REPUBLIC OF GHANA

MINISTRY OF COMMUNICATIONS & DIGITALISATION

GHANA DIGITAL ACCELERATION PROJECT (GDAP)

(IDA 70960-GH)

TERMS OF REFERENCE

FOR

CONSULTANCY SERVICES FOR DEVELOPMENT OF AN ICT AND SECURITY POLICY FOR DPC

May, 2024

1.0 INTRODUCTION

The World Bank is providing funding support to the Government of Ghana (GOG) for the implementation of the Ghana Digital Acceleration Project (GDAP). The overall development objective of the Project is to *expand access to broadband, enhance the efficiency and experience of selected digital public services, and strengthen the digital innovation ecosystem.* The Project aims to accelerate country-wide digital transformation in the public and private sectors, focusing on critical digital enablers and safeguards that promote the digital economy. The Project will further increase Ghana's capacity to promote digital innovation, digital skills development, and sector-wide digital transformation. The guiding principle for the Project is the strengthening of the local digital entrepreneurial and innovation ecosystem, by supporting start-ups that can help develop data-driven digital products and services. The Project has four components as follows:

Component 1 – Ensuring Inclusive and Safe Digital Transformation

This Component aims at supporting the GoG's continued efforts to build solid foundational building blocks for inclusive and safe digital transformation. Specifically, it aims to establish an enabling environment for the development of a vibrant and green broadband market, expand the reach and coverage of broadband networks in lagging areas, ensure safe and resilient digital services, and strengthen the digital transformation's institutional structure and capacity.

Component 2 – Modernizing Digital Government Services

This Component aims at establishing an agile and user-centric digital government model in Ghana. The activities are focused on building the next generation government infrastructure and delivering transactional and digital by design public services. This will be achieved by (i) developing a change management moving towards a Strengthened Digital Governance, (ii) expand the availability of high-quality transactional government e-services in key sectors, and (iii) support building the next generation of government workforce.

Component 3 – Support for Digital Transformation of Productive Strategic Sectors

This Component will strengthen the local digital entrepreneurship ecosystem and talent base. Activities financed will support better innovation ecosystem coordination, better service provision by Entrepreneur Support Organizations (ESOs), expand access to early-stage financing, and promote advanced digital innovation capabilities. Activities financed will leverage and complement the interventions proposed by also encouraging the use of new public dataset made available and public goods introduced, considering recommendations of the World Development Report (WDR) 2021 on Data for Better Lives. A strong local entrepreneurship ecosystem will also aide in developing locally relevant content and services that can help stimulate digital adoption and uptake of digital services. Furthermore, this Component will support the Agriculture Sector as a pilot to unlock the digital transformation of key productive sectors. The Component will also explore synergies and opportunities for cooperation with the *YouStart* Program that forms part of the GoG's strategy to facilitate jobs creation in the country via skills and capacity development and access to funding for young entrepreneurs.

Component 4 – **Project Management and Evaluation:** This component will finance project management activities including fiduciary responsibilities, procurement, communication, and dissemination, as well as monitoring and evaluation of project implementation and its impact.

2. Background

The Data protection Commission (DPC) is an independent statutory body established under the Data Protection Act, 2012 (Act 843) to protect the privacy of the individual and personal data by regulating the processing of information. The commission provides for the process to obtain, hold, use of disclose personal information and for other related issues bordering on the protection of personal data.

The mission of the commission is to protect the privacy of the individual and personal data by regulating the processing of personal information. The vision of the commission is to be recognized by all stakeholders as an independent, effective and efficient data protection regulator in the country and beyond.

Following the introduction of the Registration & compliance as a technology platform for use in compliance audit , registration, breaches and reporting of data controller/subjects/processors in Ghana, DPC recognises the need to put in place appropriate ICT policies to cover different aspects of technology use across the different functions and particularly to institutionalise the R&C usage. DPC now requires the services of a consultant to develop an ICT and security policy aligned to the mandate of the DPC as provided in the Act 2012 and with the operational usage of the R&C in DPC, data subject and data controllers/processors.

1. Objective of the Assignment

The objective of the assignment is to develop a DPC registration & compliance system ICT and security policy that takes into account of the existing systems and ability to take on board organizational and technological changes so as to guide the continued effective, efficient and responsible use of ICT within the DPC, in the implementation of the registration & compliance and integration with other systems that work with the DPC system.

2. Scope of the Services

The scope of services under this assignment will include the following:

i. Review the current ICT environment of DPC and determine the IT processes existing in line with the mandate and functions of DPC.
ii. Review the vision, mission, goals and targets of the Registration & Compliance ICT strategy contained in the DPC strategy and ensure that the DPC ICT policy adequately considers the activities and plans contained in the strategy.
iii. Review the Ghana ICT laws, policies and regulations and ensure that the DPC ICT policy is consistent with the national laws.
iv. Review specific ICT strategies, policies and procedures in place at the National IT Agency (NITA) and ensure that the development of the DPC ICT policy adequately addresses the interagency policies currently in place and/or planned.
v. Review ICT and security policies of other key agencies that have systems integrating with the system such as Ghana Revenue Authority, Bank of Ghana, Public Procurement

Authority etc. and ensure that there are adequate provisions to ensure policy consistency in the ICT environment at DPC.

vi. Prepare the ICT and security Policy of DPC which should cover but not be limited to the following:
   a. Access policies
   b. Application development and implementation policies
   c. Third party management policies
   d. ICT security policies
   e. Cyber Security Policies
   f. Interface and integration policies
   g. Application policies
   h. Network policies
   i. Disaster recovery and business continuity policies
   j. Support and maintenance policies
   k. Documentation
   l. ICT staff training
   m. Etc.

vii. Prepare forms that are required for operationalization of the DPC ICT and security policy such as access approval forms, third party access forms, user deactivation forms etc.

viii. Prepare governance processes for ICT management in DPC including responsibility and escalation procedures for key activities in the ICT function in DPC.

ix. Evaluate and indicate any gaps that may exist in the current DPC ICT structure based on the developed policies that need to be addressed by DPC.

x. Prepare an implementation plan for the realization of the ICT and security policy in DPC, etc

xi. Present the draft DPC ICT and security policy in a workshop to DPC and other stakeholders, obtain comments and issue a final DPC ICT policy.

3. Deliverables

The deliverables under this assignment shall be as follows:

#	**Deliverable**	**Submission Time for each Deliverable**	**Payment Schedule**
i.	Inception Report	3 Weeks	15% of the contract sum
ii.	Draft ICT and Security Policy Report	8 weeks	65% of the contract sum
iii.	Stakeholder Workshop	1 week	
iv.	Final ICT and Security Policy Report	2 Weeks	20% of the contract sum
Total		**14 Weeks**	

4. Firm/Consultant Experience and Qualifications

The following are the firm experience and qualification requirements required for the implementation of the above assignment:

i. Must be an established firm with atleast 10 years of experience in providing ICT consulting services, with demonstrable experience in Sub-Saharan Africa.

ii. Practical experience in ICT management in central government institutions responsible for ICT policy development and management;
iii. Experience in undertaking preparation of ICT policies in government institutions with atleast 3 successfully concluded assignments of similar nature in the public sector.
iv. Experience in development of ICT security policies with working experience in management and maintenance of ICT security environments.
v. Experience in developing procedure manuals, forms and conducting training and capacity building in an ICT environment in the public sector.
vi. Familiarity with the experience in ICT frameworks such as COBIT, ISACA, relevant ISO IT standards, ITIL, ITSM and System Development Lifecycle.

5. Team Composition

The following shall be the team composition required for the assignment.

i. **Team Leader – ICT Consultant**

The team leader shall be an ICT expert with the following experience and qualifications:

a. Should possess at least Masters or higher degree in Computer Science, Information Technology, Information Systems, Business Technology Management or a related field from a recognized university.
b. Should have training and atleast 10 years working experience in public sector ICT environment with experience in sub-Saharan Africa.
c. Should have atleast 2 projects in which he/she has led the development of an ICT policy on a public sector institution with a scale and complexity such as the DPC environment.
d. Should be qualified in ITIL, ITSM, CDPS or CIPT and have working knowledge of application, engineered systems and application integration.
e. Must be a team player and have experience in leading teams in development of ICT policy documentation.
f. Working experience in Data protection Compliance System environments will be an added advantage.

ii. **Data Centre Expert**

The Data Centre expert shall have the following experience and qualifications:

a. Should possess at least Masters or higher degree in Computer Science, Information Technology, Information Systems or a related field from a recognized university.
b. Should have training and atleast 7 years working experience in public sector ICT environment with experience in sub-Saharan Africa.
c. Should have atleast 2 projects with data centre management experience.
d. Should be qualified in ITIL, ITSM and have working knowledge of application, engineered systems and application integration.
e. Must be a team player and have experience in leading teams in development of ICT policy documentation.
f. Working experience in Data protection Compliance System environments will be an added advantage.

iii. **ICT Security Expert**

The ICT Security expert shall have the following experience and qualifications:

a. Should possess at least Masters or higher degree in Computer Science, Information Technology, Information Systems, Business Technology Management or a related field from a recognized university.
b. Should possess professional certification in CISA, CDPS, or CIPT with atleast 3 years working experience in the ICT security.
c. Should have training and atleast 5 years working experience in public sector ICT environment with experience in sub-Saharan Africa.
d. Should have atleast 2 projects in which he/she has led the development of ICT security policies in a public sector institution with a scale and complexity such as the DPC environment.
e. Should have experience in undertaking information security audits, expertise in developing disaster recovery and continuity plans and developing security management programs. Must be a team player and have experience in leading teams in development of ICT policy documentation.
f. Working experience in Data protection compliance System environments such as the GIFMIS will be an added advantage.

6. Contract Duration, Location and Reporting

The assignment is planned for a maximum duration of 14 weeks. The firm will report to the Data Protection Commission -Accra and with visits to other regional offices of DPC. DPC will assign a counterpart team to work with the consultant to undertake the planned tasks.

7. Data, Local Services, Personnel and Facilities to be provided by the Client

DPC will make available on request all data necessary to assist the Consultant in carrying out the assignment. DPC will provide office space and relevant office facilities during the period of the assignment. Furthermore, DPC shall be responsible for forming an adequate counterpart team alongside the steering committee and a user's group in a properly structured set of Governance structures.