TERMS OF REFERENCE

I. General information

Assignment name	Short term expertise for technical assistance in high-level technical and legal expertise to the Ministry of ICT and Digital Economy (MICDE) in the finalization of the draft National Cybersecurity Policy
Project Title	Strengthen the resilience of the cybersecurity ecosystem of Kenya (KCR)
Country	Kenya
Total estimated number of days	40 man-days

II. Context and justification of the need

The overall objective of the project is to support Kenya to strengthen the resilience of the cybersecurity ecosystem of Kenya to ensure that citizens enjoy an open, free, secure, gender responsive and peaceful cyberspace. This will enhance Kenya's overall defense mechanisms against cyber-threats thus help mitigate the risks of cyber-attacks targeting public and private sector entities and increase users trust. The project is designed to assist the beneficiary country, specifically Kenyan authorities and actors, in strengthening their cybersecurity capacities in all aspects. The project started on March 1st, 2025 and will end in late February 2027.

The specific objectives of the project are:

(I) The national cybersecurity regulatory and legal frameworks are improved

(II) The cybersecurity incidents management capacities are strengthened

(III) Users cybersecurity culture and capacities are increased

To reach the objective, the project is expected to achieve 3 Outcomes:

(I) Adoption and implementation of a coherent, holistic, gender responsive, strategic and actionable national approach to CyberResilience is facilitated;

(II) National operational capacities to adequately prevent, respond to, and recover from cyber-attacks and/or accidental failures are improved;

(III) Trust of users, organizations and companies in the use of the cyberspace is enhanced (from a human rights and gender perspectives).

The project started in March 2025, with an inception phase to get an overview of the situation in the country, to identify the needs and to propose the adapted activities in close coordination with the national authorities.

III. Objectives and desired results

1) General objective

The general objective is to provide high-level technical and legal expertise to the Ministry of ICT and Digital Economy (MICDE) in the finalization of the draft National Cybersecurity Policy, ensuring alignment with Kenya's existing digital transformation initiatives, the draft National Cybersecurity Strategy, and international best practices, particularly the EU NIS2 Directive principles.

2) Specific objectives

(I) To conduct a technical and legal review of the draft National Cybersecurity Policy to ensure internal consistency and alignment with national and regional frameworks.

(II) To assess the coherence of the draft policy with the National Cybersecurity Strategy, the Critical Infrastructure Protection Bill, and other relevant policies and legal instruments.

(III) To provide technical assistance to the MICDE technical working group (TWG) in preparing and conducting public participation and stakeholder consultations, in compliance with Kenya's 2024 Policy Development Guidelines.

(IV) To assist the MICDE in consolidating, analysing, and integrating public feedback into a final validated policy draft ready for Cabinet consideration.

(V) To provide strategic guidance and technical notes supporting the final stages of approval, up to Cabinet submission and potential gazettement.

3) Expected results

This short term expertise needs to provide strategic advices to the MICDE in close collaboration with the Project Team. The expected results following this short term expertise are:

- A technically sound, inclusive, and coherent draft National Cybersecurity Policy aligned with national and international standards is finalized.
- Coordination and ownership of the policy process among key Kenyan institutions are improved.
- Effective and well-documented public participation process is conducted according to Kenyan law.
- A final policy ready for Cabinet is ready for approved and published in the Kenya Gazette.

IV. Description of the assignement

1) Planned activities

The expert will be responsible for carrying out, under the supervision of the Project Team, all the necessary tasks needed to deliver the expected deliverables in accordance with best international recognized practices in the field. These tasks may include:

Phase 1 – Review and alignment

- Review the latest draft of the National Cybersecurity Policy and related documents.
- Map and assess coherence with national (e.g., National Cybersecurity Strategy, CIIP Bill, Data Protection Act, Digital Economy Blueprint) and regional/international frameworks (e.g., AU Convention, EAC, EU NIS2) and best practices.
- Identify gaps, overlaps, and inconsistencies, and provide annotated feedback and recommendations.
- Prepare an Inception Report summarizing approach, methodology and initial findings

Phase 2 – Support to public participation with a stakeholder consultation

- Advise and assist the TWG in developing the Public Participation Plan, ensuring compliance with Kenya's guidelines for the development of National Government Policy and Legislation (2024).
- Prepare or contribute to preparation of materials for public participation (summaries, briefing notes, online consultation guidance, validation templates).
- Where relevant and feasible, participate in stakeholder engagement meetings, provide facilitation support, and ensure proper documentation of feedback.

Phase 3 – Policy finalization and approval process

- Consolidate stakeholder input and support the revision of the final draft National Cybersecurity Policy.
- Prepare the cabinet memorandum and validation report and explanatory note in line with official processes.
- Provide guidance to MICDE for the submission of the final policy to the cabinet and its subsequent gazettement.
- Deliver a final technical report summarizing the review, process, and recommendations for next steps (if required).

2) Deliverables

Deliverables	End date
1. Inception report with annotated version of the draft National Cybersecurity Policy with comments and recommendations	T0 + 10 days
2. Mapping report showing policy coherence and alignment with existing national and regional/international frameworks and best practices	Deadline to be fixed with MICDE
3. Public participation plan and supporting documentation package (briefing materials, feedback templates, etc.)	Deadline to be fixed with MICDE
4. Consolidated summary report of stakeholder consultations and recommendations	Deadline to be fixed with MICDE
5. Revised final draft of the National Cybersecurity Policy	Deadline to be fixed with MICDE
6. Cabinet submission package: Cabinet Memorandum, Validation Report, and Explanatory Note	Deadline to be fixed with MICDE
7. Final mission report summarizing activities, outcomes, and recommendations	Deadline to be fixed with MICDE

3) Technical-methodological concept

The consultant shall provide a comprehensive approach covering:

- Analytical framework: Systematic policy review using benchmark criteria (legality, coherence, feasibility, inclusivity).
- Stakeholder management: Clear engagement strategy for government, private sector, civil society and academia.
- Knowledge management: Documenting lessons, providing templates and recommendations for future cybersecurity governance.
- Monitoring and reporting: Progress updates, milestone tracking and coordination meetings with MICDE and Expertise France.
- Gender and inclusion: Ensuring gender-responsive approaches and inclusion of marginalized groups.

- Sustainability: Integrating recommendations for policy implementation, capacity development and institutionalization.

4) Coordination

The expert will be reporting to the Project Manager.
A launch meeting shall be held few days after the contract has been notified.
Close collaboration must take place with the project team and the other experts from assignment preparation right up to completion. Furthermore, regular exchanges must take place with the Project Manager and the Key expert on assignment progress and any difficulties that may be encountered.

V. Place, duration and terms of performance

1) **Place:** Home based and/or in Nairobi, Kenya
2) **Implementation period:** November 2025 to March 2026
3) **Start date:** as soon as possible
4) **Effective duration per assignment:** 40 man-days
5) **Schedule/programme:**

The provisional programme for assignment implementation is as follows:

Activity	Place	Period	Duration (man/days)
Phase 1 – Review and Alignment	Home Based	TBC	10 days
Phase 2 – Support to Public Participation	Hybrid	TBC	20 days
Phase 3 – Policy Finalization and Approval Process	Hybrid	TBC	10 days
Total			**40 days**

VI. Required expertise and profile

1) **Number of experts per assignment:** 1

2) **Profile of the designated expert(s) responsible for contract execution**

(I) **Academic qualifications and experience:**

- At least Master's degree (or equivalent) in Information Security, Law, Public Administration, International Relations, Computer Science, or related field.
- At least 10 years of professional experience in cybersecurity governance, digital policy, or institutional reform, preferably with government or international organisations.
- Demonstrated experience in drafting, reviewing, or advising on national policies or strategies related to cybersecurity, digital transformation, or critical infrastructure protection.
- Solid understanding of Kenya's ICT and cybersecurity institutional and legal landscape (MICDE, NC4, CAK/KE-CIRT, ODPC, etc.).
- Understanding relevant legislation and policy coherence and regulatory alignment issues across government sectors.

- Familiarity with EU and international standards, including the EU NIS2 Directive, ENISA guidelines, and OECD/ITU cybersecurity frameworks.
- Experience in facilitating multi-stakeholder consultations and public participation processes, ideally within Kenyan or Commonwealth legal frameworks.

(II) Additional specific requirements:

- Excellent communication, and advisory skills for senior-level government engagement.
- Proven ability to produce high-quality reports, strategic papers, and legal-technical analyses.
- Ability to facilitate technical workshops and engage with diverse stakeholders (government, private sector, civil society).
- Demonstrated negotiating, cultural sensitivity and diplomatic skills.
- Proficiency in English (written and spoken) is mandatory. Working knowledge of French is an asset.

VII. Assignment reports

Please refer to the deliverables tab.
A report following the template provided must be forwarded by e-mail on conclusion of the assignment.

VIII. Practical information

Please send your CV in EU format and cover letter highlighting relevant domains of expertise to be considered in English.

NB: Candidates interested in this opportunity are invited to submit their application as soon as possible, with Expertise France reserving the possibility of pre-screening before that date.

Any incomplete application will not be considered.

Without a response from us within 3 weeks, please consider that your application has not been accepted.