**COUNTRY: KENYA**

**PROJECT: KENYA DIGITAL ECONOMY ACCELERATION PROJECT (KDEAP)**

**IMPLEMENTING AGENCY: INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY (ICTA)**

**PROJECT ID: P170941; CREDIT NUMBERS 7289-KE AND 7290-KE**

# TERMS OF REFERENCE FOR:

# EXPRESSION OF INTEREST
# FOR

# CONSULTING SERVICES FOR PROJECT SECURITY LIAISON OFFICER
# (INDIVIDUAL CONSULTANT)

## CONTRACT NO: KE-ICTA- 553316-CS-INDV

## ISSUE DATE: 9TH JUNE 2026
## CLOSING DATE: 25TH JUNE 2026 AT 10:00AM EAT

**Client:**
The Chief Executive Officer,
ICT Authority
Telposta Towers 12th Floor, Kenyatta Ave
PO Box 27150 - 00100 Nairobi Kenya
Tel: +254 20 2089061/ 2211960 Fax: +254 20 2211960
Email: procurement@ict.go.ke, info@icta.go.ke
Website: www.icta.go.ke

## TERMS OF REFERENCE

## 1.0 INTRODUCTION

The Government of Kenya, through the Ministry of Information, Communications, and the Digital Economy (MICDE) and the ICT Authority (ICTA), is implementing the Kenya Digital Economy Acceleration Project (KDEAP), funded by a credit facility from the International Development Association (IDA). This project aims to expand access to high-speed internet, enhance digital government services, and strengthening Kenya's digital economy. As part of its implementation, there is a need to ensure the safety and security of project assets, personnel, infrastructure, and information systems.

To support this objective, the PIU seeks to engage a qualified Part-Time Security Consultant to provide expert advice, risk assessments, and oversight on security-related matters. In view of this the PIU intends to apply a portion of the credit for provision of Consulting Services for Project Security Liaison Officer (Individual Consultant) under component 4.

The project components are;

1. **Digital Infrastructure and Access** - This component, encompassing US$320 million, aims to create a robust digital backbone by boosting middle-mile connectivity and last-mile access, particularly in education. The intention is to connect key public institutions and enhance overall digital access for a population that is rapidly embracing technology.
2. **Digital Government and Services** - With a budget of US$104 million, this component focuses on automating essential government services to facilitate a transition to a paperless framework. Efforts will prioritize enhancing service delivery and employing user-centric design for better public access to online services.
3. **Digital Skills and Markets** - Allocating US$51 million, KDEAP seeks to equip young people with digital competencies through targeted programs in formal and vocational education, preparing them for competitive roles in the digital economy. This includes a commitment to the National Digital Skills Program, which aims to cultivate 10,000 high-end ICT professionals by 2030.
4. **Project Management** - A budget of US$15 million is dedicated to guiding the strategic implementation of the KDEAP, ensuring effective stakeholder engagement and project monitoring through a specialized Project Implementation Unit based at the Ministry of Information, Communications, and the Digital Economy (MICDE).

5. **Contingent Emergency Response Component** - Though initially unfunded, this component offers the flexibility to respond to emergencies, aligning with the global trend of integrating disaster resilience into large-scale projects.

## 2.0 OBJECTIVES

The primary objective of this consultancy is to enhance the overall security framework of KDEAP by identifying risks, recommending mitigation measures, and supporting the implementation of effective security strategies. This will enhance the capacity of PIU to manage security risks associated with the implementation of activities under KDEAP across the country.

## 3.0 SCOPE OF CONSULTING SERVICES

### 3.1 General Requirements

The Consultant shall perform all work herein described and provide all resources as required to attain the objectives given above. The Consultant shall perform his duties in accordance with accepted professional standards. In the conduct of this work, the Consultant shall cooperate fully with government officials who will provide the data and services as outlined herein section 6; the Consultant shall be solely responsible, however for the analysis and interpretation of all data received and for the conclusions and recommendations contained in its reports.

### 3.2 Consultancy Services

The anticipated Consultant's services shall include, but not necessarily be limited to the following:
Overall

- Identify vulnerabilities and potential threats (physical and operational).
- Develop risk profiles and prioritize mitigation measures.
- **Support KDEAP officers and contractors** in ensuring **security awareness, prevention, and mitigation of existing and emerging security risks** in the course of the project.
- Support the implementation of the Security Management Plan for the Project as a member and the lead of the KDEAP Security Team.
- Provide **clear communication and coordination** between all implementing agencies and security agencies in matters of security during the project period.
- **Assist in ensuring compliance** with laws of Kenya and World Bank's safeguarding standards in security management through monitoring and reporting.

Specifically:

**a) Site-Specific Security Management Planning**
The Security Liaison Officer will advise the PIU and all project contractors in line with the overall KDEAP Security Risk Assessment and Security Management Plan, through conducting site-specific security risks assessments and management plans along the project implementation areas. This includes but not limited to:

- Proposing appropriate emergency communication systems
- Assessing and monitoring the use, management and maintenance of the project facilities and resources allocated to the security agencies.
- Support journey management planning, making sure that security aspects are mainstreamed in route selection (involving movement of vehicles and equipment).
- Establishing and maintaining physical barriers, fencing, and controlled access measures at project worksites and field offices to support site security

**b) Security Risk Information Gathering and Assessment**
The Security Liaison Officer will:

- Gather information and intelligence relevant for understanding and assessing security risks facing the project. This activity will build on the KDEAP Security Risk Assessment and Security Management Plan.
- Manage the collection, analysis, and dissemination of security related information;
- Ensure that the site-specific security assessments and management plans are relevant and constantly updated as appropriate and that all staff know their roles and responsibilities;
- Liaise and participate in meeting with county security focal points
- Based on the security information gathered, advise the resident engineer on working schedule of work/journey management plans.

**c) Communication**
The Security Liaison Officer will:

- Liaise closely with the National Police service and other security entities;
- Provide detailed daily/weekly and monthly surety intelligence briefing to the contractors and PIU. Submit daily/weekly/monthly intelligence briefing concerning recent incidents and trends. The information should be specific and applicable to the project area

- Provide necessary security-related information to communities and their representatives
- Ensure always to maintain a solid communication with staff, security teams and other stakeholders and value any information, even based on rumors and pass to responsible authority. The Security Liaison Officer will provide any other assistance related to the above as may be requested.

**d) Preemptive Security Risk Management Services**

The Security Liaison Officer will be required to;

- Provide detailed instructions on precautions and emergency procedures that should be taken;
- Coordinate emergency response, crisis management plans related to KDEAP;
- Work with contractors to prepare site specific emergency response plan which will include the -transportation, evacuation and exit routes
- Liaise and work with GoK security teams in developing detailed security and evacuation plans;
- Monitor implementation of KDEAP and PIU security plans and physical protection guidelines as well as fire and safety guidelines;
- Issue guidelines and advise on residential accommodations conduct, undertake periodic security awareness meetings; and schedule appropriate drills to test and strengthen incident response procedures.

**e) Security Incident Management**

The Security Liaison Officer will:

- Support ICTA and contractors in reporting, investigating and resolving security related incidents and accidents related to the project and all security grievances reported to the contractors and third parties where applicable.
- Provide directions on coordination and implementation of all security incident response procedures and guidelines consistent with the KDEAP requirements;
- Lead root cause analysis for all security-related incidents and oversee the implementation of corrective actions; and undertake identification of lessons learnt after all incidents.

## 4.0 DURATION & LOCATION OF ASSIGNMENT

The Project area covers the entire country with a particular focus on counties with security challenges. This assignment will be focusing on security advisory and ensuring project activities are undertaken with all necessary security measures and protocols taken care off. The consultant may be required to travel where the KDEAP projects will be undertaken to assess and support project personnel.
It is envisaged that the Consultant's Services will be for an initial term of **twelve (12) months** from the contract commencement date.
The Contract may be extended for up to 12 months at a time, not exceeding a total contract duration of 48 months (initial 12 months plus up to 36 months of extension), subject to the following conditions:

1. Ongoing project needs requiring continued security liaison services
2. Satisfactory performance of the Individual Consultant
3. Availability of funds
4. Mutual Agreement between ICTA and the Individual Consultant

ICTA will initiate any extension by communicating, in writing, the intention to extend the contract at least 60 days before the current contract period ends. Extensions will be formalized through a written addendum to the original contract.
A comprehensive performance review will be conducted prior to any extension to evaluate the Individual Consultant's effectiveness in meeting the project's security objectives.

## 5.0 REPORTING DELIVERABLES AND TIME SCHEDULE

The minimum reports required under this assignment are described in the preceding sections and tabulated below. The Individual Consultant shall additionally prepare any other reports required to adequately and professionally discharge the assignment**.**

The types of reports are:-

| **Report Type** | **Timelines after Contract Commencement Date** | **Format and No. of Copies** |
|---|---|---|
| Inception Report | 2 weeks | |
| Monthly Report | Within 5 days of the following month | |

| | | |
|---|---|---|
| Quarterly Report | Within 15 days at the end of every quarter | Three (3) hard copies and an electronic version (soft copy) in flash disks |
| Ad Hoc Report | As and when need arises | |
| Annual Security Review Report | Within 30 days of the completion of each year of the Individual Consultant's contract period | |
| Final Report | Within 30 days of the completion of the consultancy assignment | |

**Reporting Requirements**

The Consultant shall report to the Project Coordinator, (PC) on all matters pertaining to this contract. The Consultant shall prepare and submit three (3) hard copies and an electronic version (soft copy) of the following reports at the beginning of the assignment. The electronic version (soft copies) shall be in two versions; a searchable, colour pdf version (in one single file) and editable versions of the component sections of the report (i.e. in formats compatible with MS Word, MS Excel, MS Project etc).

**(i) Inception report**

The inception report shall contain a detailed schedule of work, Methodology, etc. and Inception Workshop to discuss with Client (2 weeks after contract signing)
The Consultant shall prepare the following reports as the project is on-going:

**(ii) Quarterly report**

The Quarterly Report will contain an assessment of Implementation of the KDEAP Security Risk Assessment and Security Management Plan and recommendations. The quarterly report will be submitted within 15 days of the end of every quarter.
The content and format of the Quarterly progress report, which shall be as agreed with the Project Coordinator and will include but not limited to the following:

a) Details of activities undertaken during the Quarter, site visits, meetings etc
b) Details and status of security installations and manpower under the project,
c) List / document of any security incidences reported on site through a security log
d) Update on the security situation in the surrounding area
e) Details of any new security plans created or changes to security plans.

f) Training activities undertaken and also any new people for whom training is pending but not yet done
g) Analysis of security response to incidences
h) Analysis of Implementation of the KDEAP Security Risk Assessment and Security Management Plan
i) Recommendations for improving security risks management

### (iii) Ad Hoc Reports

The Individual Consultant may be required to produce ad hoc reports on specific security issues or incidents as they arise during the course of the assignment. These reports should be timely, factual, and include clear recommendations for action. Ad hoc reports shall include, but not be limited to, the following:

**a) Incident Reports**

- To be submitted within 24 hours of any significant security incident
- Detailed description of the incident, including date, time, location, and parties involved
- Immediate actions taken in response to the incident
- Preliminary assessment of the root causes and impacts of incidents on project operations and staff safety
- Recommendations for further actions or preventive measures

**b) Threat Analysis Reports**

- To be submitted when new or evolving security threats are identified
- Analysis of the nature and severity of the threat
- Potential impact on the project and stakeholders
- Recommended mitigation strategies and adjustments to security protocols

**c) Special Security Assessment Reports**

- To be produced upon request from ICTA or when significant changes occur in the security landscape
- In-depth analysis of specific security aspects or areas of concern
- Evaluation of current security measures related to the area of focus
- Detailed recommendations for addressing identified issues or enhancing security measures

**d) Emergency Response Evaluation Reports**

- To be submitted following any activation of emergency response protocols
- Review of the effectiveness of emergency response procedures
- Analysis of coordination with relevant security agencies and stakeholders during the emergency
- Lessons learned and recommendations for improving emergency response capabilities

The format and length of ad hoc reports may vary depending on the nature and urgency of the
situation. However, all ad hoc reports should include:

- Clear and concise executive summary
- Detailed analysis of the situation or issue
- Evidence-based findings
- Specific, actionable recommendations
- Relevant supporting documentation or data

Ad hoc reports shall be submitted in electronic format via email to designated ICTA officials, with hard copies to follow if required. The Individual Consultant shall maintain a log of all ad hoc reports submitted, which should be included as an appendix in the proceeding quarterly report.

**(iv) Annual Security Review Report**

The Individual Consultant shall prepare an Annual Security Review Report to provide a comprehensive overview of the security situation and management for the KDEAP in Country. This report shall be submitted within 30 days of the completion of each year of the Individual Consultant's contract period. The report shall include, but not be limited to, the following:

**a) A holistic review of the year's security situation and management**
- Comprehensive assessment of the security environment in the project area
- Evaluation of the implementation and effectiveness of the Security Management Plan
- Analysis of major security incidents and their impact on project operations

**b) Long-term security trends analysis**
- Identification and analysis of significant security trends affecting the project
- Comparison with previous years' data (where available)
- Projections of potential future security scenarios based on observed trends

**c) Effectiveness of the overall security strategy**
- Assessment of the success of implemented security measures

- Evaluation of coordination efforts with security agencies and stakeholders
- Analysis of the impact of security management on project progress and community relations

**d) Major achievements and challenges**

- Highlight of key security management successes over the past year
- Discussion of significant security challenges faced and how they were addressed
- Lessons learned from both successes and challenges

***e)*** **Strategic recommendations for the coming year**

- Proposed enhancements or modifications to the Security Management Plan
- Suggestions for improving coordination with security agencies and stakeholders
- Recommendations for addressing identified security trends and challenge

The Individual Consultant shall submit three (3) hard copies and an electronic version (soft copy) of the reports in flash disk drives. The soft copies shall be in two versions; a searchable, color pdf version (in one single file) and editable versions of the component sections of the report (i.e. MS Word, Excel, MS Project, etc).

### (v) Final Report

Report at the end of the assignment (after 12 months) on the key issues dealt with and recommendations/interventions undertaken during the entire duration of the assignment.

The Final Report shall be submitted within 30 days of the completion of the consultancy assignment. The report should provide a comprehensive overview of the entire consultancy period, focusing on the overall impact of the security liaison role on the KDEAP across the country. The Final Report shall include, but not be limited to, the following:

**a) Overview of all security management activities conducted throughout the assignment**

- Comprehensive summary of major security initiatives and interventions implemented
- Review of the evolution of the Security Management Plan over the consultancy period

- Analysis of coordination efforts with security agencies, local administration, and communities

**b) Assessment of the overall effectiveness of security strategies implemented**

- Evaluation of the success of implemented security measures in mitigating risks
- Analysis of the impact of security management on project progress and stakeholder relations
- Review of the adaptability and responsiveness of security strategies to changing threats

**c) Key achievements, challenges, and lessons learned**

- Highlight of significant security management successes over the consultancy period
- Discussion of major security challenges faced and how they were addressed
- Documentation of key lessons learned and best practices identified

**d) Long-term recommendations for sustaining effective security management**

- Proposed enhancements to security policies, procedures, and resources
- Suggestions for aligning future security strategies with long-term project goals
- Recommendations for ongoing capacity development in security management

***e) Handover notes for continued security management after the assignment***

- Detailed guidance for the continuation of effective security practices
- Overview of ongoing security initiatives and pending matters
- Key contacts and resources for future security management

**Lateness in reporting:** Where a report required under any section of these Terms of Reference is delayed beyond the stipulated time for submission, the consultant shall provide to the Client an explanation satisfactory to the Client for the delay in submission and the remedial measures to be undertaken.;

## 6.0 PAYMENT SCHEDULE/REMUNERATION

The Security Liaison Officer shall be remunerated based on a consolidated monthly rate (inclusive of all tax obligations), which will be negotiated with the successful candidate during negotiations. Remuneration will be based on competitive rates, commensurate with the selected candidate's area of expertise and work experience, provided he or she has satisfactorily fulfilled all requirements stipulated herein above.

Payment shall be monthly upon submission and approval of the monthly reports. Costs incurred by the **Security Liaison Officer** outside the assignment location will be reimbursed upon submission of a statement of expense and verifiable supporting documentation to the KDEAP Project Coordinator.

**The payment schedule shall be as follows:**

- Monthly Payments: The Security Liaison Officer shall submit **to the Project Coordinator, a monthly timesheet, with a supporting invoice, as the basis for payment for the services** with a monthly report by the 5th day of the following month. Upon approval by ICTA, payment shall be made within 30 days of receipt of the invoice.

- Reimbursable Expenses: All reasonable, necessary, and pre-approved project-related expenses (such as travel costs) shall be reimbursed at cost upon submission of receipts and invoices. These expenses shall not exceed the agreed-upon budget without prior written approval from ICTA

The Security Liaison Officer shall maintain accurate records and evidence of all time spent and expenses incurred in providing the services. ICTA reserves the right to audit these records at any time during the contract period.

The monthly fee rate and any allowances or reimbursements shall be agreed upon between ICTA and the Individual Consultant prior to contract signing and shall remain fixed for the duration of the contract unless otherwise agreed in writing by both parties.

## 7.0 MINIMUM QUALIFICATIONS AND EXPERIENCE REQUIREMENT

### 7.1 Qualification Requirements.

- Minimum of a Bachelor's degree in Security Studies, Military science, Criminology, public administration or related field.
- The Security Liaison Officer will have a minimum of 7yrs work experience in security management sector with proven ability to work independently and under pressure in challenging and dynamic environments.
- Demonstrated 5 years experience working in security prone conditions and in crisis management including knowledge on IEDs, drones, and terrorism/radicalization.
- Proven track record in developing and implementing security management plans for large-scale infrastructure projects in high-risk areas.
- Certification in relevant security management courses (e.g., Certified Protection Professional) would be an added advantage

**Required Capabilities**

- In-depth understanding of national security policies and procedures in Kenya.
- Ability to work with different security agencies and government departments.
- Comprehensive knowledge of security risk assessment methodologies and mitigation strategies.
- Strong familiarity with international standards on human rights and best practices in security management.
- Excellent analytical and problem-solving skills, with the ability to make sound judgments in complex security situations.
- Strong leadership and team management capabilities.
- Excellent written and oral communication skills in English and Swahili;
- Excellent organization skills, attention to detail and ability to contribute to the team.
- Proficiency in using computer applications for security management, reporting, and data analysis.

The Security Liaison Officer must be prepared to travel frequently to security prone project implementation areas and occasionally to other project areas as required by the assignment.

## 8.0 MANAGEMENT AND ACCOUNTABILITY OF THE ASSIGNMENT

The ICTA will be the client for the services and the Client will be represented by the Chief Executive Officer (CEO). The KDEAP Project Coordinator of the KDEAP PIU will supervise the work of the Consultant, and shall be responsible for coordination of activities of the consultants. On a day-to-day work basis, the consultant shall work and report to the Project Coordinator.

## 9.0 RESPONSIBILITY OF THE CLIENT

The Client shall provide the KDEAP Security Risk Assessment and Security Management Plan and any relevant data on the project implementation and give all possible assistance as shall be reasonably requested for carrying out the services by the consultant. This includes requirement for confidentiality under the applicable laws in Kenya.

## 10.0 RESPONSIBILITY OF THE CONSULTANT

The Security Liaison Officer shall be responsible for carrying out their duties as outlined in their job descriptions, ensuring that all security related advisory tasks are performed in accordance with applicable laws, security protocols and World Bank safety requirements.

All official work-related travel and associated expenses shall be covered as per the applicable Government of Kenya (GoK) public service rates. Prior approval from the Project Coordinator is required for any official travel. ICTA shall provide the necessary tools, resources, and access to systems required for the execution of their roles. Security officer will be expected to maintain the highest standards of integrity, confidentiality, and accuracy in managing project security related matters.