The Republic of Uganda

MINISTRY OF AGRICULTURE, ANIMAL INDUSTRY AND FISHERIES

UGANDA CLIMATE SMART AGRICULTURAL TRANSFORMATION PROJECT (UCSATP)

PROJECT SECURITY MANAGEMENT PLAN

December, 2025

Table of Contents

PROJECT SECURITY MANAGEMENT PLAN

1 BACKGROUND

The Ministry of Agriculture Animal Industry and Fisheries (MAAIF) is implementing a six (6) year Uganda Climate-Smart Agricultural Transformation Project (UCSATP) with a Project Development Objective (PDO) of increasing productivity, market access, and resilience of select value chains in the project area and to respond promptly and effectively to an eligible crisis or emergency. The Project components include: (i) Strengthening Climate Smart Agricultural Research, Seed, and Agro-Climatic Information Systems; (ii) Promoting Adoption of Climate Smart Agriculture Technologies and Practices; (iii) Market Development and Linkages to Selected Value Chains; (iv) Contingency Emergency Response Component; (v) Project Management, Coordination, and Implementation. The Project is being implemented in 69 districts including 7 selected refugee host districts, covering value chains of crop, livestock, fisheries, and beneficial insects.

Execution of project interventions may require involvement of security with a sole purpose of providing and maintaining a safe physical environment and managing staff activities to reduce the risk of personal injury and property loss. MAAIF through the UCSATP National Project Coordinator has an overall responsibility of ensuring that security procedures and criteria are fully designed and updated, and the means fully available to ensure the security for project operations. Ultimately, the Project Security Management Plan has been developed with clear operational modalities in respect of various security alerts that may occur during project implementation.

1.1 Purpose of the Security Management Plan

This plan has been prepared to;

i. describe how security is organized to face identified threats; and
ii. how security will be continuously reassessed and reorganized in correlation with security situations and operations being undertaken

Whenever deemed necessary, services of a specific security organisation will be sought to provide a secure operating environment to project operations and its contractors while undertaking operations in the insecure areas such as Karamoja region and/ throughout the project districts.

1.2 Legal Framework - Standards

This security management plan is anchored on World Bank Environmental and Social Standard 4 (ESS4) that covers Community Health and Safety on sub section (b) Personnel Security in line with the World Bank Good Practice Note on Assessing and Managing Risks and Impacts of the Use of Security. The Plan is also consistent with Police Force Act

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.

MAAIF and all its project implementers shall abide by 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 project implementation. This will be consistent with the national legislation governing security matters.

1.3 Good International Practice

MAAIF and all its project implementers shall ensure that;

i. All deployed security personnel sign a Code of Conduct guided by the principles of proportionality and GIIP, and by applicable law, in relation to hiring, rules of conduct, training, equipping, and monitoring of such security workers;
ii. Any use of force by direct or contracted workers in providing security is not sanctioned except when used for preventive and defensive purposes in proportion to the nature and extent of the threat;
iii. Make reasonable inquiries to verify that the direct or contracted workers retained to provide security are not implicated in past abuses;
iv. All deployed security personnel have adequate training (or determine that they are properly trained) in the use of force (and where applicable, firearms), and appropriate conduct toward workers and affected communities;
v. All deployed security personnel act within the applicable law and any requirements set out in the ESCP; and

vi. All allegations of unlawful or abusive acts of security personnel are reviewed and appropriate action taken (or urge appropriate parties to take action) to prevent recurrence and, where necessary, report unlawful and abusive acts to the relevant authorities.

1.4 Security Management

Security Management for the project lies under the oversight and responsibility of the National Project Coordinator and the District Resident District Commissioners. The management of security for UCSAT project operations will comply with the four basic pillars of security management:

a. ***Detect*** an adversary.
b. ***Deter*** an adversary if possible.
c. ***Delay*** the adversary until appropriate authorities can intervene.
d. ***Respond*** to the adversary's actions.

1.5 Analysis of Security situation in Project Area

Different security risks exist in the selected project districts and can be categorized into:

i. **Internal Risks** may include but not limited to: illegal, unethical, or inappropriate behaviour of project personnel or those directly affiliated with it, such as employee theft, workplace violence, and labor unrest, potentially with associated sabotage).
ii. **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 terrorism, armed insurgency, coups, or war.

Project related security risks

The main security risks within the project districts include:

a. Criminal offences
b. Terrorism
c. Cattle rustling / Inter-tribal or communal violence becomes a threat to project personnel
d. Industrial Action leading to strike or disruption of work, social conflict, civil unrest
e. Breakdown of relationships with Community groups and Committees

f. Reaction of community to an incident or accident involving project personnel or asset.
g. Threat of armed attack
h. Theft/ Larceny
i. Kidnapping

1. **Social conflicts, civil un-rest*:*** The potential main risk is the general population including the local communities, who presume to have been aggrieved that can easily and quickly mobilize for a demonstration. Compensation and environmental as well as social concerns can create this kind of scenario. The crowds will usually include villagers. Most of the time, negotiations can resolve the situation but in some cases an escalation can occur, leading to violent actions.

   Any indications of such a threat must be communicated through the Office of the Resident District Commissioner, the District Police Commander to the designated field Police officers at the nearest Police Post. Complaints may be made to the Police Station officer-in-charge and recorded in an occurrence book for future reference.

   -The Office of the RDC will coordinate all communication between the Security apparatus, the project technical teams local leaders and government entities during any demonstration or unrest. Technical discussions shall be led and guided by the Project Teams both at National, District, Sub-County and Parish levels. Local Structures including the GRCs shall be used in resolving non-security threats That may occur during project implementation.

   However, demonstrations or workers' strikes at National, District and local/contractor/farmer level which could have perceived from discrimination or unfair working conditions in terms of wages, overtime and welfare will be handled in accordance with the Labour Management Procedures.

2. **Criminal Offenses:** The main risk remains small scale thefts of light equipment, nitrogen kits, gas cylinders laboratory equipment, fuel and personal effects which can involve aggressions. The project may be exposed to this kind of criminality.

3. **Terrorism:** There is the ever-imminent threat of terrorism from the lawless Allied Democratic Forces (ADF) rebels based in Democratic Republic of Congo and Al-shabab from neighbouring Somalia which could pose a serious threat to the implementation of the project.

4. **Cattle rustling*:*** Nomadic pastoralists in Northern Kenya and Karamoja Region are known to be armed, and thus pose a direct security risk to the smooth implementation of the project in the Karamoja area, especially if incidents of cattle rustling are prevalent. Security safety measures should be instituted to ensure the safety of project staff and host community during implementation of activities within these areas. . ***However, care must be taken to ensure that security response or presence of security forces does not result in additional risks to communities or individuals within the project implementation areas.***

5. **Sexual Exploitation, Abuse and Harassment (SEAH):** The risk of SEAH in the project activities or operations is expected to be low and all stakeholders especially the girls and women will be sensitised on how to precautionary measures and incident management procedures to be undertaken including referral of incidents. . The project Grievance Redress Mechanism will have a dedicated channel to handle SEAH incidents.

1.6 Security Risk Assessment and Management

The project has adopted a systematic and careful examination of the workplace, work activity, working environment and those people who may be at any security risk. Risk assessments shall identify what might go wrong, evaluation of y security hazards, propose adequate control measures needed to prevent or minimize the potential security risks. A consequence risk assessment matrix below (table 1) has been adopted comprising of the anticipate threat or security risk, likelihood of it happening/occurring and potential impact;

Table 1: shows consequence risk assessment matrix

Threat	Likelihood	Impact
Site invasions	Medium	High
Banditry/gang theft	Medium	High
Violent attack	Medium	High
Terrorism	Low	Medium
Targeted activism	Medium	Medium

Threat	Likelihood	Impact
Theft	Medium	Medium

The Likelihood verses Consequences Risk Assessment Matrix has been supported with table 2 which shows the risks with the mitigations, roles and responsibilities and timelines in respect to a security situation.

Table 2: shows consequence risk assessment, severity, mitigations, roles and responsibilities in respect to a security situation.

SN	Risk description	Likelihood of the risk occurring	Impact if risk occurs	Severity	Responsibility (Person who will manage the risk)	Mitigating action (action to avoid or reduce the risk impact	Contingent action (Action to be taken if the risk happens)	Progress on actions	Resource materials
	Criminal offences: Theft/ Larceny	**Medium**	**Medium**	**Medium**	**PC**	• Use of physical security personnel i.e., private unarmed security guards • Staff crime security awareness, • Permanently etching on equipment (spray paint and initials on a piece of equipment does not qualify as being "positively" identified). • Installation CCTV and Alarm Systems: either standalone or integrated combined with wireless communication to an off-site, • Establish formal and consistent reporting and communications mechanisms with public security forces and other stakeholders • Adequate lighting, • Perimeter fencing especially materials areas and camp(s).	• Escalate to the Project Coordinator • Undertake joint risk assessment process including representatives of Police Force (PF) in use • Maintain close contact with representatives of Police Force at different levels		

SN	Risk description	Likelihood of the risk occurring	Impact if risk occurs	Severity	Responsibility (Person who will manage the risk)	Mitigating action (action to avoid or reduce the risk impact	Contingent action (Action to be taken if the risk happens)	Progress on actions	Resource materials
	Terrorism	Medium	High	High	Project Coordinator	• Enhance intra/intra agency cooperation within the project area and PF. • Meet on regular basis with the security apparatus at the sub-county and district level • Assess the security situation and make changes to the security management plan • Ensure travelling project staff have PF escort • Engage with and empower border communities as key contributors in border security and management, • Implement Border Community Policing programs, • Implement information exchange programs and mechanisms	• Conduct effective risk analysis assessments, and SWOT analyses and Force-Field Analyses related to gaps and needs assessments		
	Cattle rustling	Medium	Medium	Medium	Project Coordinator	• Initiate peace building process among the affected project counties, • Use Traditional institutions in creating peace, security, law and	• Strengthening of surveillance within the County boundaries and develop		

SN	Risk description	Likelihood of the risk occurring	Impact if risk occurs	Severity	Responsibility (Person who will manage the risk)	Mitigating action (action to avoid or reduce the risk impact	Contingent action (Action to be taken if the risk happens)	Progress on actions	Resource materials
						order in community policing and conflict management, • Carry out civic education by use of the local Civil Society Groups, and offer vocational and technical skills to the youths and or initiate income generating project to engage youths	protocols for cross border use,		
	Armed	Medium	High	High	Project Coordinator	• Use of physical security personnel, • Staff crime security awareness, • Permanently etching on equipment (spray paint and initials on a piece ofequipment does not qualify as being"positively" identified). • Installation CCTV and Alarm Systems: either standalone or integrated combined with wireless communicationto an off-site, • Establish formal and consistent reporting and communications mechanisms with Police forces and other stakeholders	• Never fight back when apprehended with armed people, • 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), • Inform the victim's family timely manner, • Do not make any sudden movements that might startle the criminals or be interpreted as an attempt to resist or escape,		

SN	Risk description	Likelihood of the risk occurring	Impact if risk occurs	Severity	Responsibility (Person who will manage the risk)	Mitigating action (action to avoid or reduce the risk impact	Contingent action (Action to be taken if the risk happens)	Progress on actions	Resource materials
						• Adequate lighting • Perimeter fencing especially materials areas and camp (s).	• Do not hesitate if told to move and do so in a controlled manner. • Do not try to argue or make provocative comments. • Do not stare or make eye contact with the criminals.		
	Industrial Action	Low	Medium	Medium	Project Coordinator	• Adhere to all provisions in the Project Labour Management Procedures, • Understand the nature of the dispute the stated reasons, the underlying reasons and any "hidden agenda",	• Use the alternative dispute resolution: Conciliation, mediation and or arbitration, • Identify the legal strategy to be pursued and associated consequences		UCSATP Labour Management Procedures
	Community Hostility	Low	Medium	Medium	Project Coordinator	Adhere to all provisions in the Project Stakeholder Engagement Plan,	Set some ground rules within the community groups, and Revisit the group's purpose.		UCSATP Stakeholder Engagement Plan

SN	Risk description	Likelihood of the risk occurring	Impact if risk occurs	Severity	Responsibility (Person who will manage the risk)	Mitigating action (action to avoid or reduce the risk impact	Contingent action (Action to be taken if the risk happens)	Progress on actions	Resource materials
	SEAH and incident response	Low	Low	Low	Project Coordinator	• Adhere to all provisions in the Project Grievance Redress Mechanism • Abide by the requirements of SEAH Action Plan for the project beingprepared,	Continuous SEAH awareness creation the hired firm.		UCSATP Grievance Mechanism/ UCSATP SEAH Action Plan

Due diligence involving back ground checks shall be undertaken by the NPCU to ensure that only security personnel from reputable security firms or organisations are engaged. The unarmed security personnel shall undertake basic security duties such as access control and perimeter security management; and if deemed necessary, the police may be engaged on a reactive basis. This approach will alleviate undue pressure on local policing resources and reduce the risks of engaging armed officers. An appropriate, formal agreement will be developed to support service delivery and mitigate the identified security risks and respond to any stakeholder concerns.

NB: Care will be taken to ensure that security response or presence of security forces will not result in additional risks to communities or individuals within the project implementation areas.

2 PROJECT ALERT STATUS

The Project Alert levels provide specific guidance on recommended security measures and actions to be adopted on the basis of the prevailing security situation, locally, nationally and internationally, ultimately taking into consideration security context issues at a given project location.

Local and regional events (triggers) will be linked to the district alerts; the local security situation will be monitored daily and all available information assessed to ensure early identification of any increase in risk, which may require a change in alert state. Change of rate level will be done on instruction from the NPCU.

The following alert status evoking the security state response levels (depicted with colour shades of Green, Yellow, Orange and Red respectively), triggers and actions specific to the project site is elaborated in Tables 3,4,5,6 below:

Table 3: Security Response Level: Green- Business as Usual- Security Risks Effectively Controlled

Security Response Level GREEN **Business as Usual- Security Risks Effectively Controlled**	
Event Indicator	**Recommended Action(s)**
No direct threat exists and no incidents have taken place to warrant heightened security measures: This is the default threat level. There is no current, general, or undirected threat to government supported works projects within the district. Under this level the status remains at GREEN.	**No restriction to normal movement compliant with local Journey Management Plan (JMP) requirements. Staff and vehicles may move around the area within the protective envelope of the project area security.** • Complete all pre-planning actions • All visitors or returning staff receive an arrivals Security brief • Train staff and ensure awareness of actions to be taken- site drills.

Security Response Level GREEN Business as Usual- Security Risks Effectively Controlled	
Event Indicator	**Recommended Action(s)**
• Site operations are running normally with employees going about their lives with no, or very limited, restrictions. • There are no restrictions on vehicle movement or crew changes • Peaceful protest demonstrations take place. • Occasional unrest or demonstrations away from operational sites. No direct threat to the operation • Effective government control and/or rule of law in place. Liaison remains regular and effective • Continued good will of the majority of the local community remains assured	• Ensure JMP is in place and followed • All crisis management and evacuation plans are in place and are maintained as 'living documents' • The security situation, crime levels, political and social events are monitored closely. On-going collection and assessment of information through liaison with authorities and local community, • Ensure daily Personnel On Board (POB) is maintained. • All stakeholders are aware of the contents of the evacuation plan and understand their role within it • Vehicle Escorts taken when traveling to areas where civil unrest or cattle raids has occurred. • Maintain close liaison with project Social Development Officer and good Community Relations
STANDARD OPERATING PROCEDURES	
Project Security Assets <u>Police Foot Patrols and Escort:</u> Roles and responsibilities include: • The conduct of regular inner peripheral patrols and reporting of findings to Control room. • To ensure safe weapon handling and clearing is carried out at the unloading bays prior to entry to the guard rest area or main compound. • Gathering information and intelligence by interaction with local people. • Questioning of strangers or suspicious persons or vehicles.	

Security Response Level GREEN Business as Usual- Security Risks Effectively Controlled	
Event Indicator	**Recommended Action(s)**
• Observing physical signs or evidence of potential hostile activity or presence (Noise, footprints, fire traces, etc.) and reporting to Control Room. • Developing Hearts & Minds assurances with the community of security in the Area. • Developing community relations on behalf of UCSATP. • Creating a deterrent factor by the presence of the patrol in the area <u>Centralized Mobile Police Patrols</u> • **Introduction**: The Centralized Police Mobile Patrols has responsibility for security of the entire project by patrolling the surrounding area, visiting areas of possible threat, local villages and satellite locations. Their secondary responsibility is to provide immediate reaction and support inner peripheral security, **Roles and responsibilities of** Officer-in-Charge of Station include: • conducting regular area patrols and reporting of findings • Carrying out pre-arranged visits to the Airstrip, boreholes, valley dams, animal holding grounds, community markets, and other areas of interest. • React to Emergency situations as a Quick Reaction Force as directed, • Ensure that safe weapon handling and clearing is carried out at the unloading bays prior to entry to the guard rest area or main compound, • Gathering information and intelligence by interaction with and questioning local people, • Questioning of strangers or suspicious persons or vehicles, • Developing hearts and minds assurances with the community of security in the area, • Developing community relations on behalf of UCSAT project, • Creating a deterrent factor by the presence of the patrol in the area. <u>Base Camp Sites/Project Offices:</u> • Main Gate - Barrier Check of vehicle occupants and main gate access control. Random Cursory Vehicle searches on arrival and random checks (10% of vehicles) on departure to deter theft or when a vehicle is deemed suspicious.	

Security Response Level GREEN Business as Usual- Security Risks Effectively Controlled	
Event Indicator	**Recommended Action(s)**
• Perimeter Foot Patrol – Daytime (every hour at irregular times around camp/office perimeter). • Assist Journey Management with coordination of vehicles departing and arriving at camp/office, and the management of visitors. • Quick Reaction Force (QRF) (if allocated) specific to Contractor	

Table 4: Security Response Level: Yellow- Enhanced Security Measures Required

Security Response Level: Yellow **Enhanced Security Measures Required**	
Event Indicator	**Recommended Action(s)**
Increased level of disturbance and/or increased probability of impact to operations. Sporadic civil disorder events (such as inter-ethnic cattle rustling/raids) common in the Karamoja Region in the UCSAT project. A direct threat has been detected to one or more areas of the operation but it is not considered imminent. • 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 works.	**Project operations continue. Enhanced security controls and operational restrictions required:** • Necessary communications equipment Satellite Phones / Very Small Aperture Terminal & Very high frequency radio calls (SATPHONES/VSAT/VHF) available and all systems checked. • Ensure site specific plans are available to the FRT and have been revised and practiced. • Ensure all security, crisis and evacuation plan representatives understand their roles and responsibilities. • Brief local security forces on roles and responsibilities and rules of engagement. Apply controls to ensure actions are tracked. • Review local security risks and controls; operating area Journey Management Plan- implements additional controls.

Security Response Level: Yellow **Enhanced Security Measures Required**	
Event Indicator	**Recommended Action(s)**

• Increase in inter-tribal and cross border violence adjacent to project area of operations or camp/office locations.
• Vehicle or aircraft movement is disrupted.
• Increased difficulty in accessing mission critical items or functions due to local security situation.
• Significant police or paramilitary deployment required to maintain rule of law; localized curfews in place.
• Heavy handed response from police and security service.
• Erosion of the support and good will of local communities.
• Difficulties in maintaining good relations with local authorities and traditional leaders.
• Livestock raids within close proximity of the field or office/camp locations
	• Maintain regular communication with all stakeholders, including authorities, local community, other sites and activities.
	• Daily call with OC Station.
	• If situation likely to continue, re-assess stocks of resources at operational sites and ability to re-supply (food / water / fuel / people).
	• Verify POB and carry out muster drills,
	• Assess requirements to increase physical security controls, access, perimeter protection, and road escorts.
	• Issue "Business Essential" travel advisory (If not already done).
	• All employees are briefed / updated on the security situation and controls- revise the evacuation plan.
	• Confirm all expatriates registered with appropriate embassy and all visas and passports valid.
	• Consideration given to recommending changes to the daily routine to include:
	  ○ identification of any out of bounds areas;
	  ○ local travel restrictions;
	• Review which business critical and sensitive documents need to be protected and how.

STANDARD OPERATING PROCEDURES	
These actions are in addition to the normal activities required at Security Status Green. Increased Actions are: <u>Police Foot Patrols:</u>	

Security Response Level: Yellow **Enhanced Security Measures Required**	
Event Indicator	**Recommended Action(s)**
Roles and responsibilities include: • Reinforce office/camp sites entries. • Conduct patrols around camp inner and exit gates. • Off office/camp personnel interrogation. <u>Centralized Mobile Police Patrols</u> <u>Armed Security Force</u> (ASF): **Quick Reaction Force** (QRF)4x Man armed team on standby within the office/camp on Notice to Move (NTM) States: **Daytime** - No change. But to include: ❖ Local area patrols should increase and cover the clearance patrol area of a radius of 300m from the office/camp perimeter. ❖ Clearance Patrols must be completed after any suspicious activity is noted or the offices/camp is stood to. ❖ **Night time** – As per normal daytime QRF with second pair at 2 minutes NTM. ❖ **Mobile Patrol** – location of the threat will dictate the exact patrol requirement. Options: ❖ 1 x patrol performing routine zone patrols or operating in a screening role. <u>Project Offices/Camp Sites:</u> • Check ID along with Issued Badge for all External workers whenever arriving. • All external contractor/vendor visits must have been notified to the Main Gate Reception in advance – no unexpected arrivals will be allowed at the entrance. As with Green all individuals and guests must be escorted by their host. • Implementation of restricted access areas. Areas such as the offices/camp site will be by authorised badge only. Access point to be physically controlled. • Lighting must cover all areas of the site to ensure guard force have clear visibility whilst conducting foot patrols. • Vehicle checks will go up to 25% of vehicles (10% comprehensive, 15% cursory).	

Security Response Level: Yellow **Enhanced Security Measures Required**	
Event Indicator	**Recommended Action(s)**
• Quick Reaction Force (QRF) (specific to Contractor) • **Isolated Locations** Consider increasing security at isolated locations and field operations.	

Table 5: Security Response Level: Orange-Increased Security Measures

Security Response Level: Orange **Implementation of Increased Security Controls and Preparation for Lock Down and/or Site Evacuation**	
Event Indicator	**Recommended Actions**
Significant obstacle or direct threat has been detected to operations and is deemed imminent, or a security incident has taken place close to one of the project sites: • Wide spread civil unrest, cattle raids and/or ethnic clashes, and disarmament exercise not contained by police or paramilitary forces. • Frequent acts of violence close to project operations. • UCSAT project activities specifically threatened and/or targeted. • Reinforcement of police by military forces to enforce martial law and impose curfews in key areas. • Substantial political or inter-tribal violence • Government ordered curfew in place • Law and order become fragile, shortages of food/water/supplies/power/communication outages. • Failure to observe security restrictions regarded as life-threatening. • Loss of support and good will of majority of local community, • Liaison with authorities and traditional leaders breaks down	**Project operations are suspended. Significant increase in security controls and operational restrictions. All movement outside project offices/ camps ceases.** • All external movement ceases • Twice daily call schedule with Client Security Manager • Ensure sites including plant, machinery and equipment are secured – security protection in place. • Consider further increase in security controls including; further reinforcement of security guarding, (police/army support) and asset hardening of critical equipment and safe havens. • Briefings to local security forces on roles and responsibilities- liaison with local commanders increased. • Consider resupply requirements for all locations and caretaker maintenance and security of unmanned locations. • Instigate evacuation drills and brief all staff on actions • Pack grab bags and ensure POB and documentation is available

	• Prepare vehicles for possible road moves and ensure thorough rehearsals have been conducted for any moves under escort.

STANDARD OPERATING PROCEDURES

These actions are in addition to the normal activities operating at Security Status Yellow. Increased Actions:

Police Foot Patrols:

- Reinforce Project Office/Camp main gate and Emergency Exits security.
- Conduct thorough searches on the arrivals.
- Ensure all gates within the Offices/camp/s are padlocked.
- Intensify inner perimeter patrols.

Centralized Mobile Police Patrols

- Inner perimeter fence 360 area check.
- Ready to react to emergency.
- Main gate and Emergency Exit manning.
- Should be ready for escort tasks.
- Questioning strangers or suspicious persons or vehicles.
- Developing hearts and minds assurance.

Project Offices/Base Camp Sites:

- Amber checks as standard but now there will also be cross checks at individual's place of work.
- Essential visitors only are given access.
- Vendors and local contractors must be escorted at all times, even when moving vehicles to a site of work.
- All vehicles will have complete cargo manifest checked against cargo on entry and exit.
- 100% of vehicles to have a cursory vehicle check.
- Exit Vehicle checks must consist of 25% comprehensive vehicle searches.
- Local area patrols should increase and cover the clearance patrol area at a radius of 300m from the office/camp perimeter.

- Increased internal and external patrols – for extended periods this will require an increase in manpower.
- Static guards to be paired.
- Armed guards to operate in support of main gate.
- Physical placement of chicane and main gate entry obstacles to stop forced access.

For a site to operate at Status Orange for more than a short period, the physical security measures below must be implemented and fitted:

- Key locations must have physical deterrent measures such as bars fitted to windows.
- Guard Force unarmed and armed to be supplemented.
- Improvements to be made to the number and quality of the work force safe muster areas.
- Further integration with state police and military forces – wider area patrolling and vehicle check points.

Table 6: Security Response Level: Red-Cease Operations, Lock down & Evacuation

Security Response Level: RED **Cease Operations and Lock Down or Evacuate Site**	
Event Indicator	**Recommended Actions**
The operation has experienced a direct attack or there is credible evidence of an imminent attack. • Direct threats against project operations • Major civil disorder in areas of operation • Lines of supply untenable (road closures / security risks) • Total collapse of law and order • Diplomatic missions advise nationals to leave. • No or limited local security forces protection	**Suspension of operations and/or activation of total lock down or evacuation plan:** • Confirm operational plan and nomination of alternative managers or key points of contact during evacuation. • Implement evacuation plan • Ensure adequate caretaker security in place if full operations are suspended. • Ensure all critical or sensitive documents have been collected and are readies for destruction or removal • Detailed briefing of all remaining personnel on situation and emergency response plans.

Security Response Level: RED **Cease Operations and Lock Down or Evacuate Site**	
• Security force reaction may damage reputation • Major difficulties in accessing basic necessities • Frequent power and communications disruption.	• Provide ongoing communications, guidance and assistance to local and security staff remaining in country • Finalize plans for remote management of operations if full evacuation is implemented.

STANDARD OPERATING PROCEDURES

These actions apply to ensure the project area and offices/camps are locked down to maintain the security of the core staff, whilst the UCSAT project Incident Management Team decides on the final course of action. Increased Actions:

Police Foot Patrols:

- Main gate Sentry reinforcement.
- Intensify inner perimeter patrols.
- POB confirmation.
- Conducting thorough searches at the main gate.
- Ensure all exits are padlocked.
- Reporting suspicious activities to the control room.

Centralized Mobile Police Patrols:

- Inner perimeter fence 360 area check.
- Ready to react to emergency.
- Main gate and Emergency Exit manning.
- Should be ready for escort tasks.
- Questioning strangers or suspicious persons or vehicles.
- Developing hearts and minds assurance.

Project Offices/ Camp Sites:

- Main gate and all access routes closed and secured with vehicle entry prevention devices. This is in addition to vehicle tyre spikes.

Security Response Level: RED Cease Operations and Lock Down or Evacuate Site
• No access allowed unless authorised by security management. If authorised Red measures apply and all vehicles are searched comprehensively. • No vehicle is authorised to move in or out of the perimeter unless directed by the security advisor. • Static guards reinforced by armed police or military if available. All perimeter patrols and main gate to operate with an armed presence as well as the unarmed guard. • Wider patrolling only as situation requires, as this should be done with coordination of any military presence. • Perimeter is secured so internal and external patrols are stopped to provide manpower to reinforce the perimeter security. • Internal security patrols to ensure direct observation on the perimeter at all times.

2.1 Alert State Status Boards

Alert State boards are to be displayed at the camp/ project offices and indicate the current security alert state and associated movement restrictions in the project area. Movement restrictions are to be covered in Journey Management Plan.

2.2 Site Security Layers

All project facilities will undergo the following security layers/protocols.

i. Physical security (guards).
ii. Access control system.
iii. Intelligence Network.
iv. Security induction.
v. Awareness.
vi. Trainings.

These different security layers together reduce the risk of having one system being by-passed. They are implemented by the Security commanders.

Physical Security

Physical security will involve the use of security barriers, such as fences, gates, locks, guard posts, surveillance/electronic security systems used, and the overall security management system at all the project premises.

Security barriers

These will mainly comprise of fences, gates, guard posts, surveillance / electronic cameras which will be manned by trained personnel who shall document and record daily incidents at the various points and provide reports to their superiors for appropriate action. Personnel shall maintain a daily register of persons, vehicles accessing the project area or facilities.

Security operating Procedures

This shall entail some of the key security operating procedures which will comprise of:

a. ***Boundary security:*** Security will maintain control of the project's perimeter by deploying personnel at strategic points along the boundaries of the project facilities and also channel people to access-control points that will have security personnel (both armed and unarmed as well as those in uniform and non-uniformed personnel);

b. ***Access Control Policy and Procedures:*** Access to project sites will by project personnel and visitors will be through a formal, documented access control procedures to facilitate the implementation of access control policy and associated access controls. MAAIF personnel will be issued with badges and will at all times carry and display these badges when in the field. The badges will enable the bearer to access project facilities upon site security enquiry. Visitor badges will be issued to all visitors who are not employees of MAAIF;

c. ***Unexpected/Unplanned Visitors:*** In case of unexpected (unplanned) visitors, the Project Administrator will be notified immediately by the security officers, access endorsement/authorization will be issued only by the Project Administrator after consultation with the Project Coordinator, and thereafter a visitor's badge will be issued. The visit should not exceed few hours and they must be accompanied by the project personnel /staff in charge of the visit at all times.

d. ***Visitor Badge Process:*** Visitor's badge will be issued after the visitor has been authorised by the site security managers. The visitor will then fill a visitor form providing all his details and purpose of the visit. A badge will then be processed and issued by the Access control office. Security induction must be done before the badge is issued to the applicant by Security officer and the visitor must sign on the induction document for acknowledgement. A data file with information regarding the visitor will be recorded and kept in the site access register.

e. ***Luggage search:*** A search of personal luggage will be performed by the guards at the access control point to ensure no access of all the prohibited items into the project facilities like: - Alcoholic Beverages, Firearms, knives and dangerous drugs are not smuggled onto project facilities.

f. ***Vehicle Access Control Procedures:*** All Vehicles accessing project facilities will be accessed through with the driver only after going through a security check/search for prohibited items i.e. Alcohol Beverages, Firearms, Knives and dangerous drugs. The driver must declare his entire luggage at the main gate (Personal luggage) for checking as well.

g. ***Materials Storage and Control:*** *w*here applicable, the project will institute controls over the transport, inventory, and maintenance of storage areas for raw materials, equipment, etc. Note that these are stored in accordance with appropriate Ugandan national laws and regulations and relevant good international industry practice, including the World Bank Group Environmental, Health and Safety Guidelines.

h. ***Information and Communication:*** The project will detail procedures for categorizing, handling, and controlling sensitive information.

i. ***Firearms Security:*** The project will develop a policy regarding firearms on-site, as well as the responsibilities and procedures for issuing and storing any security firearms, ammunition, and non-lethal weapons. This shall include: location for storage; how weapons are properly secured during storage; records for issuance; who they may be issued to; safeguarding while in possession of the personnel; and audits.

j. ***Special Situations:*** There may be instances where large-scale events (e.g., criminal activity, demonstrations, civil disorder, cattle rustling/raids, etc) require interventions by public security which is not specifically associated with the project. When planning for such events or emergencies, there shall be clarity on how project security passes control over to formal public security (for example, police, military, emergency responders in line with the National Police Service procedures.

3 SECURITY SUPERVISION AND CONTROL

The project will have a clearly defined management structure and responsibility, including overall lines of control, accountability, and supervision for the security effort. In making such arrangements, the project will be guided by the principles of proportionality and GIIP, and by applicable law, in relation to hiring, rules of conduct, training, equipping, and monitoring of such security workers.

All incidents including thefts, attempted, attempted break-ins must be reported to the Project Administrator and recorded in the occurrence book. The project administrator will initiate an investigation to determine sequence of events, what may have contributed to the incident, probable cause(s), contributing factors), , corrective actions, and mitigation measures (based on investigative findings). An incident report will be issued to the National Project Coordinator with details of the above actions.

Depending on the security incident, the National Project Coordinator will decide as to whether there is need to inform external agencies such as UPF of the security incident. Project organization will require security personnel to manage security aspects.

3.1 Security Organisation

All security activities are supervised and coordinated by the Project Administrator on behalf of the National Project Coordinator (NPC).

All security communication ranging from instructions, responsibilities to reporting security breaches will follow hierarchy of command from Security organisation to NPC to project vice-versa as the case may be**.**

District Project Focal Point person is responsible for overseeing operations within or around the project area including the security of any persons or property therein.

Security Team / Officers will be appointed to oversee all security activities for project sites (offices, storage and lay down areas, work sites, field transportation and day to day operations). They will supervise all project security activities and report directly to the NPC or through the district Project Focal person.

All project personnel are required to be aware of the need for constant vigilance, care and compliance with security procedures, as well as the necessity to report any incident or suspicion to the Project Administrator.

Public Security Personnel: Security personnel, the police/army will be deployed to provide security to all project sites and facilities overseen by Project Administrator. Security personnel, police/army officers have been trained on the following specific topics; securing project sites, patrols, communication, management of crowds/ riots with in accordance with principles of proportionality and GIIP, rules of conduct, use of radio call units, Quick intervention and access control procedures.

They are professional with a very good appearance and good English and Swahili command in terms of spoken and written. Their roles and responsibilities are detailed below;

- To Implement the Standard Operating Procedures properly without fear or discrimination;
- To ensure respect of the access control procedures and make sure that they are applied to all project personnel;
- Perform interior Patrols days and nights to ensure that the national borders are intact or no intruders within the project facilities;
- Check the border status on a regular basis using back tracking security method;
- To report any security incident to the guard posts or security commanders;
- Maintain constant communication with the control room on hourly basis while on duty;
- Report to the control room in case of any technical issues;
- Ensure a proper behaviour at all time while applying the SOP; avoid exchanging of words with the project staff.

3.2 Journey Management

The National Project Coordinator has the overarching responsibility for project-wide journey management. This is delegated to the District Chief Administrative Officer who will monitor all staff in and while in the field through the journey management system in collaboration with the District Project Focal Persons. A journey management log with clear vehicle movement orders will be monitored and maintained by the Project Administrator.

Project staff will be required to complete a Journey Management Plan form, which has to be authorised by the NPC. All staff will be required to inform the Project Administrator on arrival and departure to update the journey movement log/register.

Journey management will require periodic contact via radio or telephone in order to monitor the location of personnel.

3.3 Alarms

Alarms (Hand winding and electric sirens) for emergencies are to be held at the Project Administrator or site manager's office or site contractor's office. All security related incidents shall be document in the Security Log Event on **Error! Reference source not found.**.

Table 7: Security Occurrence Book/Log Matrix

Security Log Event.			
DATE	TIME	INCIDENT	Event Logger: Name +Signature
TIME	**DEVELOPMENT/ACTIONS TAKEN**		

3.4 Security Grievance Mechanism

To extent possible, the SMP shall adopt the Project Grievance Redress Mechanism in managing the security related grievances. The NPC shall engage the relevant project personnel to ensure security personnel grievances are included in the Project GRM and Stakeholder Engagement Plan, and work with public security leaders to integrate the project GRM with internal procedures.

Key areas of emphasis will be on the following steps:
Step 1: Publicizing Grievance Management Procedures,
Step 2: Receiving and Keeping Track of grievances,
Step 3: Reviewing and Investigating grievances,
Step 4: Developing Resolution Options and Preparing a Response,
Step 5: Monitoring, Reporting, and Evaluating a Grievance Redress Mechanism, and
Step 6: Dedication of adequate resources both human and capital.

Grievances related to the security team shall adhere to the Police Force Act and other related security legislations.