

**Republic of Kenya**

**Information Communication Technology Authority (ICTA)**

**Kenya Digital Economy Acceleration Project**

**SECURITY MANAGEMENT PLAN (SMP)**

**August 2023**

# TABLE OF CONTENTS

Table of Contents

[TABLE OF CONTENTS ii](#_Toc141694112)

[LIST OF TABLES iii](#_Toc141694113)

[ABBREVIATIONS & ACRONYMS iv](#_Toc141694114)

[Acknowledgement v](#_Toc141694115)

[1 INTRODUCTION 1](#_Toc141694116)

[1.1 Objective of the Security Management Plan (SMP) 1](#_Toc141694117)

[1.2 Security Approach 1](#_Toc141694118)

[2 STANDARDS AND GOOD INTERNATIONAL INDUSTRY PRACTICE 1](#_Toc141694119)

[3 OVERVIEW OF THE SECURITY SITUATION 2](#_Toc141694120)

[3.1 Security Risk Categories 2](#_Toc141694121)

[3.2 Security Risk Assessment (SRA) 3](#_Toc141694122)

[3.2.1 Social Conflicts and Civil Unrest 10](#_Toc141694123)

[3.2.2 Criminal Offenses 10](#_Toc141694124)

[3.2.3 Terrorism 10](#_Toc141694125)

[3.2.4 Cattle Rustling 10](#_Toc141694126)

[3.2.5 Armed Attacks and Kidnappings 11](#_Toc141694127)

[3.2.6 SEAH 11](#_Toc141694128)

[4 SECURITY RISK MANAGEMENT AND CONTROL 11](#_Toc141694129)

[4.1 Physical Security 11](#_Toc141694130)

[4.1.1 Communications 11](#_Toc141694131)

[4.1.2 Construction Security 11](#_Toc141694132)

[4.1.3 Fencing and Gates 11](#_Toc141694133)

[4.1.4 Exterior Lighting 12](#_Toc141694134)

[4.2 Security Operating Procedures 12](#_Toc141694135)

[4.2.1 Security Guards 12](#_Toc141694136)

[4.2.2 Law Enforcement Support 12](#_Toc141694137)

[4.3 Managing Public Security personnel 13](#_Toc141694138)

[4.3.1 Overview 13](#_Toc141694139)

[4.3.2 Public Security Deployment Risks 14](#_Toc141694140)

[4.3.3 Reporting Police Abuses 14](#_Toc141694141)

[5 SECURITY SUPERVISION AND CONTROL 15](#_Toc141694142)

[5.1 Security Management Committee (SMC) 15](#_Toc141694143)

[5.2 Security Management Chain of Command 15](#_Toc141694144)

[5.3 Responsibility for Conducting Security Risk Assessments 15](#_Toc141694145)

[5.4 Incident Reporting and Disclosure 15](#_Toc141694146)

[5.5 Community Engagement and Grievance Redressing Mechanism 17](#_Toc141694147)

[5.5.1 Security Grievance Redress Mechanism (GRM) and Procedure 17](#_Toc141694148)

[5.5.2 Special Procedures to Address Issues Related to GBV/SEAH 17](#_Toc141694149)

[6 BASIC PRINCIPLES ON THE USE OF FORCE AND FIREARMS BY LAW ENFORCEMENT OFFICIALS 18](#_Toc141694150)

[7 BUDGET AND RESOURCES FOR SMP IMPLEMENTATION 18](#_Toc141694151)

# LIST OF TABLES

[Table 3‑1 Security Risk Level Determination Matrix 3](#_Toc141694373)

[Table 3‑2 Security Risk Level Findings, Mitigation and Contingent Actions 4](#_Toc141694374)

[Table 3‑3 Situation Analysis Matrix for the security within some of the project counties 8](#_Toc141694375)

[Table 4‑1 Link between Level of Risk and Level of Public Security Deployment 13](#_Toc141694376)

[Table 7‑1 Implementation Budget for the Security Management Plan 19](#_Toc141694377)

# ABBREVIATIONS & ACRONYMS

CERC Contingent Emergency Response Component

EHS Environmental, Health and Safety

ESS Environmental and Social Standard

GBV Gender Based Violence

GIIP Good International Industry Practice

GRC Grievance Redress Committee

GRM Grievance Redress Mechanism

IAU Internal Affairs Unit

ICTA Information Communication Technology Authority

KDEAP Kenya Digital Economy Acceleration Project

KDF Kenya Defense Forces

LMP Labour Management Procedure

MICDE Ministry of Information Communication Technology and Digital Economy

NPS National Police Service

OCS Officer Commanding Station

OHS Occupational Health and Safety

PAPs Project Affected Persons

PIU Project Implementation Unit

SEAH Sexual Exploitation, Abuse and Harassment

SMC Security Management Committee

SRA Security Risk Assessment

WBG World Bank Group

# ACKNOWLEDGEMENT

The Security Management Plan (SMP) for the project, Kenya Digital Acceleration Project (KDEAP) was prepared by Ambuya John of Earthcare Services Limited, with the support of the KDEAP proponents, Information Communication Technology Authority (ICTA) and the Ministry of Information Communication Technology and Digital Economy (MICDE) of the Government of Kenya. We appreciate the input and comments from officers at ICTA, MICDE, and the World Bank.

# INTRODUCTION

## Objective of the Security Management Plan (SMP)

The objective of this SMP is to provide and maintain a safe physical environment and manage staff activities to reduce the risk of personal injury and asset loss during the implementation of Kenya Digital Economy Acceleration Project (KDEAP). The plan describes how security will be organized to face identified threats and how reassessment and reorganization in response to emerging security situations will be undertaken.

KDEAP aims to expand access to high-speed internet, improve the quality and delivery of education and selected government services, and build skills for the regional digital economy. KDEAP comprises five components: Component 1: Digital Infrastructure and Access; Component 2: Digital Government and Services; Component 3: Digital Skills and Markets**;** Component 4: Project Management;and Component 5: Contingent Emergency Response Component (CERC)**.**

This SMP covers sub-component activities for components 1, 2, 3 and 4 that may present occupational health and safety (OHS) risks to security personnel.

## Security Approach

Project Implementation Unit (PIU) Coordinator will ensure that security procedures and criteria are fully designed and updated, and the means fully available to ensure the security for project operations.

The PIU will leverage existing national and local security infrastructure to access and share conflict related information and encourage local police leaders to specifically address conflict risks in community engagement activities in a timely manner.

The use of private security personnel is preferred for subprojects. Local public security may be engaged on ad hoc basis depending on the level of security threat.

# STANDARDS AND GOOD INTERNATIONAL INDUSTRY PRACTICE

This SMP is anchored on:

1. World Bank Group (WBG) Environmental and Social Standard 1 (ESS1) on assessment and management of environmental and social risks and impacts – Clause 28(b) “the environmental and social assessment, informed by the scoping of the issues, will take into account all relevant environmental and social risks and impacts of the project, including: ... threats to human security through the escalation of personal, communal or inter-state conflict, crime or violence ...”;
2. WBG Environmental and Social Standard 4 (ESS4) on Community Health and Safety sub-section (B) on Personnel Security;
3. WBG General Environmental, Health and Safety (EHS) Guidelines;
4. Good Practice Note on Assessing and Managing Risks and Impacts of the Use of Security; and
5. the Guidelines for Implementation of the UN Basic Principles on the Use of Force and Firearms by law Enforcement Officials.

The standard role of public security agencies will be to maintain the rule of law, including safeguarding human rights and deterring acts that threaten the project personnel and facilities. The public security agencies to be deployed when needed shall be competent, appropriate, and proportional to the threat. Government of Kenya security on the Project is expected to comply with:

* WBG Good Practice Note on Assessing and Managing Risks and Impacts of the Use of Security Personnel, 2018;
* 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;
* The Penal Code, 2016;
* Prevention of Terrorism Act, 2012;
* Prevention of Organized Crime Act, 2012;
* Counter-Trafficking in Persons Act, 2010;
* Independent Policing Oversight Act, 2011;
* Kenya Police Service, Service Delivery Charter, 2015;
* The Universal Declaration of Human Rights, 1948;
* National Police Service Act, 2014;
* Private Security Regulation Act, 2016; and
* The National Government Coordination Act, 2013;

The management of security 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; and
* **RESPOND** to the adversary’s actions.

# OVERVIEW OF THE SECURITY SITUATION

## Security Risk Categories

Different security risks exist in Kenya and may impact the Project, whether new or changing. The risks must be communicated without delay through the relevant designated officers at national, county and community levels and be recorded as identified security risks in the security log. The security risks can be categorized into:

1. **Internal Risks** may include but not limited to illegal, unethical, or inappropriate behavior of project personnel or those directly affiliated with it, such as employee theft, workplace violence, and labor unrest, potentially with associated sabotage). Other risks include the risks emanating from security personnel and associated arrangements; and
2. **External Risks** caused by the actions of people outside the project who seek to take advantage of opportunities presented by the implementation 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, banditry, inter/intra community conflicts, armed insurgency, coups, or war.

The main security risks in Kenya include:

1. Criminal offences;
2. Terrorism;
3. Cattle rustling/inter-tribal or communal violence which could pose a threat to project personnel;
4. Industrial action leading to strike or disruption of work, social conflict, civil unrest;
5. Breakdown of relationships with community groups and committees;
6. Reaction of community to an incident or accident involving project personnel or asset;
7. Threat of armed attack;
8. Theft/ Larceny;
9. Kidnapping;
10. SEAH/GBV; and
11. Occupational health and safety (OHS) risks for security personnel at construction sites.

## Security Risk Assessment (SRA)

The project will adopt 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 and how, with an evaluation of any security hazards undertaken, this will determine the control measures needed to prevent or minimize the potential security risks.

The SRAs will be commissioned by either the PIU or the public or private network operators (such as Telkom Kenya, KETC, KPLC, Safaricom, Liquid Telecom, etc.). The SRA findings will be used to develop site specific SMPs and feed into the method statements. The public or private network operators shall submit their SMPs as part of method statements to PIU for review and approval.

An impact and likelihood risk matrix has been adopted to determine the security risk level.

Table 3‑1 shows the three security risk levels (Low, Medium, and High) and how they are determined based on likelihood and consequences/sensitivity. Likelihood and consequence values range from 1 to 4 as follows; very low=1, low=2, medium=3, or high=4. Security risk level is determined by multiplying the sensitivity and likelihood values for each identified risk.

Table 3‑1 Security Risk Level Determination Matrix

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Risk Level** | | **Consequence** | | | |
| C1 | C2 | C3 | C4 |
| **Likelihood** | L1 | 1 Low | 2 Low | 3 Low | 4 Medium |
| L2 | 2 Low | 4 Medium | 6 Medium | 8 Medium |
| L3 | 3 Low | 6 Medium | 9 High | 12 High |
| L4 | 4 Medium | 8 Medium | 12 High | 16 High |

Table 3‑2 Security Risk Level Findings, Mitigation and Contingent Actions

| Risk description | Risk Category | | | Responsibility | Mitigation | Contingent action | Useful resources |
| --- | --- | --- | --- | --- | --- | --- | --- |
| L | C | R |
| Criminal offences  Theft/Larceny | L2 | C1 | M | PIU  Contractor | Use of physical security personnel e.g., unarmed guards, etc.  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 material storage areas. | Escalate to the Kenya Police  Undertake joint risk assessment process including representatives of public security forces in use  Maintain close contact with representatives of public security forces at different levels | VPSHR toolkit  [https://www.miga.org/sites/default/files/archive/Documents/VPSHR\_Toolkit\_v3.pdf](http://?) |
| Terrorism | L4 | C4 | H | PIU  Contractor | Enhance inter/intra agency cooperation within the project area.  Meet on regular basis with the security apparatus at the sub-county and county level  Assess the security situation and make changes to the security management plan  Ensure travelling project staff have NPS 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[[1]](#footnote-1). | Conduct effective risk analysis assessments, and SWOT analyses and Force-Field Analyses related to gaps and needs assessments. | VPSHR toolkit  [https://www.miga.org/sites/default/files/archive/Documents/VPSHR\_Toolkit\_v3.pdf](http://?) |
| Cattle rustling | L1 | C1 | M | PIU  Contractor | Initiate peace building process among the affected communities  Use traditional institutions in creating peace, security, law and order in community policing and conflict management.  Carry out civic education by use of the local CSOs.  Offer vocational and technical skills to the youths and or initiate income generating project to engage youths. | Strengthening of surveillance within the County boundaries and develop protocols for cross border use  Initiate “List of Shame” among the politicians and prominent pastoralists who incite youth to engage in cattle rustling |  |
| Armed attack/ Kidnapping | L3 | C4 | H | PIU  Contractor | Use of physical security personnel  Conduct project 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 storage areas | 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.  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. | VPSHR toolkit  [https://www.miga.org/sites/default/files/archive/Documents/VPSHR\_Toolkit\_v3.pdf](http://?) |
| Industrial action | L1 | C4 | M | PIU  Contractor | Adhere to all provisions in the Project Labour Management Procedure (LMP)  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. | KDEAP’s LMP |
| Hostility | L1 | C4 | M | PIU  Contractor | Adhere to all provisions in the Project Stakeholder Engagement Plan (SEP) | Set some ground rules within the community groups, and  Revisit the group’s purpose. | KDEAP’s SEP |
| SEA/GBV, and incident response | L1 | C1 | L | PIU  Contractor | Adhere to all provisions in the Project Grievance Redress Mechanism (GRM)  Abide by the requirements of SEA/GBV Action Plan for the project being prepared | Continuous SEA/GBV awareness creation the hired firm. | KDEAP’s GRM in SEP and LMP  KDEAP’s SEA/GBV Action Plan |
| OHS Risks for Construction Sites Security Personnel (Not rated) | | | | | | | |
| Slips, trips, and falls |  |  |  | PIU  Contractor | Conduct site assessments to identify dangers/hazards.  Conduct site-specific training to make security personnel familiar with the site.  Clear communication of expectations is important to injury prevention.  Conduct health and safety training  Barricade and/or use warning tape to mark off hazardous areas and prevent people and vehicles from going into those areas.  Regularly inspect sites for ground instability.  Inspect ladders before climbing. Never climb on a shaky ladder or a ladder with slippery rungs.  Conduct routine worksite safety inspections for hazards that can arise from changing conditions (weather, soil conditions, construction activity, and so on).  Work with site safety personnel to make sure that the environment is made as safe as possible for the personnel who must patrol the site after hours. | Include OHS for security personnel requirement in all contracts with NPS, security companies and partner telcos. | WBG EHS Guidelines  WBG ESF  Online resources on security personnel OHS risks and management |
| Assaults |  |  |  | PIU  Contractor | Equip security personnel with personal protective equipment (PPE), lone worker safety devices e.g., handheld satellite devices, etc., as well as accessible communication devices to increase their safety, particularly those working alone, during late hours.  Learn techniques for dealing with violent behavior. |  |  |
| Contact with objects/animals |  |  |  | PIU  Contractor | Use services of an expert dog trainer; verify that all the dogs have mouth muzzles. |  |  |
| Transportation accidents |  |  |  | PIU  Contractor | Ensure vehicles are properly maintained and regularly serviced.  Ensure vehicles are loaded safely and correctly, as overloading or improper loading can cause accidents.  Provide PPE e.g., gloves and safety glasses, etc., and enforce usage.  Ensure personnel handling materials are trained to handle them safely and that the materials are packaged and labeled correctly. |  |  |
| Overexertion |  |  |  | PIU  Contractor | Clear communication of expectations is important to injury prevention e.g., Include lifting requirements in job descriptions.  Identify overexertion risks.  Provide lifting aids or use safe lifting techniques e.g., lift knees instead of lower back, etc.  Prohibit solo lifting of heavy loads.  Require frequent short breaks.  Encourage early reporting of overexertion injuries.  Conduct health and safety training |  |  |
| Exposure to harmful substances or environment. |  |  |  | PIU  Contractor | Conduct regular checks and proper storage according to the temperature requirements of the chemical or substance.  Conduct health and safety training |  |  |

Situation Analysis Matrix for the security within some of the project counties is shown in Table 3‑3.

Table 3‑3 Situation Analysis Matrix for the security within some of the project counties

| **#** | **SECURITY THREATS PROJECT / COUNTIES** | **Criminal offences** | **Theft/ Larceny** | **Terrorism** | **Cattle rustling** | **Armed attack / Kidnapping** | **Industrial Action** | **Community Hostility** | **SEAH, and incident response** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Kitui | Medium | Medium | Medium | Low | Medium | Low | Low | Medium |
|  | Machakos | Low | Medium | Medium | Low | Medium | Low | Low | Medium |
|  | Migori | Medium | Low | Medium | Low | Medium | Low | Low | Medium |
|  | Makueni | Medium | Low | Medium | Low | Medium | Low | Low | Medium |
|  | Bomet | Medium | Low | Medium | Low | Medium | Low | Low | Medium |
|  | Embu | Medium | Low | Medium | Low | Medium | Low | Low | Medium |
|  | Meru | Medium | Low | Medium | Low | Medium | Low | Low | Medium |
|  | Homa Bay | Medium | Low | Medium | Low | Medium | Low | Medium | Medium |
|  | Kiambu | Medium | Low | Medium | Low | Medium | Low | Medium | Medium |
|  | Kilifi | Medium | Low | Medium | Low | Medium | Low | Medium | Medium |
|  | Muranga | Medium | Low | Medium | Low | Medium | Low | Medium | Medium |
|  | Kisii | Medium | Low | Medium | Low | Medium | Low | Medium | Medium |
|  | Kakamega | Medium | Low | Medium | Low | Medium | Low | Medium | Medium |
|  | Taita Taveta | Medium | Low | Medium | Low | Medium | Low | Medium | Medium |
|  | Nakuru | Medium | Low | Medium | Low | Medium | Low | Medium | Medium |
|  | Nandi | Medium | Low | Medium | Low | Medium | Low | Medium | Medium |
|  | Narok | Medium | Low | Medium | Low | Medium | Low | Medium | Medium |
|  | Nyandarua | Medium | Low | Medium | Low | Medium | Low | Medium | Medium |
|  | Busia | Medium | Low | Medium | Low | Medium | Low | Medium | Medium |
|  | Transnzoia | Medium | Low | Medium | Low | Medium | Low | Medium | Medium |
|  | Uasin Gishu | Medium | Low | Medium | Low | Medium | Low | Medium | Medium |
|  | Tana River | Medium | Low | Medium | Low | Medium | Low | Medium | Medium |
|  | Nyeri | Medium | Low | Medium | Low | Medium | Low | Medium | Medium |
|  | Kakamega | Medium | Low | Medium | Low | Medium | Low | Medium | Medium |
|  | Kirinyaga | Medium | Low | Medium | Low | Medium | Low | Medium | Medium |
|  | Kwale | Medium | Low | Medium | Low | Medium | Low | Medium | Medium |
|  | Mandera | Medium | Low | High | High | High | Low | Medium | Medium |
|  | Marsabit | Medium | Low | High | High | High | Low | Medium | Medium |
|  | Wajir | Medium | Low | High | High | High | Low | Medium | Medium |
|  | Garissa | Medium | Low | High | High | High | Low | Medium | Medium |
|  | Tharaka Nithi | Medium | Low | Medium | High | High | Low | Medium | Medium |
|  | Isiolo | Medium | Low | Medium | High | High | Low | Medium | Medium |
|  | Samburu | Medium | Low | Medium | High | High | Low | Medium | Medium |
|  | Baringo | Medium | Low | Medium | High | High | Low | Medium | Medium |
|  | Turkana | Medium | Low | High | High | High | Low | Medium | Medium |
|  | West Pokot | Medium | Low | Medium | High | High | Low | Medium | Medium |
|  | Elgeyo Marakwet | Medium | Low | Medium | High | High | Low | Medium | Medium |

In counties with low-risk security threat, the Project could consider using private unarmed security personnel. Due diligence involving background checks can be undertaken to ensure that only those from reputable security firms are engaged. The unarmed security personnel can 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.

### Social Conflicts and Civil Unrest

The main risk in the local communities who presume to have been aggrieved that can easily and quickly mobilize for a demonstration. Inadequate compensation, and environmental and social concerns can create this kind of scenario. The crowds 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 project contractor security manager to the local police officers and complaints may be made to the officer-in-charge of a Police Station [Officer Commanding Station (OCS)] and be recorded in an occurrence book for future reference. The threat should in turn be communicated to the Sub-county Police Commander at the sub-County level and to the County Police Commander using the existing public security channels.

National, county, and local workers could also demonstrate, if there is a perceived discrimination and unfair working conditions in terms of wages, overtime, and welfare. It is PIU’s responsibility to ensure that working conditions for all workers/employees are in line with the national legal framework.

### Criminal Offenses

The main risk remains small scale thefts of light equipment, fuel and personal effects which can involve aggressions. To mitigate this risk, materials storage and control, equipment, etc. will be according to the national laws and regulations and relevant good international industry practice (GIIP), including the WBG EHS Guidelines.

### Terrorism

There is the ever-imminent threat of terrorism from the lawless Al-Shabab from neighbouring Somalia in the northern counties that could pose a serious threat to the implementation of the KDEAP activities. As such, the project stakeholders will be on high alert to avoid incidences of infiltration of the terrorists into the project areas. The stakeholders will also be sensitised to report any situations that may indicate signs of an attack from the terrorist groups. Al-Shabaab militants are suspected to attack telecommunication masts in Mandera County to deter communication[[2]](#footnote-2).

### Cattle Rustling

Nomadic pastoralists in Northern Kenya are also known to be armed with light arms, these could pose a security risk to Project workers and the smooth implementation of the Project in the area, especially if incidents of cattle rustling occur. This occurrence could increase conflict between communities.

### Armed Attacks and Kidnappings

The project stakeholders may be exposed to this risk where the project personnel will be expected to carry huge sums of money or valuable items. The stakeholders will be sensitised to use cashless transactions as much as possible. Where risks may be high, the armed security teams may be called upon to provide escort to the destinations.

### SEAH

The risk of SEAH in the project activities/operations is expected to be medium and all stakeholders especially the girls and women will be sensitised on how to avoid such incidences and the correct steps to take and channels to use to report in case they face the are affected. The project GRM will also have a dedicated channel to handle SEAH incidents.

# SECURITY RISK MANAGEMENT AND CONTROL

## Physical Security

As indicated in [Section 3.2](#_Security_Risk_Assessment), all public or private network operators involved in project implementation will be required to develop site/subproject specific SMP. The subproject SMPs should capture the specific site potential risks and assess the specific physical security, internal and external security risks and shall be submitted to the PIU for review and approval as part of the method statements.

### Communications

Communications with employees and contractors will be critical to ensuring a safe work environment during construction of the project. Selected employees’ supervisors working on the site and contractor who is working at the Project will be required to carry a two-way radio. Cell phone coverage may be limited in some project area, so alternative forms of communication will be needed. The two-way radios supplied to employees and contractors will be capable of:

* Providing immediate emergency instruction to personnel; and
* Notifying proper personnel of a security incident.

PIU will work closely with contractor and security consultant to develop a program to ensuring proper communications during construction, including identification of procedures and equipment for summoning emergency assistance from local authorities.

### Construction Security

To reduce security risks during construction, public access to the subproject sites will be limited. The contractor will be required to prepare a subproject SMP for construction phase. Preparation of the final site security plan will begin immediately following selection of the contractor within mobilization period and the final plan will be provided to the PIU and WBG.

### Fencing and Gates

Fencing is the first layer of security for any contractor camp, deep holes, machinery locations, quarry and borrow it sites, and other dangerous areas with standardized on above 2m fencing, using tension wire in lieu of bars, placing fence barbs up, and securing the bottom of the fencing below grade. Access points/gates are secured through one of the following methods: Manually opened and secured with heavy-duty approved padlock, electronically accessed with card credential, or electronically accessed with remote gate fob. All essential perimeters and access points of the road will be monitored 24/7 by CCTV or contracted security guards during construction and operation phases of the project.

### Exterior Lighting

Exterior lighting can be used in addition to fencing to emphasize and highlight perimeters, gate and guard post access points, entry points into buildings, and areas of interest.

## Security Operating Procedures

### Security Guards

The contractors will employ experienced security guards from the local community in collaboration with local administrators for the technical help during employment process. Guards maybe stationed at the contractor’s camps, if any and where project machineries are parked. Additionally, "patrol" guards maybe assigned to conduct security checks of the contractor's properties. Furthermore, after giving the guards with specific training on potential security and other OHS risks at construction sites, and risk mitigation and emergency response measures, they will perform the following activities:

* **Boundary Security:** the security guard will maintain control of the camps, storage areas and machineries’, if any, boundary and protect people from accessing except authorized persons through erecting-control points; and
* **Access-Point Operations:** the security guards will check and screen anybody get into the camps and facility sites, if any. If somebody armed firearms with the recognition of government and asked to get into the camp, the guard will ask the person to submit the firearm with his/her identification card to the guard and receive guest permission card to enter. Similarly, vehicles will be checked and screened in the same manner at the entrance gate.
* **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.

### Law Enforcement Support

ICTA will develop strong partnerships with the law enforcement agencies in the country. These agencies will support ICTA secure the installed broadband infrastructure, observation patrols and respond to incidents during proposed project implementation.

* **Security Patrols:** police in each county/sub-county in will patrol the subproject sites to check and supervise the security situation of the sites.
* **Materials Storage and Control**: where 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 national laws and regulations and relevant GIIP, including the World Bank Group Environmental, Health and Safety Guidelines.
* **Decision tree model**: the project security shall adopt a structured approach using the collaborative approach for all the armed security operatives in prioritizing the collection of relevant data during incident response. The structured tree model approach helps to define how questions are answered, allows the incident response team to respond consistently with predictable results. The structured approach also provides for definable, reproducible structures to be created facilitating controlled cost exposure during an incident response cycle.
* **Information and Communication:** information gathering organizing and dissemination will be handled by the cooperation work of local/ward, subcounty, county, regional and national level security officials. Ward level security official will have closely relation with the contactor’s security management official to categorize, handle, and control sensitive information. Then, ward level security officials will communicate with higher level security officials e.g., subcounty, county, regional, and national level, etc., to handle sensitive security issues immediately before it poses any damage on the human life and contractor’s asset. Again, the project will detail procedures for categorizing, handling, and controlling sensitive information.

## Managing Public Security personnel

### Overview

Interaction with public security forces can be the most challenging aspect of security management for private companies such as contractor and/ or consultants as they do not have power to control their decisions or behaviour. This issue often arises when government security personnel are deployed to provide security services related to projects implemented by private companies, such as construction of key infrastructure developments. Public security may also be assigned to provide regular or temporary support to a local community where the project implementation takes place, but not be involved in protecting the specific project on a regular basis. Public security forces involvement in site security emanates from contractor request due to a perceived increase in security threat level at subproject site.

The contractors generally encouraged to rely first on private security forces to solve site security problems, whenever possible, and to not think of public security forces as a replacement for private security forces. To meet the principles of ESS4, the contractor should review any existing codes of conduct of private security companies before hiring. If the public security forces are used. The contractors will lose control if public security forces are engaged and take the lead; however, public security forces have broader roles and responsibilities, and may be appropriate in certain situations, as indicated in Table 4‑1. The type, strength, training, and equipment of security forces should be proportionate and appropriate to the threats, risks and tasks.

Table 4‑1 Link between Level of Risk and Level of Public Security Deployment

| Level of Risk | Level of Public Security Deployment |
| --- | --- |
| Low-level risk | On-call law enforcement from off-site  General law enforcement  Guard the potential area that could be affected by hazardous materials and support public safety response personnel (e.g., fire extinguishing crews, etc.) access the area and perform their work without concern of security risks.  Patrol security |
| Medium-level risk | Nearby or on-site security backup  Immediately available to handle protests or civil disturbance  Armed convoy security  Close personal protection |
| High-level risk | Dedicated & heavy on-site security as protection from armed groups  Perimeter security  Defensive patrols outside the perimeter |

### Public Security Deployment Risks

Even though the responsibility to enforce law and order lies with government, and the contractor is not directly responsible for the actions of public security personnel, the company may be associated with these actions in the eyes of local communities and other stakeholders. The actions of public security forces can pose a significant reputational risk and can increase tensions with the local population. Consequently, in situations where public forces are responding to incidents related to the project, the contractor has an obligation of conducting detailed risk assessment on the deployment of public security personnel. Public security personnel may pose the following risks on the local community if deployed to provide security on the project.

* **Human Right Abuse –** Public security forces may violate human right of the local community through illegal use of force, intimidation and harassments;
* **Gender based violence (GBV) –** Similar public security personnel may commit gender-based violence such as sexual abuse, sexual harassment, early marriage and rape on women and girls at subproject sites. The GRM indicated in the LMP and the GBV action plan will apply for addressing the GBV cases of security personnel.

### Reporting Police Abuses

The reporting mechanisms include: using of the emails: [incidents@ke-cirt.go.ke](http://?), [info@dcicpu.co.ke](http://?), [nps@nationalpolice.go.ke](http://?), and the toll free numbers: call 116, 112, 911, and 999.

In cases where it is reporting against the security teams (Police), the documented channels of receiving complaints at National Police Service Internal Affairs Unit (IAU) are:

1. Visiting the nearest police stations
2. Through letters P.O Box 1880 -00200 Nairobi
3. Through-email: [iau@nationalpolice.go.ke](http://?)
4. Social media – Twitter - @NPSOfficial-KE
5. Anonymous Reporting Information System (ARIS) USSD \*683#, SMS 40683, Toll Free Line 0800721230, Mobile App ARIS, NPS, & Web Form [www.iau.go.ke](http://?)
6. Mobile +254 798474619
7. WhatsApp (Videos and Pictures) 0758729917, and
8. Through the media.

# SECURITY SUPERVISION AND CONTROL

The ICTA/PIU bears the overall responsibility for security risks and risk mitigation. The PIU takes final decisions on security-related issues in consultation with the responsible stakeholders like the contractors and community members. To manage the proposed KDEAP security issues, all project stakeholders must know their role and responsibility and play pivotal role for the success of the project. Hence, Figure 6‑1 shows organogram for the practical implementation of this SMP.

## Security Management Committee (SMC)

SMC composed of KDEAP’s project coordinator, a security consultant recruited by PIU, Project manager from contractor (on ad hoc basis), representative from MICDE, representative from NPS and Ministry of Defence (for subprojects in border counties), will be established to follow up the security issues during project implementation.

Other security bodies listed Figure 5‑1 will be communicated by the SMC and information will be exchanged for the successful security safeguarding of the project.

## Security Management Chain of Command

The security management chain of command will follow both (i) top to bottom for the response and (ii) bottom to top for information sharing as indicated in the organogram in the Figure 6-1. Therefore, the top management for the security management of KDEAP will be the SMC, while the MICDE will monitor the practical implementation of the SMP. Other stakeholders indicated in the organogram such as Ministry of Defence – Kenya Defence Forces (KDF) and NPS will receive command from the SMC and then they will pass command to the regional level; the regional level respective security organ will pass the command to County levels and then to local security (ward level) bodies for keeping and protecting the workforce of the project.

## Responsibility for Conducting Security Risk Assessments

Security risk assessment (SRA) is important to identify potential risks and device appropriate risk management plan. Therefore, it is the responsibility of the contractor to assess security risks at the subproject site and submit to the PIU. Additionally, the PIU will perform its own security risk evaluation as owners of the project.

## Incident Reporting and Disclosure

It is the responsibility of the contractor to record and report monthly any incident to PIU except for fatalities and other serious incidents causing bodily harm to workers and others connected to the Project which must be reported within 24 hours of occurrence. Similarly, the SMC will report weekly, monthly and quarterly to PIU the security situation and status of the project. Furthermore, the security situation of the project will be disclosed as required to the local community and interested third party such as WBG. Fatalities will be reported to WBG within 24 hours of occurrence by the PIU.

Figure 5‑1 SMP Implementation Organogram

## Community Engagement and Grievance Redressing Mechanism

As noted in the SEP, PIU will devise community engagement and grievance redressing mechanism to engage with community members on matters related to security risks.

### Security Grievance Redress Mechanism (GRM) and Procedure

The GRM established for the project will serve for settling complaints related to security personnel. In compliance with the WBG’s ESS10 requirement, a specific grievance mechanism, as indicated in the SEP, will be set- up for the project. The main objective of a GRM is to respond to concerns and grievances of project-affected parties related to the environmental and social (E&S) performance of the project as well as complaints on the security personnel/use of security forces in a timely, effective and efficient manner. Dedicated communication materials (e.g., GRM pamphlets, posters, etc.) will be created to help local communities familiarize themselves with the grievance redress channels and procedures. A GRM guideline will also be produced for subprojects that ensures opportunities for the affected community to settle and solve their complaints and grievances amicably. To capture and track grievances received under the project, a dedicated grievance redress committee (GRC) will be established for each subproject. It will also provide information on the way the GRC works, both in terms of procedure and deadlines to settle the raised compliant respecting to the project. GRC composition will vary depending on local situations and project affected persons (PAPs). The local administration will be responsible for establishing the GRCs while PIU will play has a facilitating role.

GRM assures PAPs that they will be provided with the appropriate remedy including issues related with security personnel. It provides opportunity for PAPs to settle their complaints and grievances amicably. The procedure allows PAPs not to lose their time and resources from going through lengthy administrative and legal procedures. Additionally, in accordance with ESS2, the project will establish a worker grievance mechanism (WGM), to enable all direct workers and contracted workers to raise workplace concerns, including in relation to workplace sexual harassment and security.

PIU’s environmental and social safeguards specialists will implement the GRM to ensure that it is responsive to any concerns and complaints particularly from affected stakeholders and communities. Again, the GRM will ensure that the Contractor and other implementers of the project are responsive to any concerns and complaints particularly from affected stakeholders and communities regarding security personnel. The steps indicated in the SEP GRM, the timeline, grievance registering and lodging, monitoring and reporting system will be applicable for security personnel.

### Special Procedures to Address Issues Related to GBV/SEAH

For the GRM to effectively address the grievances on security personnel related to sexual exploitation and other forms of gender-based violence, the project in general and the subproject level GRC must set proactive mechanism functional throughout the project cycle. In this regard, the NPS Children and Women Desks at the County level will be the focal person on issues related with sexual exploitation and other forms of gender-based violence. The GBV assessment report for the project shows that an effective GRM with multiple, confidential and safe channels to initiate a complaint, investigate and redress cases that are safe, confidential, non-segmental and effective is required to be established. Strengthen GRC with training, hiring GBV expert on ad hoc basis, and support to ensure safe and confidential reporting, investigation, and remedial action to mitigate cases of GBV/SEA are mandatory.

# BASIC PRINCIPLES ON THE USE OF FORCE AND FIREARMS BY LAW ENFORCEMENT OFFICIALS

The project has adopted the basic principles from the guidelines for implementation of the UN basic principles on the use of force and firearms by law enforcement officials to promote the proper role of law enforcement officials will consider and must be respected by project implementers within the framework of Kenya national legislation and practice and shall be brought to the attention of law enforcement officials as well as other project persons. The adopted principles include:

1. ICTA and appointed law enforcement agency (National Police service) shall adopt and implement rules and regulations on the use of force and firearms against persons by law enforcement officials;
2. ICTA and the law enforcement agency shall develop a range of means as broad as possible and equip law enforcement officials with various types of weapons and ammunition that would allow for a differentiated use of force and firearms;
3. The use and deployment of non-lethal incapacitating weapons shall be carefully evaluated to minimize the risk of endangering uninvolved persons;
4. Law enforcement officials, in carrying out their duty, shall, as far as possible, apply non-violent means before resorting to the use of force and firearms. They may use force and firearms only if other means remain ineffective or without any promise of achieving the intended result;
5. Whenever the lawful use of force and firearms is unavoidable, law enforcement officials shall:
   1. Exercise restraint in such use and act in proportion to the seriousness of the offence and the legitimate objective to be achieved;
   2. Minimize damage and injury, and respect and preserve human life;
   3. Ensure that assistance and medical aid are rendered to any injured or affected persons at the earliest possible moment; and
   4. Ensure that relatives or close friends of the injured or affected person are notified at the earliest possible moment.
6. Where injury or death is caused using force and firearms by law enforcement officials, they shall report the incident promptly to their superiors. A detailed report shall be sent promptly to the Internal Affairs Unit for responsible administrative review and judicial control;
7. ICTA shall ensure that arbitrary or abusive use of force and firearms by law enforcement officials is punished as a criminal offence in line with National Police Service Internal Affairs Unit and the Independent Policing Oversight Authority;
8. Exceptional circumstances such as internal political instability or any other public emergency may not be invoked to justify any departure from these basic principles;
9. The law enforcement agency shall ensure that all law enforcement officials are selected by proper screening procedures, have appropriate moral, psychological and physical qualities for the effective exercise of their functions and receive continuous professional training; and
10. ICTA and the law enforcement agency(ies) shall undertake the policing of unlawful assemblies, policing persons in custody or detention in line with the provision of the UN basic principles on the use of force and firearms by law enforcement officials, 2016.

# BUDGET AND RESOURCES FOR SMP IMPLEMENTATION

Table 7‑1 below presents budget source and estimated cost for the implementation of SMP. Detailed costs will be included when the contractors prepare their site-specific SMPs. The requirement to be prepare the site-specific plans will also be reflected in the contract/bidding documents.

Table 7‑1 Implementation Budget for the Security Management Plan

| No. | Security Management Issue | Detailed Tasks | Budget Source | Estimated Cost |
| --- | --- | --- | --- | --- |
|  | Provision of Physical Security | Two-way radio communication between selected employees and the Contractor  Cost for preparation of SMP by the Contractor.  Provision of Fencing using tension wire in lieu of bars and gates and monitoring 24/7 by CCTV or Security guards at the camp sites, machinery locations quarry and borrow sites.  Provision of Exterior lighting to emphasize and highlight perimeters, gate and Guard Post access points, entry points into buildings, and areas of interest. | Contractor (for e.g., multi-agency, public and private network operators, and PPP, etc.) | The cost will be prepared when contractors prepare their site specific SMPs. |
|  | Security Operations | Employment of experienced security guards from the local community. | Contractor | Contractor is responsible for payment of the monthly salary of security guards/security agencies and per diems for local security officials for their technical assistance |
|  | Law Enforcement Support | Local police in each county assigned to patrol the subproject sites whenever necessary. Besides, the Contractor can request for additional forces to be assigned conditionally. | NPS and Contractor | The budget for the local police forces will be handled by the NPS (No separate budget is required). However, if the local police are assigned upon the request of the Contractor, he/she shall cover the expenses including daily per diems for the security personnel. |
| Hazardous Materials Storage and Control | NPS and Contractor | The Contractor is responsible for paying a per diem for the local police who guard and supervise the utilization of the hazardous materials. |
| Management of Large-scale events such as criminal activity, demonstrations, civil disorder and/ or border conflicts which is not specifically associated with the project. | GOK Security Apparatus (Kenya Defense Forces and NPS) in collaboration with the security guards of the Contractor | GOK is responsible for covering any costs related to securing the subproject areas. |
| Human Right Abuse and Gender based violence (GBV) management. | NPS | GOK, under each law enforcement levels are responsible for covering any costs related to enforcing the law. |
|  | Capacity Building for law enforcement personnel and workers. | Capacity building for security Personnel deployed and workers on what one should do in case of gunshots, grenades, kidnapping, assault, etc.  Health and safety training. | Contractor | The cost will be prepared when contractors prepare their site specific SMPs. |

1. [Good Practices in the Area of Border Security and Management in the Context of Counterterrorism and Stemming the Flow of “Foreign Terrorist Fighters”](http://?) [↑](#footnote-ref-1)
2. See [https://nation.africa/kenya/counties/mandera/suspected-shabaab-telecommunications-mast-3255916](http://?) [↑](#footnote-ref-2)