights extended throughout the RCRP project activities and bolstered by its compliance with:

- Voluntary Principles on Security and Human Rights Toolkit Version 3, 2008.
- Guidelines for Implementation of the UN Basic Principles on the Use of Force and Firearms by law Enforcement Officials, 2016.
- Proclamation No. 1176/2020 Prevention and Suppression of Terrorism Crimes of Ethiopia.
- Law No. 45/2008 of 09/09/2008 on Counter Terrorism in Rwanda.
- The Ethiopian Federal Police Commission Establishment Proclamation 720/2011 (and its amendments).

## **2.2 ENTRO & NELSP-CU RCRP Project Security Management Plan**

Lead Technical Specialist, Project Coordinator for the Unyama-Ame and Social Development and Environmental Officer will be responsible for project security management at both the Basin and country levels under the direct oversight and guidance of their respective managements and

ENSAPT/TAC leaders of the respective water affairs institutions of the four countries. ENSAPT/TAC leaders will also work closely with the respective security agencies of their respective countries to obtain security information and seek guidance on the start of field activities/plans, ahead of visits.

The management of security for the RCRP project operations will comply with the four basic pillars of security management:

- DETECT an adversary.
- DETER an adversary if possible.
- DELAY the adversary until appropriate authorities can intervene.
- RESPOND to the adversary's actions.

### *2.2.1 Overview of the Project Implementation Sites' Security Situation*

RCRP project is implemented in three project sites: 1) Development of Flood Risk Mapping for selected areas in the Baro-Akobo-Sobat (BAS) sub-basin (involving Ethiopia and South Sudan); 2) Feasibility study for flood management interventions in the Yabus catchments and associated riverine (involving Ethiopia, South Sudan and Sudan); and 3) the Integrated Transboundary flood management at the Elegu-Nimule border between South Sudan and Uganda.

Different security risks exist in the target RCRP project implementation sites, which might exist for a long time, be new, or change from time to time, which may impact the project activities:

#### **i. Security situation of BAS implementation site (Gambella Region of Ethiopia)**

The security situation in the Gambella Region of Ethiopia through which the Baro-Sobat River corridor study area passes remains fragile and volatile, marked by periodic outbreaks of inter-communal violence and heightened tensions. In late 2025, serious security incidents—including the killing of a senior police official—triggered renewed unrest, particularly in Gambella town and nearby areas. This violence involved Anyuak and Nuer communities and is driven by long-standing ethnic grievances related to competition over resources, and local politics. In response, the regional and federal governments have deployed federal security forces, imposed curfews, restricted night movement, and tightened controls on civilian firearms<sup>1</sup>. Despite these measures, sporadic violence and fear persist, especially in rural areas, affecting civilians, humanitarian operations, and the large South Sudanese refugee population hosted in the region. Overall, access

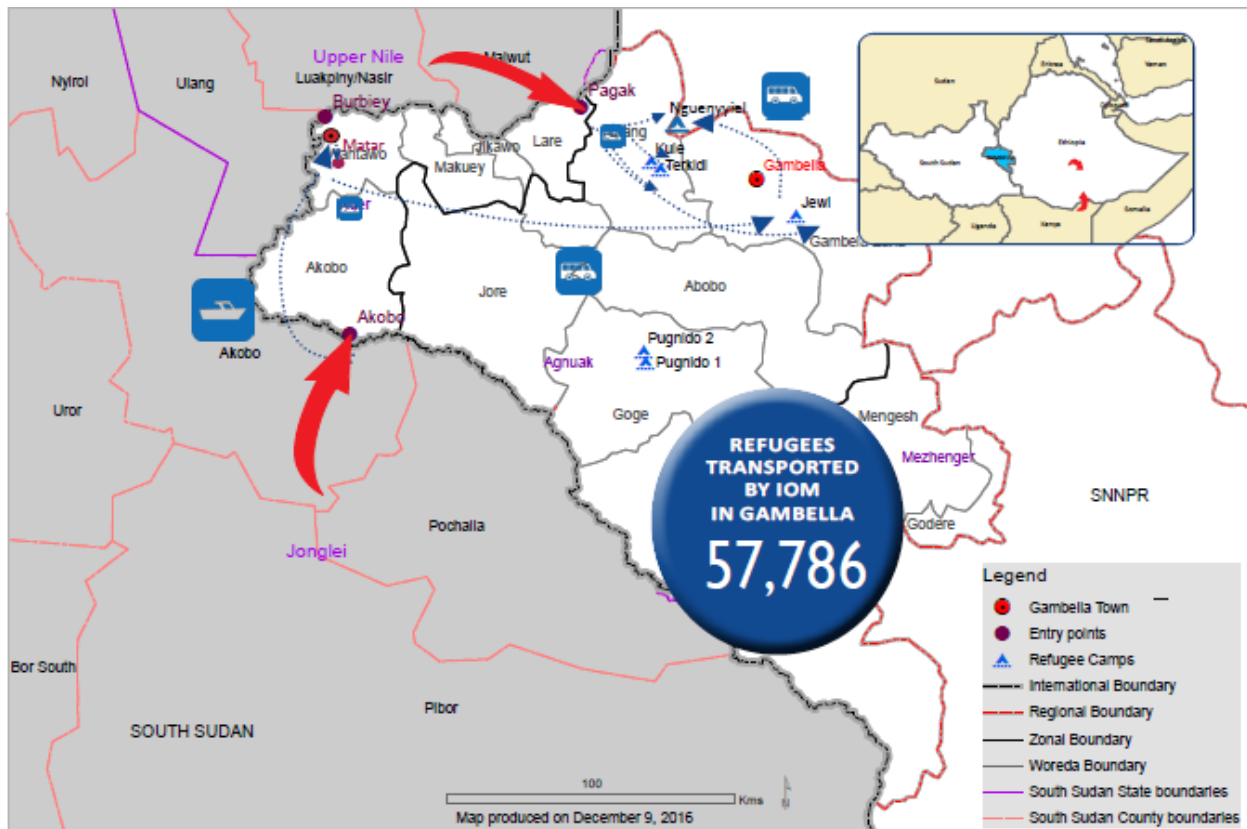
---

<sup>1</sup> [https://addisstandard.com/gambella-city-imposes-curfew-after-gunfire-attacks-kill-four-injure-eight/?fbclid=IwY2xjawOnm3pleHRuA2FlbQlxMABicmlkETBkMEU2eVdraW1iV3E1TVlOc3J0YwZhcHBfaWQQMjlyMDM5MTc4ODlwMDg5MgABHk56so\\_Az76DD5Yshs-DGZV8ju72TyLm0C3a-njyVXa6SY5cotkLRyaRlsK4\\_aem\\_3-T8P\\_siyYtFcyjLfDwLvQ#google\\_vignette](https://addisstandard.com/gambella-city-imposes-curfew-after-gunfire-attacks-kill-four-injure-eight/?fbclid=IwY2xjawOnm3pleHRuA2FlbQlxMABicmlkETBkMEU2eVdraW1iV3E1TVlOc3J0YwZhcHBfaWQQMjlyMDM5MTc4ODlwMDg5MgABHk56so_Az76DD5Yshs-DGZV8ju72TyLm0C3a-njyVXa6SY5cotkLRyaRlsK4_aem_3-T8P_siyYtFcyjLfDwLvQ#google_vignette)

to project site at Zonal Areas and Woredas targeted in the Gambela Region continues to present a high-risk security environment requiring close monitoring and cautious movement.

**ii. Security Situation of BAS in South Sudan involved Counties in Upper Nile and Jonglei States**

ii) Overall Security Situation in South Sudan’s areas through which the Baro-Sobat River corridor study area passes is fragile as the implementation of a peace agreement signed between rebel factions and the government in 2018 has significantly deteriorated since early 2025, with fighting spreading across several counties, including in Jonglei and Upper Nile States. Clashes between the South Sudan People’s Defense Forces (SSPDF) and armed opposition groups — notably the Sudan People’s Liberation Movement/Army-in-Opposition (SPLM/A-IO) and allied militias such as the White Army — have intensified. This escalation has displaced tens of thousands, with reports of over 230,000 people fleeing their homes in Jonglei alone since December 2025<sup>2</sup>.



**Figure 2.1: South Sudan displacement into the Gambella Region of Ethiopia because of armed conflict (IOM SLO Ethiopia, January 2017)**

**Humanitarian Crisis and Civilian Impact**

<sup>2</sup> [https://apnews.com/article/174d9f4bb51b107f497891beb03fe98f?utm\\_source=chatgpt.com](https://apnews.com/article/174d9f4bb51b107f497891beb03fe98f?utm_source=chatgpt.com)

As came in the same reference quoted above, the conflict has severely restricted humanitarian access, with fighting hampering aid deliveries, disrupting medical evacuations, and forcing temporary suspension of critical services. Humanitarian organizations report acute food insecurity, with large portions of the population reliant on emergency assistance.

UN peacekeeping monitoring (UNMISS) documented hundreds of conflict-related incidents affecting civilians, including killings, injuries, abductions, and cases of sexual violence, even amid slight reductions in some categories compared to previous quarters.

### **Widespread Violence & Localized Clashes**

*Conflict dynamics remain complex:*

- Jonglei clashes (Dec 2025–present): Armed confrontations between government and SPLM/A-IO forces have resulted in significant displacement and civilian casualties<sup>3</sup>.
- Historical incidents like the Nasir clashes in March 2025 and attacks on healthcare facilities show how localized battles can escalate and disrupt services<sup>4</sup>

*Travel & Security Risk:*

South Sudan remains one of the most unstable and high-risk environments in Africa. Armed conflict, unpredictable violence, and volatile checkpoints make travel dangerous across many areas. There is also a risk from landmines and unexploded ordnance in conflict-affected zones<sup>5</sup>.

#### **iii. Yabus implementation site Security situation (Ethiopia Benishangul-Gumuz Region; South Sudan Maban County, Upper Nile State; & Sudan Blue Nile State)**

Security wise, the project sites, northwestern Ethiopia, northeastern South Sudan and southeastern Sudan (east of the White Nile) were largely peaceful till the time of field visit mid November 2025, to Bunj-Maban that hosts a big population of Sudanese refugees. During the previous conflicts of SPLM/A North with Khartoum; and when the conflict erupted in April 2023 between the Sudanese Armed Forces (SAF) and the Rapid Support Forces (RSF) that became key belligerents in the broader civil war in Sudan, thousands of people were displaced, fled violence and sought refuge.

---

<sup>3</sup> [https://en.wikipedia.org/wiki/Jonglei\\_clashes\\_%282025%E2%80%93present%29?utm\\_source=chatgpt.com](https://en.wikipedia.org/wiki/Jonglei_clashes_%282025%E2%80%93present%29?utm_source=chatgpt.com)

<sup>4</sup> [https://en.wikipedia.org/wiki/2025\\_Nasir\\_clashes?utm\\_source=chatgpt.com](https://en.wikipedia.org/wiki/2025_Nasir_clashes?utm_source=chatgpt.com)

<sup>5</sup> [https://www.gov.uk/foreign-travel-advice/south-sudan/safety-and-security?utm\\_source=chatgpt.com](https://www.gov.uk/foreign-travel-advice/south-sudan/safety-and-security?utm_source=chatgpt.com)

Afterward, the war in and around Damazin (Blue Nile State) subsided and these areas became different from the other areas of Sudan and South Sudan where fights have been raging between SAF & RSF on one hand; and between SSPDF & SPLM/A-IO on the other respectively. So, the conditions were safe enough for travel and work in this zone covered by the Yabus catchments and associated riverine between the three countries.

However, a fragile situation evolved again, since December 2025. As reported in ACLED<sup>6</sup>, by Jalale Getachew Birru, on 25 January 2026, the Rapid Support Forces (RSF) and the Sudan People's Liberation Movement-North faction led by Abdelaziz al-Hilu (SPLM-N Hilu) clashed with the Sudanese Armed Forces (SAF) in several locations of Blue Nile state's Bau locality, after crossing from South Sudan. Bau county critically lies between the state capital, al-Damazin, and Kurmuk locality — which hosts Yabusa, SPLM-N Hilu's stronghold in Blue Nile and borders South Sudan. This fighting is the first on-the-ground confrontation between the two groups after the SAF's accusations in recent months that the RSF uses neighboring states, particularly Ethiopia, to train and mobilize fighters.



Figure 1.2: Base map of the border between the Sudan Blue Nile State, Ethiopia's Benishangul-Gumuz Region & Northeastern South Sudan, involving the Yabus study area

<sup>6</sup> <https://acleddata.com/report/blue-nile-peripheral-front-central-battleground-sudan-conflict>

The SAF, RSF, and allied groups have increased deployments in the Blue Nile since at least mid-December 2025, when the SAF publicly accused Ethiopia of providing military support to the RSF. The latest campaign in Blue Nile, though, began in earnest on 11 January, when the SAF carried out airstrikes on a convoy in Yabus, killing an unspecified number of people. The SAF said the convoy carried foreign mercenaries trained in Ethiopia to reinforce the RSF and the Hilu faction. SPLM-N Hilu countered that the strike killed civilians returning from markets and workplaces. SAF airstrikes continued on 22 January in the Yabusa and Bellila areas.

On 2025-01-29, RSF issued a condemnation on an alleged attack on the (WFP) office in Yabus area, Blue Nile State, which tragically claimed the lives of three staff members and complete destruction of the facility<sup>7</sup>, according to RSF.

The renewed violence with mistrust between the three governments have resulted in security challenges, making the area highly unstable and unpredictable. The main security situations arising include the following:

- **Persistent insecurity:** Military threats, such as exposure to air attacks, which create constant security risk, fear among civilians, disrupt normal life, and work environment.
- **Risk of spillover fighting:** Active clashes in surrounding parts of Blue Nile State increase the risk that fighting could spread into or near the city, making the security situation volatile and subject to sudden deterioration.
- **Breakdown of law and order:** The conflict has weakened local security structures, leading to increased criminality, including looting, armed robbery, and the proliferation of small arms among civilians and militias.
- **Movement restrictions and access constraints:** Insecurity on main roads and checkpoints has limited freedom of movement, disrupted supply routes, and increased the risk of ambushes, especially outside urban areas.
- **Targeting of infrastructure:** Attacks on critical infrastructure such as power stations, roads, and communication facilities have caused service disruptions, affecting hospitals, water supply, and markets.
- **High civilian protection risks:** Civilians face threats from indiscriminate attacks, stray munitions, and unexploded ordnance, particularly in areas close to military positions.
- **Humanitarian and operational risks:** Insecurity has constrained humanitarian access, delayed aid delivery, and increased risks for aid workers, further exacerbating civilian vulnerability

#### iv. South Sudan – Uganda Border Security Situation at Unyama-Ame Project Site

---

<sup>7</sup> <https://rapidsupportforce.com/en/news-details/The%20Rapid%20Support%20Forces%20strongly%20condemn%20the%20attack%20on%20the%20World%20Food%20Program%20WFP%20office>

Security situation is mostly triggered by border issues between South Sudan and Uganda. As reported by Radio Tamazuj, on July 30, 2025, Uganda deploys more troops<sup>8</sup> after border clash in South Sudan Kajo-Keji County of Central Equatoria State, which is adjacent to Nimule RCRP Unyama project site in Magwi County of Eastern Equatoria State, following a deadly clash that killed several soldiers and displaced thousands of civilians, a South Sudanese chief said on Wednesday, raising fears of further escalation. Speaking to Radio Tamazuj, Chief Tumiyo described a chaotic scene on Monday. “Up to today, there have been more deployments by the UPDF,” said Ernesto Tumiyo, executive chief of Bori Boma, Kajo-Keji County. He insisted the contested area, known as Nyainga Muda, belongs to South Sudan and accused Uganda of sabotaging planned peace talks.

Kajo-Keji County Commissioner Wani Jackson Mule confirmed more deployment of military forces in the area from both sides and called for urgent humanitarian aid, saying thousands—mostly women and children—had fled their homes and were sheltering in schools and churches without food or medicine. South Sudan’s military said Tuesday both sides agreed to an immediate ceasefire and would form a joint investigation committee. “We are engaging through the joint technical border committee to find a peaceful resolution,” said SSPDF spokesperson Maj. Gen. Lul Ruai Koang. But South Sudanese lawmakers and activists accused Uganda of violating its sovereignty. “This is not the first incursion, but this time it has turned deadly,” said Milla Amos Peter, chairperson of Kajo-Keji’s parliamentary caucus.

---

<sup>8</sup> <https://www.radiotamazuj.org/en/news/article/uganda-deploys-more-troops-after-border-clash-in-kajo-keji>



Figure 2.3: A map showing part of Uganda – South Sudan Border

### 2.2.2 Categories of Security Risks

- **Internal Risks:** May include but are not limited to illegal; unethical; or inappropriate behavior of project personnel or those directly affiliated with it, such as employee theft, workplace violence, and labour unrest, potentially with associated sabotage.
- **External Risks:** Are those caused by the actions of people outside the project who seek to take advantage of opportunities presented by the development and operation of the project, such as common criminal activity; disruption of the project for economic, political, or social objectives; and other deliberate actions that have a negative impact on the effective, efficient, and safe operation of the project. In extreme cases, these could include banditry attacks, terrorism, armed insurgency, coups, or war.

### *2.2.3 The main security risks at the RCRP project implementation sites*

Based on the information from discussions held with ENSAPT and TAC leaders; grievance focal points; and other officials in the countries, by ENTRO and NELSAP-CU project program and management experts, the main security risks of the project include Civil Unrest; Crime (Street Crime/Kidnap & Ransom/Robbery); Inter-tribal or Communal Violence; Sexual and Gender-Based Violence (SH, GBV, and SEA); Armed Attacks; and Community Hostility.

#### **i. Civil Unrest**

This includes protests and demonstrations, riots and strikes. The RCRP project operates in a complex regional security environment, with varying levels of civil unrest across its countries. Civil unrest includes protests, demonstrations, riots, strikes, intercommunal violence, and armed clashes, all of which can affect project implementation.

**Sudan:** Sudan is experiencing severe civil unrest, including widespread protests and demonstrations, and riots linked to the ongoing conflict between the Sudanese Armed Forces (SAF) and Rapid Support Forces (RSF). Fighting across multiple regions has caused mass displacement, ethnic violence, and humanitarian crises, disrupting access to project areas and threatening staff safety.

**South Sudan:** Civil unrest in South Sudan is localized but escalating, encompassing intercommunal violence, armed clashes, political faction tensions, sporadic protests, and occasional riots. Areas such as Jonglei and Upper Nile states have witnessed significant civilian displacement, disruption of services, and humanitarian challenges, directly impacting RCRP project implementation.

**Ethiopia:** Civil unrest in Ethiopia is persistent and largely localized, including community-level tensions, protests, demonstrations, and strikes. Security risks are heightened in border regions, compounded by spillovers from neighboring conflicts. The ongoing Sudan war has generated refugee inflows into Amhara and Benishangul-Gumuz regions, while unrest in South Sudan, including the Akobo area, has caused mass migration into Gambella. These movements increase pressure on local resources, humanitarian services, and community security, posing operational risks for the project.

**Uganda:** Uganda remains relatively stable, but experiences occasional public protests, demonstrations, and strikes linked to economic or political grievances. Border districts such as Yumbe, Adjumani, and Moyo are particularly exposed to spillovers from South Sudan instability, hosting large numbers of refugees and facing localized risks including cross-border tensions and security incidents.

#### **ii. Crime**

Crime, including street crime, robbery, and kidnapping for ransom, poses significant risks to the RCRP project by threatening the safety of personnel, disrupting field operations, and jeopardizing project assets and logistics. Street crime and local theft can reduce staff mobility and delay

activities, while robbery of project equipment or vehicles can interrupt the timely delivery of materials and services. Kidnap and ransom incidents, particularly in high-risk areas of Ethiopia, South Sudan, and Sudan, create serious safety, financial, and reputational risks, potentially leading to suspension of the project operations. These threats underscore the need for robust mitigation measures—such as security awareness training, safe transport protocols, coordination with local authorities, and contingency planning to ensure the protection of staff, assets, and project continuity.

**iii. Inter-tribal or communal violence**

Inter-tribal or communal violence in RCRP project implementation sites is mainly rooted in long-standing competition over land, water, and other natural resources, particularly in pastoral and agro-pastoral areas. These tensions are reinforced by historical grievances, ethnic identity politics, and unequal access to political power and public services. Weak governance and limited state security presence in remote regions often allow local disputes to escalate into violence. In addition, poverty, youth unemployment, and economic marginalization increase frustration and susceptibility to mobilization along ethnic lines, while cross-border dynamics, refugee movements, proliferation of small arms, and climate shocks further intensify and prolong communal conflicts. The risk in the project activities/operations is expected to be medium.

**iv. Armed attack: inter-state conflicts/intra-state conflicts**

The threat of armed attacks or rebel activity and kidnapping in project areas is often driven by political instability, weak governance/law enforcement, ethnic tensions, poverty, competition over resources, and spillover from regional conflicts. Such threats can disrupt project activities, endanger staff, damage assets, restrict community engagement, increase costs, and undermine overall project progress and credibility.

Kidnapping for ransom, organized criminal networks, and cross-border insecurity can pose potential danger to project staff with cash at hand or high-value precious materials like gold as prime targets. In such a situation, project stakeholders will be sensitized to use cashless transactions as much as possible. Where risks may be high, the armed security teams may be called upon to provide escorts to the destinations. The risk in the project activities/operations is expected to be medium.

**v. GBV, SEA, and SH**

The risk of GBV, SEA and SH in the project activities/operations is expected to be low, and all stakeholders, especially the girls and women, will be sensitized on how to avoid such incidents and the correct steps to take and channels to use to report in case they are affected or become a victim. The project GRM will also have a dedicated channel to handle SEAH incidents.

**vi. Community hostility/grievance**

Community refusal to allow project implementation in their area can delay or halt project activities, restrict access to sites, reduce stakeholder engagement, and undermine project objectives. It may

also increase costs due to the need for additional consultations, negotiations, or mitigation measures, and can affect the overall credibility and success of the project.

Community refusal to project implementation can be mitigated through early and inclusive community engagement, transparent communication about project benefits and risks, effective grievance redress mechanisms, fair benefit-sharing, and active involvement of local leaders and community members. These measures help build trust, address concerns, and promote community ownership, thereby enabling smoother project implementation. The risk in the project activities/operations is expected to be medium.

Consequence risk assessment matrix has been adopted, comprising of the impact and likelihood of potential security risks (Table 2.1). The matrix works by selecting the appropriate consequences from the bottom, then cross-referencing against the row containing the likelihood to read off the estimated risk rating. Annexes III and IV provide further definitions of impact levels and the corresponding risk ratings.

**Table 2.1: Risk Assessment Matrix**

		Impact →				
		Low	Low Med	Medium	Med Hi	High
Likelihood ↑	Very Likely	Low Med	Medium	Med Hi	High	High
	Likely	Low	Low Med	Medium	Med Hi	High
	Possible	Low	Low Med	Medium	Med Hi	Med Hi
	Unlikely	Low	Low Med	Low Med	Medium	Med Hi
	Very Unlikely	Low	Low	Low Med	Medium	Medium

The Likelihood versus Consequences Risk Assessment Matrix has been supported with a table which ties together the risks with the mitigations, roles and responsibilities and timelines, and the security situation analysis for the four Countries (see Table 2.2).

**Table 2.2: RCRP Project Security Risks and Mitigation Measures**

No.	Risk description	Likelihood of risk occurring	Impact if risk occurs	Severity rating based on impact and likelihood	Responsibility	Mitigating action	Contingent action	Progress on actions	Useful resources
1	Crime: Street crime/Kidnap & Ransom/Robbery	Likely	High	High	Lead Technical Specialist	<p>Ensure the immediate safety of staff and beneficiaries and promptly notify security forces.</p> <p>Activate emergency and incident response protocols, account for all personnel, and provide support to individuals affected by the crime.</p> <p>Maintain reliable communication systems for real-time coordination and reporting. Deploy staff who have received Hostile Environment Awareness Training (HEAT) to enhance response effectiveness.</p> <p>Temporarily suspend activities, if necessary, conduct a rapid risk reassessment, and strengthen security measures. Coordinate closely with authorities, ENSAPT leaders, and GRM focal points, and update contingency and response plans accordingly.</p>	<p>Conduct effective risk analysis assessments, and SWOT analyses and Force-Field Analyses related to gaps and needs assessments.</p> <p>Establish formal and consistent reporting and communications mechanisms with ENSAPT/TAC and other stakeholders</p> <p>Immediate suspension of activities in affected areas, prioritize the safety of workers</p>		<p><a href="https://www.miga.org/sites/default/files/archive/Documents/VP_SHR_Toolkit_v3.pdf">VPSHR Toolkit</a>  <a href="https://www.miga.org/sites/default/files/archive/Documents/VP_SHR_Toolkit_v3.pdf">https://www.miga.org/sites/default/files/archive/Documents/VP_SHR_Toolkit_v3.pdf</a></p>
2	Inter-tribal or communal violence	Likely	High	High	Lead Technical Specialist	<p>Work closely with respective ENSAPT/TAC leaders and implement structured information exchange mechanisms supported by reliable communication systems.</p>			<p>Customary law, and traditional, community-</p>

No.	Risk description	Likelihood of risk occurring	Impact if risk occurs	Severity rating based on impact and likelihood	Responsibility	Mitigating action	Contingent action	Progress on actions	Useful resources
						<p>Prioritize the safety of staff and communities and suspend activities if necessary.</p> <p>Ensure personnel have received Hostile Environment Awareness Training (HEAT) to operate safely in volatile contexts. Engage local leaders and authorities to de-escalate tensions, activate grievance mechanisms, and maintain neutral communication.</p> <p>Conduct conflict analysis, adapt project approaches to remain conflict-sensitive, and strengthen community dialogue, inclusion, and continuous risk monitoring.</p>	and communities, restrict staff movement, and coordinate with local authorities, community leaders, and relevant partners to support de-escalation.		based mechanisms
3	Armed attack: inter-state conflicts/intra-state conflicts	Likely	High	High	Lead Technical Specialist	<p>Continuous consultation with ENSAPT/TAC leaders of respective countries should be maintained to gather timely information on the security situation, while enhancing inter- and intra-agency cooperation within the project area, including coordination with police forces.</p> <p>Implement structured information exchange programs supported by reliable and redundant communication systems. Conduct regular risk assessments, engage local communities, and avoid high-risk areas.</p> <p>Develop and operationalize comprehensive security protocols, including evacuation</p>	<p>Never fight back when apprehended with armed people.</p> <p>Listen carefully to instructions and do as you are told (if instructions are difficult to hear, ask politely but firmly for them to be repeated).</p>		<p><u>VPSHR Toolkit</u>  <a href="https://www.miga.org/sites/default/files/archive/Documents/VP_SHR_Toolkkit_v3.pdf">https://www.miga.org/sites/default/files/archive/Documents/VP_SHR_Toolkkit_v3.pdf</a></p>

No.	Risk description	Likelihood of risk occurring	Impact if risk occurs	Severity rating based on impact and likelihood	Responsibility	Mitigating action	Contingent action	Progress on actions	Useful resources
						<p>plans and medical evacuation (MEDEVAC) plans, and ensure staff receive Hostile Environment Awareness Training (HEAT).</p> <p>During attacks, prioritize staff safety, maintain communication, coordinate with security forces, and activate crisis management procedures. Post-incident, assess damage, communicate with stakeholders, adjust project plans, and integrate lessons learned to strengthen future resilience.</p>	<p>Inform the victim's family in a timely manner.</p> <p>Do not make any sudden movements that might startle the criminals or be interpreted as an attempt to resist or escape.</p>		
4	<b>GBV and SH</b>	<b>Very unlikely</b>	<b>High</b>	<b>Midum</b>	E&S officer	<p>Adhere to all provisions in the Project Grievance Redress Mechanism and use of labor code of conduct for project personnel.</p> <p>Establish a zero-tolerance policy and Code of Conduct for all staff and contractors, with clear definitions, reporting channels, and consequences. Conduct gender-sensitive risk assessments, ensure safe access to project sites, and engage communities through awareness campaigns.</p> <p>Provide staff training on GBV, survivor-centered response, and reporting mechanisms.</p>	<p>Prioritize the survivor's safety, dignity, and confidentiality.</p> <p>Provide immediate medical and psychosocial support, report through secure channels, and obtain informed consent before referrals.</p>		<p><a href="https://www.miga.org/sites/default/files/archive/Documents/VP_SHR_To">https://www.miga.org/sites/default/files/archive/Documents/VP_SHR_To</a></p>

No.	Risk description	Likelihood of risk occurring	Impact if risk occurs	Severity rating based on impact and likelihood	Responsibility	Mitigating action	Contingent action	Progress on actions	Useful resources
						<p>Implement confidential reporting, referral pathways, and safeguarding officers.</p> <p>During incidents, prioritize survivor safety, medical and psychosocial support, and accountability, and use lessons learned to strengthen policies and prevent recurrence.</p>	<p>Initiate impartial investigation and apply zero tolerance measures.</p> <p>Protect against retaliation, ensure secure documentation, and follow a strict survivor-centered, do-no-harm approach.</p>		
5	Community hostility	<b>Unlikely</b>	<b>High</b>	<b>Medium</b>	Lead Technical Specialist	<p>Adhere to all provisions in the Project Stakeholder Engagement Plan through early and continuous stakeholder engagement, transparent communication of project objectives, and equitable inclusion of local participation, supported by reliable and redundant communication systems.</p> <p>Establish accessible grievance mechanisms and monitor community sentiment for early warning signs. Train staff in conflict sensitivity, negotiation, cultural awareness, and Hostile Environment Awareness Training (HEAT), and prepare contingency plans for staff safety.</p>	<p>Engage stakeholders promptly, ensure staff safety, and de-escalate tensions through dialogue.</p> <p>Activate grievance mechanisms, involve local leaders, and communicate transparently.</p>		RCRP Stakeholder Engagement Plan

No.	Risk description	Likelihood of risk occurring	Impact if risk occurs	Severity rating based on impact and likelihood	Responsibility	Mitigating action	Contingent action	Progress on actions	Useful resources
						During periods of hostility, pause sensitive activities, maintain safe zones, and engage local leaders to mediate disputes. Post-incident, assess impacts, adjust project plans, reinforce trust through communication, and continue monitoring to prevent recurrence.	Assess root causes, adjust project activities if needed, and strengthen conflict-sensitive approaches while monitoring risks and maintaining continuous community engagement.		

**Table 2.3: Situation Analysis Matrix for security within the project sites**

#	SECURITY THREATS PROJECT IMPLEMENTATION SITS	Crime: Street crime/Kidnap & Ransom/Robbery	Inter-tribal or communal violence	Armed attack: inter-state conflicts/intra-state conflicts	GBV and SH	Community Hostility
1	RCRP-BAS-Ethiopia site	Yellow	Red	Red	Green	Green
2	RCRP-BAS-South Sudan site	Yellow	Red	Red	Green	Green
3	RCRP-Yabus-Ethiopia Site	Yellow	Yellow	Yellow	Green	Green
4	RCRP-Yabus-South Sudan Site	Yellow	Yellow	Yellow	Green	Green
5	RCRP-Yabus-Sudan Site	Yellow	Red	Red	Green	Green
6	RCRP-Unyama-South Sudan Site	Yellow	Yellow	Red	Green	Yellow
7	RCRP-Unyama-Uganda Site	Yellow	Yellow	Yellow	Green	Green

N.B. These color codes will be adjusted based on the status/situation on the ground

In periods of low risk at the project implementation sites in the countries, security threats, the project could consider using technical expertise/unarmed security personnel assigned by institutions supporting the project implementation at all levels. If deemed necessary, the local police may be engaged on a reactive basis.

#### 2.2.4 Potential Impacts of Project Security Personnel on Communities and Workers

Deployment of security personnel is intended to safeguard project staff, Technical Assistants, contractors, and beneficiaries. However, the presence, behavior, and conduct of security personnel may create both positive and negative impacts on communities and project workers if not properly managed. Potential impacts can be categorized as follows:

**i. Impacts on Local Communities:**

**• Intimidation and Fear**

- Armed or uniformed security personnel may create fear among community members, particularly women, children, elderly persons, and vulnerable groups.
- A visible security presence may be perceived as militarization of a civilian development project.
- Community members may feel restricted from freely accessing public areas near project sites.

**• Excessive Use of Force**

- In situations involving protests, land disputes, or grievances, security personnel may use disproportionate force.

- Poorly trained guards may respond aggressively to misunderstandings or minor conflicts.
- **Conflict Escalation**
  - If security personnel show favoritism toward certain groups (e.g., clans, ethnic groups, or local elites), this may heighten local tensions.
  - Miscommunication between security personnel and communities could escalate minor issues into larger conflicts.
- **SEA/SH Risks (Sexual Exploitation and Abuse / Sexual Harassment)**

Security personnel, especially if armed or perceived as powerful authority figures, may:

- Exploit their position to demand sexual favors in exchange for access to services, employment, or protection.
- Engage in sexual harassment of female workers or community members.
- Target vulnerable groups, including internally displaced persons, widows, or adolescent girls.
- Create an environment where survivors fear reporting abuse due to intimidation.

These risks are heightened in remote or conflict-prone areas and where oversight mechanisms are weak.

- **Retaliation Against Complainants**
  - Community members who raise grievances may face intimidation or threats.
  - Security personnel may attempt to discourage reporting of misconduct.
  - Whistleblowers within the project workforce may fear job loss or harassment.

This can undermine the effectiveness of the project's Grievance Redress Mechanism (GRM).

## ii. **Impacts on deployed Project Workers:**

- **Workplace Intimidation**
  - Project workers (project staff, TAS, Sub-consultants, and contractors) may feel pressured or intimidated by security personnel, especially if guards are armed.
  - Security staff may improperly interfere in workplace disputes or labor issues.
- **Harassment and Discrimination**
  - Security personnel may harass casual laborers, women workers, or subcontracted staff.
  - There may be discriminatory practices based on ethnicity, gender, religion, or social status.

- **Sexual Exploitation and Abuse (SEA)/SH (Sexual Harassment) Risks**
  - Female workers may face sexual harassment from security personnel.
  - Power imbalance between security staff and temporary or daily laborers increases vulnerability.
  - Survivors may fear retaliation or job loss if they report misconduct.
- **Retaliation and Suppression of Labor Rights**
  - Security personnel may be used to suppress workers' strikes, unionization efforts, or complaints.
  - Grievance focal points of respective RCRP project sites who file grievances may face threats, restricted site access, or unfair disciplinary actions.
- **Context-Specific Risks (Fragile and Conflict-Affected Areas):** Given the project implementation sites (BAS, Yabus, and Unyama may experience Cross-border tensions, Inter-communal conflicts, and Armed group activity, Security personnel could:
  - Be perceived as aligned with government or political actors.
  - Become involved in local disputes.
  - Contribute unintentionally to conflict dynamics.

Poor coordination with local authorities and communities may increase these risks.

- **Reputational and Legal Risks to the Project:** Misconduct by security personnel may result in Loss of community trust, Project delays or suspension, Legal liability, Non-compliance with international standards (e.g., World Bank ESF requirements on community health and safety), and damage to donor and government credibility.

## 2.2.5 Security Personnel Risk Management Measures

To prevent and mitigate potential misconduct by security personnel and its adverse impacts on project staff, Technical Assistants (TAs), sub-consultants, contractors, and host communities, the leadership of ENTRO–NELSAP-CU and ENSAPT in each implementing country shall enforce and oversee the following measures:

### **i. Background Checks**

- All security personnel undergo background screening.
- No personnel with records of human rights violations, GBV, SEA/SH, or excessive use of force are recruited.
- Verification is conducted in coordination with relevant authorities where applicable.

### **ii. Security personnel Deployment request (by ENSAPT)**

While requesting corresponding security authorities in the respective countries, ENSAPT will ensure that the request for a support letter must include:

- Mandatory compliance with the project Code of Conduct (Annex 2??).
- Explicit prohibition of SEA/SH, abuse of authority, discrimination, and retaliation.
- Sanctions for violations (immediate removal, referral to authorities).

### **iii. Awareness creation before deployment**

**All security personnel must receive awareness on:**

- Human rights principles
- Proportional use of force
- Community engagement and conflict sensitivity
- Cultural awareness of local communities in the project implementation sites (BAS, Yabus, and Unyama)
- SEA/SH prevention and survivor-centered response
- Anti-retaliation principles
- Project GRM procedures

### **iv. Targeted Awareness Creation on SEA/SH**

Security personnel must understand:

- Zero tolerance for SEA/SH.

- Power imbalance risks.
- Consequences of misconduct.
- Confidential reporting channels.
- Survivor-centered approach (no victim-blaming, no retaliation).

**v. Code of Conduct (CoC)**

ENTRO-NELSAP-CU and ENSAPT teams from their respective countries must ensure that all security personnel sign a detailed Code of Conduct (**Annex II**) which clearly prohibits:

- Sexual exploitation and abuse
- Sexual harassment
- Intimidation and threats
- Discrimination
- Use of excessive force
- Retaliation against complainants

**vi. Use of Force and Weapons Management**

- **Rules on Use of Force:**
  - Security personnel shall apply force only as a last resort.
  - Force must be proportionate and lawful.
  - Firearms should be avoided unless necessary and legally authorized.
- **Incident Reporting:**
  - All security incidents must be documented.
  - Serious incidents (including SEA/SH allegations) must be reported within 24–48 hours to project management and relevant authorities.
  - Maintain a secure incident log.

**vii. SEA/SH Risk Mitigation Measures**

- **Prevention Measures:**
  - Deploying mixed-gender security teams where feasible.
  - Avoid isolated interactions between security personnel and vulnerable individuals.
  - Install adequate lighting around project sites.

- Restrict unauthorized access to workers' accommodation areas.
- Conduct community awareness sessions on SEA/SH reporting channels.
- **Confidential Reporting Mechanisms:**
  - Integrate SEA/SH-sensitive channels into the project GRM.
  - Provide anonymous complaint options.
  - Ensure complaints are handled confidentially.
  - Refer survivors to available GBV service providers.
- **Survivor-Centered Approach:**
  - Ensure no retaliation against survivors.
  - Immediate removal of the alleged perpetrator during investigation.
  - Respect confidentiality and informed consent.

**Table 2.4: Summary of key mitigation measures/Management Actions related to Security personnel Misconduct during RCRP project implementation**

No.	Risk area	Management measures	Responsible body
1	Intimidation	Community sensitization, limited visible force	ENSAPT, ENTRO-NELSAP-CU project management team, and Project GRM focal points
2	Excessive Use of Force	Use-of-force rules, awareness raising, and supervision	ENSAPT and ENTRO-NELSAP-CU project management team
3	ESH/SH	Zero tolerance CoC, confidential GRM, survivor support	ENTRO-NELSAP-CU project team, Environment and Social Specialist, and GRM focal points
4	Retaliation	Awareness raising, Whistleblower protection, monitoring	ENTRO-NELSAP-CU project team, Environment, and GRM focal points, and local government
5	Discrimination	Cultural awareness raising	ENTRO-NELSAP-CU project team, Environment and Social Specialist, and GRM focal points
6	Conflict escalation	Conflict-sensitive engagement, neutrality	ENTRO-NELSAP-CU project team, Local Government, Local community GRM focal points

### 3. ALERT STATES

ENTRO & NELSAP-CU will adopt the RCRP project-area alert status to invoke the security state response levels, triggers, and actions specific to the project site, with the color shades of Green, Yellow, Orange, and Red as the security-level responses to be adhered to (Table 3.1-Alert State-Security Response Level with Crisis Management Plan and 3.2-Alert State-Security Response Level with evacuation Plan).

Alert levels provide specific guidance on recommended security measures and actions to be adopted based on the prevailing security situation. It is anticipated that local or regional events (triggers) will be monitored daily and linked to the alert status. The Alert State–Security Response Levels outlined in Tables 3.1 and 3.2 will serve as the reference framework for determining the appropriate security alert status across RCRP project implementation sites.

ENSAPT/TAC leaders, national security agencies, and GRM focal points will provide real-time, ground-level information to inform these alert levels. This information will guide ENTRO–NELSAP-CU in making evidence-based decisions regarding the safe deployment of project personnel and the implementation of planned activities. The tables (3.1 and 3.2) are developed in alignment with the standard Risk Assessment Matrix presented in Table 2.1, ensuring consistency and coherence in risk management and response actions. All available security information will be assessed to ensure early identification of risk increases that may require a change in alert state. Changing the rating level will be done based on instructions from the ENTRO & NELSAP-CU RCRP project team.

**Table 3.1: Alert State - Security Response Level with Crisis Management Plan for RCRP project sites**

Colors	Event indicators	Crisis Management Plan
Green	<p>No direct threat exists, and no incidents have taken place to warrant heightened security measures.</p> <p>This is the default threat level. There is no current, general, or undirected threat to project-supported works projects within the project mandate. Under this level, the status remains at GREEN.</p> <ul style="list-style-type: none"> <li>✓ Site activities are running normally with employees going about their lives with no or very limited restrictions.</li> <li>✓ There are no restrictions on vehicle movement</li> <li>✓ Continued good will of the majority of the local community remains assured</li> </ul>	<ul style="list-style-type: none"> <li>• ENTRO/NELSAP-CU prepares project action plans with detailed information on where and when to implement project activities</li> <li>• ENTRO/NELSAP-CU shares project action plans with ENSAPT/TAC leaders</li> <li>• ENTRO/NELSAP-CU ensures all expatriates are registered with the appropriate embassy and all visas and passports are valid.</li> <li>• ENTRO/NELSAP-CU shares project personnel (staff, TA, and contractors) details (Name, age, sex, nationality, with their IDs/Passport) with ENSAPT/TAC leaders</li> <li>• ENTRO/NELSAP-CU ensures obtainment of support letters for project personnel through ENSAPT/TAC leaders.</li> <li>• ENTRO/NELSAP-CU in collaboration with ENSAPT/TAC leaders ensures that the support letters issued to the project personnel (staff, TA, and contractors) contain details of their particulars (Name, age, sex, nationality, and IDs/Passport numbers); and the purpose of project personnel deployment on the sites.</li> <li>• ENTRO/NELSAP-CU ensures debriefing of the project personnel on security procedures on the ground, including immediate reporting first to the security agencies/forces before starting their activities.</li> <li>• ENTRO/NELSAP-CU complete all pre-planned actions/activities, including training of the project staff, to ensure their awareness of the actions to be taken based on SMP.</li> <li>• ENTRO/NELSAP-CU and project personnel closely monitor the security situation, crime levels, and political and social events.</li> <li>• ENTRO/NELSAP-CU liaises with authorities and the local community for the collection and assessment of information from the ground.</li> <li>• Project personnel maintain close liaison with GRM Focal Points and build good relations with local communities.</li> <li>• ENTRO/NELSAP-CU in collaboration with ENSAPT/TAC leaders ensures that the security agencies/forces brief project personnel on the required roles, responsibilities and rules of engagement at the project sites (including information on curfew).</li> </ul>
Yellow	<p>Increased level of disturbance and/or increased probability of impact to project activities. Sporadic civil disorder events. A direct threat has been detected to one or more areas of the operation, but it is not considered imminent.</p>	<ul style="list-style-type: none"> <li>✓ ENTRO/NELSAP-CU prepares project action plans with detailed information on where and when to implement project activities</li> <li>✓ ENTRO/NELSAP-CU shares project action plans with ENSAPT/TAC leaders</li> <li>✓ ENTRO/NELSAP-CU ensures all expatriates are registered with the appropriate embassy and all visas and passports are valid.</li> </ul>

	<ul style="list-style-type: none"> <li>✓ Area-wide protests and/or strike action that do not directly impact project operations or personnel but do present a risk to external logistical operations or implementation of activities.</li> <li>✓ Increase in inter-tribal violence adjacent to the project area of operations or locations.</li> <li>✓ Vehicle or aircraft movement is disrupted</li> <li>✓ Significant police or paramilitary deployment required to maintain rule of law, localized curfews in place.</li> <li>✓ Heavy-handed response from the police and security service</li> <li>✓ Erosion of the support and goodwill of local communities</li> <li>✓ Difficulties in maintaining good relations with local authorities and traditional leaders</li> </ul>	<ul style="list-style-type: none"> <li>✓ ENTRO/NELSAP-CU shares project personnel (staff, TA, and contractors) details (Name, age, sex, nationality, with their IDs/Passport) with ENSAPT/TAC leaders</li> <li>✓ ENTRO/NELSAP-CU ensures obtainment of support letters for project personnel through ENSAPT/TAC leaders.</li> <li>✓ ENTRO/NELSAP-CU in collaboration with ENSAPT/TAC leaders ensures that the support letters issued to the project personnel (staff, TA, and contractors) contain details of their particulars (Name, age, sex, nationality, and IDs/Passport numbers); and the purpose of project personnel deployment on the sites.</li> <li>✓ ENTRO/NELSAP-CU ensures debriefing of the project personnel on security procedures on the ground, including immediate reporting first to the security agencies/forces before starting their activities.</li> <li>✓ ENTRO/NELSAP-CU complete all pre-planned actions/activities, including training of the project staff, to ensure their awareness of the actions to be taken based on SMP.</li> <li>✓ ENTRO/NELSAP-CU and project personnel closely monitor the security situation, crime levels, and political and social events.</li> <li>✓ ENTRO/NELSAP-CU liaises with authorities and the local community for the collection and assessment of information from the ground.</li> <li>✓ Project personnel maintain close liaison with GRM Focal Point and build good relations with local communities.</li> <li>✓ ENTRO/NELSAP-CU in collaboration with ENSAPT/TAC leaders ensures that the security agencies/forces brief project personnel on the required roles, responsibilities and rules of engagement at the project sites (including information on curfew).</li> <li>✓ Project personnel, in consultation with local authorities, assess requirements to increase physical security controls, access, and road escorts.</li> <li>✓ If the situation is likely to continue, project personnel, in consultation with ENTRO/NELSAP-CU and local authorities, re-assess stocks of resources at project implementation sites and the ability to re-supply (food/water/fuel/people).</li> </ul>
<ul style="list-style-type: none"> <li>• Red</li> </ul>	<p>Implementation of the project has experienced a direct attack or there is credible evidence of an imminent attack.</p> <ul style="list-style-type: none"> <li>• Direct threats against project activity implementation/operations</li> <li>• Major civil disorder in areas of operation</li> <li>• Lines of supply untenable (road closures/security risks)</li> <li>• Total collapse of law and order</li> </ul>	<ul style="list-style-type: none"> <li>• ENTRO/NELSAP-CU prepares project action plans with detailed information on where and when to implement project activities</li> <li>• ENTRO/NELSAP-CU shares project action plans with ENSAPT/TAC leaders</li> <li>• ENTRO/NELSAP-CU ensures all expatriates are registered with the appropriate embassy and all visas and passports are valid.</li> <li>• ENTRO/NELSAP-CU shares project personnel (staff, TA, and contractors) details (Name, age, sex, nationality, with their IDs/Passport) with ENSAPT/TAC leaders</li> </ul>

	<ul style="list-style-type: none"> <li>• Diplomatic missions advise nationals to leave.</li> <li>• No or limited local security forces protection</li> <li>• Security force reaction may damage reputation</li> <li>• Major difficulties in accessing necessities</li> <li>• Frequent power and communications disruption.</li> </ul>	<ul style="list-style-type: none"> <li>• ENTRO/NELSAP-CU ensures obtainment of support letters for project personnel through ENSAPT/TAC leaders.</li> <li>• ENTRO/NELSAP-CU in collaboration with ENSAPT/TAC leaders ensures that the support letters issued to the project personnel (staff, TA, and contractors) contain details of their particulars (Name, age, sex, nationality, and IDs/Passport numbers); and the purpose of project personnel deployment on the sites.</li> <li>• ENTRO/NELSAP-CU ensures debriefing of the project personnel on security procedures on the ground, including immediate reporting first to the security agencies/forces before starting their activities.</li> <li>• ENTRO/NELSAP-CU complete all pre-planned actions/activities, including training of the project staff, to ensure their awareness of the actions to be taken based on SMP.</li> <li>• ENTRO/NELSAP-CU and project personnel closely monitor the security situation, crime levels, and political and social events.</li> <li>• ENTRO/NELSAP-CU liaises with authorities and the local community for the collection and assessment of information from the ground.</li> <li>• Project personnel maintain close liaison with GRM Focal Point and build good relations with local communities.</li> <li>• ENTRO/NELSAP-CU in collaboration with ENSAPT/TAC leaders ensures that the security agencies/forces brief project personnel on the required roles, responsibilities and rules of engagement at the project sites (including information on curfew).</li> <li>• Project personnel, in consultation with local authorities, assess requirements to increase physical security controls, access, and road escorts.</li> <li>• If the situation is likely to continue, project personnel, in consultation with ENTRO/NELSAP-CU and local authorities, re-assess stocks of resources at project implementation sites and the ability to re-supply (food/water/fuel/people).</li> <li>• Project personnel ensure all critical or sensitive documents/equipment have been collected and made ready for evacuation or kept in safe places.</li> <li>• ENTRO/NELSAP-CU in consultation with national security agencies, ensure adequate caretaker security in place for project personnels.</li> <li>• Implement evacuation plan.</li> <li>• ENTRO/NELSAP-CU prepare a plan for the implementation of suspended project activities by devising different approaches.</li> </ul>
--	---	--

**Table 3.2: Alert State-Security Response Level with evacuation Plan for RCRP project sites**

Colors	Event indicators	Recommended Action(s)	Evacuation Plan
<b>Green</b>	<p>No direct threat exists, and no incidents have taken place to warrant heightened security measures.</p> <p>This is the default threat level. There is no current, general, or undirected threat to project-supported works projects within the project mandate. Under this level, the status remains at GREEN.</p> <ul style="list-style-type: none"> <li>✓ Site activities are running normally with employees going about their lives with no or very limited restrictions.</li> <li>✓ There are no restrictions on vehicle movement</li> <li>✓ Continued good will of the majority of the local community remains assured</li> </ul>	<p>No restriction on normal movement, obedient to the local respective governments of the four countries at different levels for guidance. Staff and vehicles may move around the area within the protective envelope of the project area security.</p>	<ul style="list-style-type: none"> <li>• ENTRO/NELSAP-CU prepares project action plans with detailed information on where and when to implement project activities</li> <li>• ENTRO/NELSAP-CU shares project action plans with ENSAPT/TAC leaders</li> <li>• ENTRO/NELSAP-CU ensures all expatriates are registered with the appropriate embassy and all visas and passports are valid.</li> <li>• ENTRO/NELSAP-CU shares project personnel (staff, TA, and contractors) details (Name, age, sex, nationality, with their IDs/Passport) with ENSAPT/TAC leaders</li> <li>• ENTRO/NELSAP-CU ensures obtainment of support letters for project personnel through ENSAPT/TAC leaders.</li> <li>• ENTRO/NELSAP-CU in collaboration with ENSAPT/TAC leaders ensures that the support letters issued to the project personnel (staff, TA, and contractors) contain details of their particulars (Name, age, sex, nationality, and IDs/Passport numbers); and the purpose of project personnel deployment on the sites.</li> </ul>
<b>Yellow</b>	<p>Increased level of disturbance and/or increased probability of impact to project activities. Sporadic civil disorder events. A direct threat has been detected to one or more areas of the operation, but it is not considered imminent.</p> <ul style="list-style-type: none"> <li>✓ Area-wide protests and/or strike action that do not directly impact project operations or personnel but do present a risk to external logistical operations or implementation of activities.</li> <li>✓ Increase in inter-tribal violence adjacent to the project area of operations or locations.</li> <li>✓ Vehicle or aircraft movement is disrupted</li> <li>✓ Significant police or paramilitary deployment required to maintain rule of law, localized curfews in place.</li> </ul>	<p>Project operations continue. Enhanced security controls and operational restrictions required.</p>	<ul style="list-style-type: none"> <li>• ENTRO/NELSAP-CU prepares project action plans with detailed information on where and when to implement project activities</li> <li>• ENTRO/NELSAP-CU shares project action plans with ENSAPT/TAC leaders</li> <li>• ENTRO/NELSAP-CU ensures all expatriates are registered with the appropriate embassy and all visas and passports are valid.</li> <li>• ENTRO/NELSAP-CU shares project personnel (staff, TA, and contractors) details (Name, age, sex, nationality, with their IDs/Passport) with ENSAPT/TAC leaders</li> <li>• ENTRO/NELSAP-CU ensures obtainment of support letters for project personnel through ENSAPT/TAC leaders.</li> <li>• ENTRO/NELSAP-CU in collaboration with ENSAPT/TAC leaders ensures that the support letters issued to the project personnel (staff, TA, and contractors) contain details of their particulars (Name, age, sex, nationality, and IDs/Passport numbers); and the purpose of project personnel deployment on the sites.</li> </ul>

	<ul style="list-style-type: none"> <li>✓ Heavy-handed response from the police and security service</li> <li>✓ Erosion of the support and goodwill of local communities</li> <li>✓ Difficulties in maintaining good relations with local authorities and traditional leaders</li> </ul>		<ul style="list-style-type: none"> <li>• ENTRO/NELSAP-CU ensures debriefing of the project personnel on security procedures on the ground, including immediate reporting first to the security agencies/forces before starting their activities.</li> <li>• National security agencies/forces alert personnel based on the real-time security situation.</li> </ul>
Red	<p>Implementation of the project has experienced a direct attack or there is credible evidence of an imminent attack.</p> <ul style="list-style-type: none"> <li>✓ Direct threats against project activity implementation/operations</li> <li>✓ Major civil disorder in areas of operation</li> <li>✓ Lines of supply untenable (road closures/security risks)</li> <li>✓ Total collapse of law and order</li> <li>✓ Diplomatic missions advise nationals to leave.</li> <li>✓ No or limited local security forces protection</li> <li>✓ Security force reaction may damage reputation</li> <li>✓ Major difficulties in accessing necessities</li> </ul> <p>Frequent power and communications disruption.</p>	<p>Suspension of operations and/or activation of total lockdown or evacuation plan.</p>	<ul style="list-style-type: none"> <li>• ENTRO/NELSAP-CU prepares project action plans with detailed information on where and when to implement project activities</li> <li>• ENTRO/NELSAP-CU shares project action plans with ENSAPT/TAC leaders</li> <li>• ENTRO/NELSAP-CU ensures all expatriates are registered with the appropriate embassy and all visas and passports are valid.</li> <li>• ENTRO/NELSAP-CU shares project personnel (staff, TA, and contractors) details (Name, age, sex, nationality, with their IDs/Passport) with ENSAPT/TAC leaders</li> <li>• ENTRO/NELSAP-CU ensures obtainment of support letters for project personnel through ENSAPT/TAC leaders.</li> <li>• ENTRO/NELSAP-CU in collaboration with ENSAPT/TAC leaders ensures that the support letters issued to the project personnel (staff, TA, and contractors) contain details of their particulars (Name, age, sex, nationality, and IDs/Passport numbers); and the purpose of project personnel deployment on the sites.</li> <li>• ENTRO/NELSAP-CU ensures debriefing of the project personnel on security procedures on the ground, including immediate reporting first to the security agencies/forces before starting their activities.</li> <li>• National security agencies/forces alert personnel based on the real-time security situation.</li> <li>• National security agencies/forces escort project personnel to relocate them to safe places.</li> <li>• ENTRO/NELSAP-CU in collaboration with National security agencies/forces, arranges logistics for evacuation project personnel to the desired destination.</li> </ul>

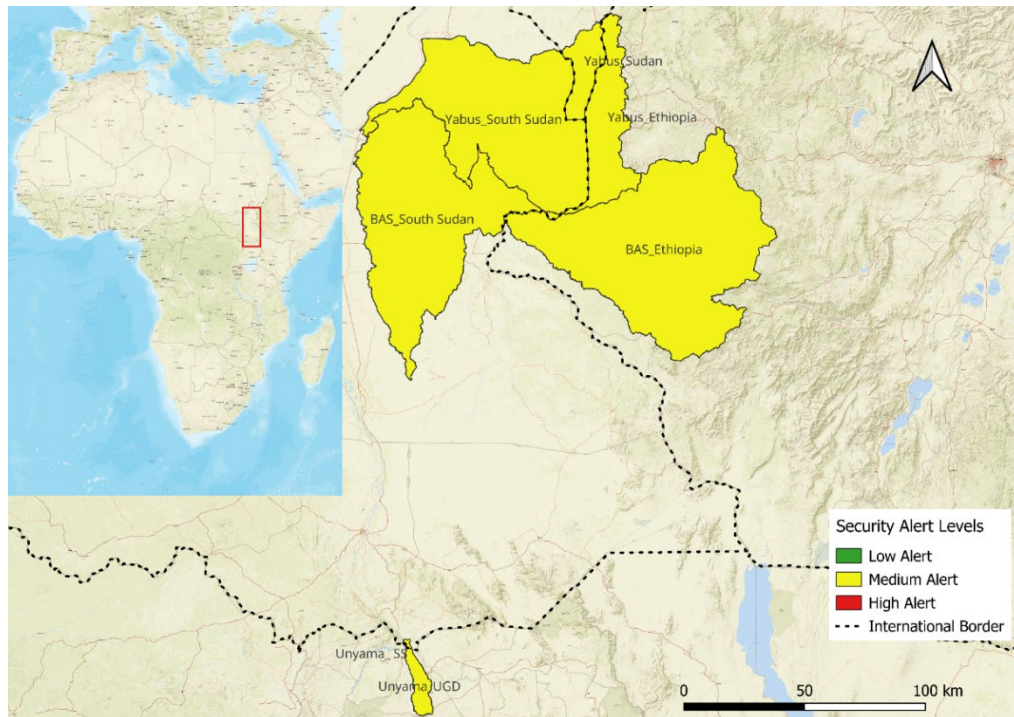
### 3.1 Alert State Status Information

Security Alert State Information will be displayed on the ENTRO website through a dedicated page, indicating the current security status of project sites and any associated movement restrictions.

The website presents Security Alert Levels using a simple, color-coded system displayed by project site, as follows:

- **Low Alert** – Indicates a stable security situation with no restrictions on movement.
- **Medium Alert** – Indicates heightened security concerns; movement is restricted and may be limited to daytime travel only, subject to curfews and management approval.
- **High Alert** – Indicates a severe security situation; movement is suspended and field activities are temporarily halted.

Figure 3.1 depicts the prevailing security alert map of the RCRP project implementation sites (BAS, Yabus and Unyama) in Ethiopia, South Sudan, Sudan and Uganda. The color code provides a medium level alert for project personnel and stakeholders.



**Figure 3.1: Security status map of RCRP project sites (BAS, Yabus and Unyama) in Ethiopia, South Sudan, Sudan and Uganda**

### 3.2 Journey Management Plan (JMP)

In addition, movements of Technical Assistants (TAs) and project staff will be guided by the approved Journey Management Plan (JMP) (**Annex V**). Project activities and schedules will be adjusted as necessary in response to the prevailing security conditions at each site. Concerning security information, ENTRO & NELSAP-CU liaise with ENSAPT & TAC leaders in the respective countries where the project is implemented—namely Ethiopia, South Sudan, Sudan, and Uganda—who serve as key sources of reliable and up-to-date information on the security situation at project sites. ENSAPT/TAC leaders play a critical role in monitoring and reporting local security dynamics, including emerging threats, community tensions, conflict incidents, and any changes in the overall risk environment. Through their close engagement with national and local authorities, security institutions, community leaders, and project partners, ENSAPT/TAC leaders provide timely, reliable, and context-specific security updates of the project implementation sites.

Subject to the prevailing security situation permitting field activities, ENTRO, NELSAP-CU & the TAs will ensure:

- Communication of the start of any field activity to the World Bank, by submitting the field trip plans, ahead of visits.
- Issuance of official support letters by respective governments (addressed “*To Whom It May Concern*” or to the relevant government authorities in the project implementation countries at all levels) for personnel deployed to project sites.
  - These letters will specify the purpose and objectives of the field activities, the roles and responsibilities of the personnel, and their official identification details.
  - Upon receipt of the support letters for deployed personnel, from the relevant government agencies in the respective countries, including the ones to the local authorities in the areas where field activities will be conducted, the planned field activities can be launched.
  - These letters will facilitate coordination and, where necessary, enable guidance or support from humanitarian organizations, unarmed or armed security personnel, depending on the prevailing security conditions on the ground.
  - Furthermore, the respective government agencies and associated bodies such as the humanitarian organizations will advise on the means and routes of transportation to the sites and accommodation thereat.
- Undertaking of awareness-raising activities to ensure that the Security Management Plan is well understood and effectively implemented by project staff, TAs, and all relevant stakeholders.

### **3.3 Institutional Arrangements and Decision-Making Processes**

The deployed personnel from the TAs and other participating stakeholders must be taken through awareness-raising sessions, so that they understand the prevailing security environment on the ground, including the safeguards to follow and available evacuation opportunities. They must meet local authorities on arrival, make courtesy calls to the highest authority or high-ranking officials; and introduce themselves, their activity agenda/program and submit their support letters.

Once they have completed introductory procedures with the authorities in the area where field activities are taking place, they must establish further contacts with the other relevant bodies such as the humanitarian organizations consortium and continue coordinating implementation of their planned field activities.

On the ground the role in security management and decision making is very much played by the deployed personnel in collaboration with local authorities through their organized or law enforcement forces/agencies; well-placed bodies like the humanitarian organizations; TAs; and ENTRO & NELSAP-CU project coordinators.

In coordination with the ENTRO & NELSAP-CU Managements and the TAs, the Lead Technical Specialist coordinating the ENTRO & NELSAP-CU Project Management Unit (PIU), will timely and promptly advise or approve the decisions to be taken, e.g., suspension/cancelation of work/activity; withdrawal/evacuation from the field, etc.

## **4. OVERVIEW OF KEY LABOR RISKS ON THE PROJECT**

Key labour risks are associated with health and safety risks related to direct and contracted workers/professionals by the consultants; in addition to participating stakeholders, ENTRO, and NELSAP-CU personnel traveling for or involved on the ground in project activities in the region covered by ENTRO & NELSAP-CU RCRP activities, as well as OHS-related risks in office for the consultants, ENTRO and NELSAP-CU employees.

### **4.1 Overview of Labor Use on the Project**

#### *4.1.1 Direct workers*

Direct workers include all staff dedicated to project implementation and management, which sum up to about 25 workers from ENTRO and NELSAP-CU. It is expected that direct workers will also include independent consultants, specialized in certain disciplines. These consultants will be hired under individual contracts, on a part-time basis, with a specific definition of the assigned tasks and responsibilities. It is estimated that the total number of direct workers will reach 30-35 workers, depending on the project phase.

#### *4.1.2 Contracted workers*

Research, Technical Assistance, and assessment activities require the use of consultancy firms, research companies or organizations. The companies' workforce will be considered under the category 'contracted workers'. About 3 associations of companies are currently engaged in the Project with 10-15 workers each.

#### *4.1.3 Security Personnel*

At the project implementation sites in the countries, depending on the security threat/risk level, the project will use security personnel (being experts/unarmed or armed), like the local police, who may be engaged by institutions supporting the project implementation at all levels as appropriate. Care will be taken to ensure that the assignment of security personnel will not result in additional risks to communities or individuals within the project implementation areas.

#### *4.1.4 How to address Labor Risks*

Site visits will be required for assessments, research and stakeholder consultations. Risks related to travel include fatigue, working in hot climates, lack of security, conflict and conflict-related violence, potential attack by wild animals and traffic accidents. In addition, the management of social and cultural risks, such as entering private property without permission, inappropriate clothing and behavior, and workplace interactions among workers and management, will be required.

Other labor risks include non-compliance with programme hosting country laws, i.e., Ethiopia's or Rwanda's labor standards and laws, as well as ESS2. For example, non-compliance with terms and conditions of contract, discrimination at the workplace, lack of equal opportunities for women, lack of respect to the role of workers' organizations, lack of compliance with working, or unavailability of workers' Grievance Redress Mechanism (GRM). Further risks are related to Sexual Exploitation and Abuse (SEA) and Sexual Harassment (SH) at the workplace or vis-à-vis beneficiaries or contractors'/clients' personnel.

The risks above will be mitigated through following specific actions listed in the LMP, including Code of Conduct, Travel Safety Plan, and SEA/SH mitigation measures, as appropriate.

On the other hand, deployment of security personnel may result in additional risks to communities or individuals within the project implementation areas. For instance, there may be excessive use of force in situations involving protests or intimidation in situations involving grievances.

### **4.2 Security Personnel Related Grievances Redress Mechanism (GRM)**

Care will be taken to ensure that deployment of security personnel or presence of security forces will not result in additional risks to communities or individuals within the project implementation areas. In accordance with good international practice and the World Bank Environmental and Social Framework (particularly ESS2 and ESS4), the RCRP shall operationalize its Project

Grievance Redress Mechanism (GRM) to address all security-related complaints in an accessible, transparent, and non-retaliatory manner.

Upon receipt of a complaint, GRM Focal Points at each project implementation site shall:

- Acknowledge and record the grievance in a secure register.
- Assess the nature and severity of the complaint.
- Initiate a timely and impartial investigation.
- Coordinate, where appropriate, with national law enforcement or oversight institutions in accordance with applicable laws; and
- Communicate resolution outcomes to the complainant.

Grievances involving security personnel shall comply with the regulatory frameworks governing national police services, security oversight bodies, and independent policing accountability institutions in each participating country. Where allegations involve criminal conduct, cases shall be formally referred to competent authorities.

The GRM shall ensure:

- Multiple accessible entry points, including anonymous reporting options;
- Confidential handling of sensitive complaints, especially SEA/SH;
- A survivor-centered approach for SEA/SH cases;
- Protection against retaliation for complainants and witnesses;
- Documentation and tracking of grievance trends;
- Periodic reporting to project leadership; and
- Allocation of adequate financial, technical, and human resources to ensure effective implementation.

The effectiveness of the security-related grievance mechanism shall be reviewed periodically, and corrective measures shall be implemented as necessary to strengthen accountability and community trust.

## 5. ANNEXES

### 5.1 Annex I: *i*Adopted ENTRO & NELSAP-CU RCRP Project Security-Related Grievance Redress

#### *Process Flow-Chart*

START



1. Complaint Lodged

(Community member, worker, TA, contractor, or other stakeholder)

- Verbal
- Written
- Phone/SMS
- Suggestion box
- Anonymous submission



2. Receipt & Registration by Site GRM Focal Point

- Log complaint in grievance register
- Assign reference number
- Acknowledge receipt (within defined timeframe)



3. Initial Screening & Classification

- Is it security-related?
  - └─ NO → Refer to appropriate project unit → Continue standard GRM process
  - └─ YES → Proceed to Step 4



4. Risk Assessment

- Does it involve:
  - SEA/SH?
  - Excessive use of force?
  - Criminal conduct?
  - Immediate safety risk?
- └─ YES → Immediate protective measures + escalate to Project Management
- └─ NO → Proceed to investigation



5. Investigation

- Conduct impartial review
- Interview relevant parties
- Maintain confidentiality

- Coordinate with national policing/oversight authorities if required



#### 6. Decision & Resolution

- Determine corrective action:
  - Warning / disciplinary action
  - Suspension / removal
  - Contract termination
  - Referral to law enforcement
- Develop response plan



#### 7. Communication of Outcome

- Inform complainant (where possible)
- Ensure confidentiality (especially for SEA/SH cases)



#### 8. Monitoring & Follow-up

- Verify implementation of corrective action
- Monitor for retaliation
- Record case closure



#### 9. Reporting & Documentation

- Update grievance database
- Include in periodic E&S reports
- Analyze trends and lessons learned



END (Case Closed)

## **5.2 Annex II: ENTRO & NELSAP-CU RCRP Project Security Personnel Code of Conduct**

### **1. Purpose**

This Code of Conduct outlines the mandatory standards of behavior for all security personnel assigned to the Regional Climate Resilience Project (RCRP). Compliance with this Code is a condition of employment and engagement on the project.

### **2. General Conduct**

As a member of the project security team, I commit to:

- Perform my duties professionally, lawfully, and with integrity.
- Respect the human rights, dignity, and cultural values of all people.
- Treat project staff, Technical Assistants (TAs), contractors, sub-consultants, and community members fairly and without discrimination.
- Carry out my duties only within my assigned mandate.
- Wear proper identification while on duty and carry the ID for identification.

### **3. Prohibited Behaviors**

I understand that the following behaviors are strictly prohibited:

#### **A. Sexual Exploitation and Abuse (SEA)**

- Engaging in sexual activity with anyone under 18 years of age.
- Exchanging money, goods, services, protection, or employment for sexual favors.
- Using my position of authority to obtain sexual advantage.

#### **B. Sexual Harassment (SH)**

- Unwelcome sexual advances or comments.
- Inappropriate touching or gestures.
- Any behavior that creates a hostile or intimidating environment.

#### **C. Abuse of Authority**

- Threatening, intimidating, or harassing any person.
- Using excessive or disproportionate force.
- Discriminating based on gender, ethnicity, religion, disability, age, or social status.

#### **D. Retaliation**

- Threatening or harming anyone who reports misconduct.
- Interfering with or discouraging the use of grievance mechanisms.

#### **E. Corruption**

- Accepting bribes or favors.
- Extorting money or goods from deployed project personnel or community members.
- Misusing project property or authority.

#### **4. Use of Force**

I understand that:

- Force may only be used as a last resort.
- Any use of force must be lawful, necessary, and proportionate.
- All security incidents must be reported immediately to my supervisor.
- Weapons, if authorized, must be handled and stored safely.

#### **5. Community Interaction**

I will:

- Engage respectfully with community members.
- Avoid unnecessary confrontation.
- Respect local customs and traditions.
- Avoid isolated interactions with vulnerable people where possible.

#### **6. Reporting Obligations**

I agree to:

- Immediately report any misconduct, including SEA/SH allegations.
- Cooperate fully in investigations.
- Maintain confidentiality in handling complaints.

Failure to report known misconduct is a violation of this Code.

#### **7. Disciplinary Measures**

I understand that violation of this Code may result in:

- Warning or suspension
- Termination of employment or contract
- Referral to law enforcement authorities

#### **8. Declaration**

I, the undersigned, confirm that:

- I have read and understood this Code of Conduct.
- I agree to comply fully with its provisions.
- I understand the consequences of non-compliance.

Name: \_\_\_\_\_

Position: \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

<sup>1</sup><https://documents.worldbank.org/en/publication/documents-reports/documentdetail/459271468338378246/addressing-grievances-from-project-affected-communities-good-practice-note>

### 5.3 Annex III: Definition of Impact Levels

Impact Level	Physical Harm (People)	Financial Loss	Reputational Damage	Operational Impact
Low	Minor injuries (first aid only); no lost time	Minimal loss; absorbed within the routine budget	Limited local concern; no media attention	Minor disruption; quickly recoverable
Low–Medium	Minor injuries requiring medical attention; short recovery	Small financial loss; manageable within contingency	Localized negative perception; limited stakeholder concern	Short-term disruption to activities
Medium	Serious but non-fatal injuries; temporary disability	Moderate financial loss; requires budget reallocation	Noticeable impact; local/regional attention	Delays in implementation; partial suspension of activities
Medium–High	Severe injuries; potential long-term disability	Significant financial loss; affects some project components	Regional/national attention; trust affected	Major disruption: key components delayed or halted
High	Fatalities or multiple severe injuries	Major financial loss; threatens overall project sustainability	Widespread damage; national/international scrutiny	Project suspension or shutdown; critical operational failure

### 5.4 Annex IV: Definition of Risk Levels Rating

Likelihood Level	Definition	Typical Frequency / Probability
<b>Very Likely</b>	The event is expected to occur in most circumstances; strong evidence or past occurrences exist.	>80% chance / occurs frequently (e.g., multiple times per year)
<b>Likely</b>	The event will probably occur in many circumstances; it has happened before.	60–80% chance / occurs regularly
<b>Possible</b>	The event might occur at some time; there is a reasonable chance, but not certain.	30–60% chance / occurs occasionally
<b>Unlikely</b>	The event could occur but is not expected; limited history or conditions are required.	10–30% chance / occurs rarely
<b>Very Unlikely</b>	The event is highly improbable; it would occur only in exceptional circumstances.	<10% chance / very rare or not observed before

Note: These definitions are aligned with international risk management practices such as ISO 31000 and World Bank SMP approaches

## 5.5 Annex V: Journey Management Plan for the RCRP project

### SECTION 1: GENERAL INFORMATION

Office	ENTRO/NELSAP-CU
Project Name	RCRP
Project Implementation Sites	BAS, Yabus, and Unyama
Field supervisor Name/Coordinator Name	RCRP Lead at ENTRO, Eng. Isaac Liabwel
Field Supervisor Coordinator Direct Report	ENTRO Acting ED, Eng. Teshome
Author of Journey Management Plan	RCRP S&E Officer at ENTRO, Dr. Assefa Gudina

### Section 2: Specific Information

Departure location	
Departure Date	
Destination location (Country/City/Province/Region/Woreda)	
Arrival Date	
RCRP project Threat alert level of the destination location	
Return Date	

### Section 3: Traveler Information

Name	Nationality	ID Number (local government or passport)
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.

### SECTION 4: THREAT INFORMATION

Question	Yes/ No	Describe
----------	---------	----------

Are there any current alerts or threats reported along the route?	Choose an item.	Click or tap here to enter text.
Are there any current alerts or threats reported at the destination?	Choose an item.	Click or tap here to enter text.

## SECTION 5: SECURITY SUPPORT

Question	Yes/ No	Describe
Will a Security Subcontractor or Team be Used?	NO	Click or tap here to enter text- Provide details including name of company/organization, composition with numbers of personnel and all other details relating to their tasks.

## SECTION 6: TRAVEL TO LOCATION

### AIR TRAVEL

<b>Will air travel be used?</b> <i>(If No, select No, and mark each cell below as "N/A")</i>	YES
<b>Departure Date</b>	Click or tap to enter a date.
<b>Departure Time</b>	TBD
<b>Departure Airport</b>	TBD
<b>Airline and Flight</b>	TBD
<b>Arrival Date</b>	TBD
<b>Arrival Time</b>	TBD
<b>Arrival Airport</b>	TBD

### ADDITIONAL FLIGHT TABLE IF NEEDED

Departure Date	Click or tap to enter a date.
Departure Time	Click or tap here to enter text.
Departure Airport	Click or tap here to enter text.
Airline and Flight	Click or tap here to enter text.
Arrival Date	Click or tap here to enter text.
Arrival Time	Click or tap here to enter text.
Arrival Airport	Click or tap here to enter text.

### AIRPORT PICK-UP

<b>Driver/s Contact Information</b> (name, phone #)	
<b>Vehicle/s Details</b>	

(Make, Model, Color and Plate Number)	
<b>Pick-Up Identification</b> (number on sign)	
<b>Specific location where driver/s will meet traveler/s</b>	

## GROUND TRAVEL

<b>Ground Travel will be used?</b> <i>(If No, select No and mark each cell below as "N/A").</i>	Choose an item.
<b>Departure Date</b>	TBD
<b>Departure Time</b>	TBD
<b>Departure Point</b>	TBD
<b>Driver/s Contact Information</b> (name, phone #)	N/A
<b>Vehicle/s Details</b> (Make, Model, Color and Plate Number)	N/A
<b>Arrival Date</b>	N/A
<b>Arrival Time</b>	N/A
<b>Arrival Location</b>	N/A

## VEHICLE INSPECTION (MUST MEET MINIMUM STANDARDS)

<b>Functional Seatbelts</b>	YES
<b>Tire Change Kit</b>	YES
<b>Spare Tire</b>	YES
<b>First Aid Bag</b>	NO
<b>Flashlight</b>	NO
<b>Water</b>	YES
<b>Food (only for journeys &gt; 3 hours)</b>	NO

## SAFE-HAVENS ALONG THE ROUTE

Pre-identified locations along the road route where the travelers can seek shelter if needed.

Property Name	Address with Grid	Contact Information
N/A	N/A	N/A
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.

## SECTION 7: LODGING

<b>Check-in Date</b>	
<b>Check-Out Date</b>	
<b>Name of Property</b>	
<b>Contact Information</b>	

<b>Address with Grid</b>	

**ADDITIONAL LODGING TABLE IF NEEDED**

<b>Check-in Date</b>	Click or tap to enter a date.
<b>Check-Out Date</b>	Click or tap to enter a date.
<b>Name of Property</b>	Click or tap here to enter text.
<b>Contact Information</b>	Click or tap here to enter text.
<b>Address with Grid</b>	Click or tap here to enter text.

**SAFE-HAVEN AT DESTINATION**

Pre-identified location at the destination where travelers can seek shelter if current lodging becomes untenable.

<b>Property Name</b>	<b>Address with Grid</b>	<b>Contact Information</b>
TBD	TBD	TBD

**SECTION 8: VENUE (LOCATION OF ACTIVITY)**

<b>Meeting Date</b>	TBD
<b>Meeting Time</b>	TBD
<b>Name of Property</b>	TBD
<b>Contact Information</b>	TBD
<b>Address with Grid</b>	N/A

**ADDITIONAL VENUE TABLES IF NEEDED**

<b>Meeting Date</b>	TBD
<b>Meeting Time</b>	TBD
<b>Name of Property</b>	TBD
<b>Contact Information</b>	TBD
<b>Address with Grid</b>	TBD

**SECTION 9: RETURN TRAVEL**

Air Travel

<b>Will air travel be used?</b> <i>(If No, select No, and mark each cell below as "N/A").</i>		Choose an item.
<b>Departure Date</b>	TBD	
<b>Departure Time</b>	TBD	
<b>Departure Airport</b>	TBD	

<b>Airline and Flight</b>	TBD
<b>Arrival Date</b>	TBD
<b>Arrival Time</b>	TBD
<b>Arrival Airport</b>	TBD

### Additional Flight Table if Needed

<b>Departure Date</b>	Click or tap to enter a date.
<b>Departure Time</b>	Click or tap here to enter text.
<b>Departure Airport</b>	Click or tap here to enter text.
<b>Airline and Flight</b>	Click or tap here to enter text.
<b>Arrival Date</b>	Click or tap here to enter text.
<b>Arrival Time</b>	Click or tap here to enter text.
<b>Arrival Airport</b>	Click or tap here to enter text.

## 1.1

### Ground Travel

<b>Ground Travel will be used?</b> <i>(If No, select No and mark each cell below as "N/A").</i>	NO
<b>Departure Date</b>	N/A
<b>Departure Time</b>	N/A
<b>Departure Point</b>	N/A
<b>Driver/s Contact Information</b> (name, phone #)	N/A
<b>Arrival Date</b>	N/A
<b>Arrival Time</b>	N/A
<b>Arrival Location</b>	N/A

## 2. Section 10: Communication

<b>Primary Means of Communication</b>	Direct via Mobile Phone
<b>Alternate Means of Communication</b>	Choose an item.
<b>Final Back-up Means of Communication</b>	Choose an item.
<b>Time Interval for Communication Checks During Travel To and From Destination</b>	Click or tap here to enter text.
<b>Phone Tree- 1<sup>st</sup> Call</b>	Click or tap here to enter text.
<b>Phone Tree- 2<sup>nd</sup> Call</b>	Click or tap here to enter Person's Name and Phone #.

<b>Phone Tree- 3<sup>rd</sup> Call</b>	Click or tap here to enter Person's Name and Phone #.
--	---

### 3. Section 11: Medical Emergency

Designation	Name	Address with Grid	Contact Information
<b>Primary Medical Facility</b>	TBD	TBD	TBD
<b>Alternate Medical Facility</b>	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.

Local medical Provider

<b>Provider</b>	TBD
<b>Phone Number</b>	TBD
<b>Client Name</b>	TBD
<b>Policy Number</b>	N/A

### 4. Section 12: Recovery Plan

State how the program will conduct a recovery of travelers should an incident occur during their movement to or from their destination.

Click or tap here to enter text.
----------------------------------

### 5. Section 13: Authorization Signature

By signing the below, the RCRP project Lead Technical Specialist, authorizes this travel to be conducted.

Date	
Name	
Title	
E-mail	
Phone Number	