DIGITAL MALAWI ACCELERATION PROJECT

PROJECT NUMBER: P505095

GRANT NUMBER: IDA-E338-MW

TERMS OF REFERENCE (TORS) FOR CYBER SECURITY SPECIALIST

---

1. Background

Information and Communication Technology (ICT) is now globally recognized as an essential tool in promoting competitiveness, job creation, sustainable development, and overall poverty reduction. A combination of widespread access to broadband and a robust ICT services ecosystem can offer a powerful platform for reducing poverty, improving human development and increasing government transparency and efficiency. ICTs have the potential to transform business and government - driving entrepreneurship, innovation and economic growth and breaking down barriers of distance and cost in the delivery of services.

In recognition of the critical role that ICTs plays in fostering socio-economic development and empowering the poor, the Government of Malawi secured a loan from the World Bank to implement an ICT Project, the Digital Malawi Acceleration Project (DMAP). The line Ministry and owner of the Project is the Ministry of Information and Digitalization (MoID) whereas the lead implementation agency for the project is the Public Private Partnership Commission (PPPC). Other stakeholders include Ministry of Education, MAREN, the National Registration Bureau, the Malawi Communications Regulatory Authority (MACRA) and others.

2. The **Digital Malawi Acceleration Project**

The US70 Million (Phase 1) Project comprises the following components:

Component 1: Affordable broadband and secure data hosting. This component will cover rural connectivity that will expand broadband coverage in rural areas with the aim of achieving universal coverage of mobile broadband, connecting at least 500 public sector sites in addition to the at least 530 sites connected though the previous Digital Malawi Foundations Project. Provision of at connectivity services to at least 2,000 schools throughout the country. Being a regional Project, regional connectivity initiatives will be used to address gaps in missing cross-border broadband links, possibly drawing upon a regional financing facility. Finally, it will include integrated infrastructure planning of 'digital corridors' for Southern Africa.

Component 2: Interoperable and secure data platforms. This component will cover the Next Generation Digital ID and identity verification services, including electronic Know Your Customer (eKYC) and Public Key Infrastructure (PKI) (because of the requirement to develop e-Signatures capability for public e-services that require a higher level of assurance). In order to reach all citizenry, the *Bomalathu* data exchange platform for Government will be expanded. The platform faces both Government agencies as well as other players in the private sector, including financial institutions, and the general public. The Component will also seek to enhance policy and regulatory frameworks, operationalization of the Data Protection Authority and support for the MCERT at MACRA.

Component 3: High impact digital services and productive digital usage. This will cover the Digital skills and digital literacy which was started by Digital Malawi Project benefiting over 19,000 beneficiaries, and it is now planned to expand. Participation in regional program on device affordability will also be a major activity in this component. This device affordability program will be complemented by an e-waste initiative that promotes recycling and resale or safe disposal of laptops and phones. This will be carried out in conjunction with the tech hubs, with a focus on skills development and job creation for young people and persons with disabilities (PWD). Finally, it will also look at the Sectoral deep dives: social protection, disaster and emergency response, financial inclusion, and lands management.

Component 4: Project management. This component will cover the establishment of Malawi Information Technology Authority (MITA) by providing funding for the establishment and operationalization of the proposed authority. The Component will also fund the DMAP management and coordination unit that includes procurement, financial management and social and environment standards.

3. Aim of the Assignment

To strengthen the capacity for the e-Government Department, the project wishes to recruit Cybersecurity Specialist as part of the DMAP Support Personnel. This position will be tenable in Lilongwe.

4. Objectives of the Assignment

The Cybersecurity Specialist will be responsible for overseeing the technical operations of the CERT, ensuring the security infrastructure is robust, responsive, and up to date. The specialist will lead the technical team, monitor and secure government systems, and respond to cybersecurity incidents, threat detections, and vulnerability management.

5. Scope of work

The Cyber Security Specialist will be responsible for the following:

- Leading the technical team in monitoring and securing Whole-of-government systems.
- Overseeing incident response, threat detection, and vulnerability management.
- Implementing and maintaining security technologies (firewalls, IDS/IPS, SIEM, etc.).
- Conducting security assessments and audits to identify and address potential vulnerabilities.
- Developing and updating security policies, procedures, and protocols
- Develop and maintain incident response plans to address potential cybersecurity incidents.

- Contribute to cyber-security penetration testing and developing mitigation measures
- Provide inputs into technical specifications of the bidding documents and terms of Reference.
- Provide detailed reports on the security posture, incidents, and mitigation actions.
- Conduct and document regular vulnerability assessments and propose remediation actions.
- Develop and update cybersecurity policies and procedures to enhance the organization's security framework. Providing technical guidance and mentorship to more junior Security Analysts.
- Organize and conduct cybersecurity awareness and training sessions for staff.

6. Required qualifications and attributes:

- Education: Bachelor's degree in Cybersecurity, Information Security, Computer Science, or a related field. A master's degree will be an added advantage.
- Must have at least one of the following certifications (or equivalent):), Certified Information Security Manager (CISM), Certified Ethical Hacker – Practical (CEH), Certified Information Systems Auditor (CISA), or similar.
- At least 7 years of relevant professional experience in cybersecurity, with a focus on security engineering, incident response, and threat management.
- Proven experience in implementing and managing security technologies such as firewalls, IDS/IPS, and SIEM systems.
- Excellent communication skills – both written and verbal, including the capacity to communicate complex and technical issues in simple terms.
- Strong analytical skills with the ability to assess risks and develop appropriate mitigations.
- Ability to work well under pressure and to meet tight deadlines.

7. Duration of the Contract

The Cybersecurity Specialist will be recruited for a period of three (3) years with the possibility of extending the contract subject to satisfactory performance. The performance will be measured based on timely submission and quality of all deliverables, advancement of the respective activities, and the feedback from management and technical team members at e-Government Department focused on technical competency, professionalism, responsiveness, and teamwork.

8. Deliverables

The Cybersecurity Specialist will be required to submit ad hoc and monthly reports covering his/her activities which will go into a common e-Governance report.

- Incident Response Plans:
- Monthly Security Reports:
- Vulnerability Assessment Reports:
- Security Policies and Procedures:
- Reports on Training and Awareness Sessions:
- Where tasks are on-going, the Consultant will be expected to report on key deliverables monthly to demonstrate impact and progress, based on a detailed quarterly work plan developed in close consultation with the Director of Government.

9. **Remuneration and Other Benefits**

The remuneration package for the position is negotiable based proficiency, qualifications and available budget.

10. Contractual Provisions

The Cybersecurity Specialist will work under conditions as stipulated in his/her Consultancy Contract which will be guided by the Laws of Malawi in line with World Bank Regulations and Statutes and PPPC conditions of service.

11. Reporting

The Consultant will work under the direct supervision of The Director, Department of e-Government. However, the legal contract holder shall be the Chief Executive Officer of the Public Private Partnership Commission. The address for whom is as follows:

The Chief Executive Officer
Public Private Partnership Commission
P.O. Box 937
Blantyre.
Malawi.
Telephone: +265 (0) 1 823 655
Fax: +265 (0) 1 821 248
Email: info@pppc.mw

12. Selection

The applicant will be selected on the basis of the approved methods of selecting individual consultants in accordance with the World Bank's "Procurement Regulations for IPF Borrowers" (Procurement Regulations) dated September 2023, and the "Guidelines on Preventing and Combating Fraud and Corruption in Projects Financed by IBRD Loans and IDA Credits and Grants", dated October 15, 2006 and revised in January 2011 and as of July 1, 2016, and other provisions stipulated in the Financing Agreements.