



Terms of Reference for Data Center (DC) Facility Engineer

1. Background

The Ministry of Communication and Technology (MoCT) is the Lead Federal government body mandated to formulate national policies, laws and regulations related to telecommunications, information and communications technology (ICT). Its mandate also include:

- Overseeing sector standards;
- Promoting the development and growth of telecommunications infrastructure and ICT;
- Protecting the interests of consumers;
- Fostering a knowledge based economy and information society

In performing its duties, the MoCT is guided by the constitution of the Federal Republic of Somalia (FGS) and other relevant Laws. The MoCT championed and supported the adoption of the National Communications Law in 2017, which lays the basis for a competitive and enabling regulatory environment for ICT services that recognizes the need for ensuring widespread and inclusive access. The Communications Law also enabled the establishment of the National Communications Authority (NCA), as the industry regulator, in 2018, which is envisioned to play a critical role in supporting and promoting universal access to ICT.

In 2019, the MoCT spearheaded the development of Somalia's first National ICT Policy and Strategy for the period 2019-2023, which aims to address existing gaps in ICT infrastructure and ecosystem. The policy aims to facilitate Somalia's digital transformation to a knowledge based and inclusive society. The policy focuses on accelerating development in the following key areas:

- Policy, legal. And regulatory frameworks;
- Universal access strategy promoting the use of ICT services by women, youth, the disabled, marginalized groups and underserved areas;
- Consumer protection, privacy and child protection;
- Digital services and content;
- E-commerce, e-Health, e-Education, and e-Governance.

A. Existing Digital Ecosystem

A handful of back-end information management systems exist that support core government functions such as the Financial Management Information System (FMIS) and Human Resource Management System (HRMIS) led by the Ministry of Finance in collaboration with Central Bank of Somalia (CBS) and the Civil Services Commission. Moreover, the CBS has been developing core banking system and is rolling out Somalia Transaction Automation Systems (STARS) as well as National Payment Switch. The ministry of planning has developed Aid Information Management System (AIMS); the Ministry of Education has introduced Education Information Management System (EIMS). Other FGS institutions such as the Ministry of Health, Immigration, Office of the Prime Minister (OPM), the Attorney General, and the Ministry of Labor and Social Affairs have been introducing and implementing various digital solutions. And recently the Office of the Accountant General has been implementing electronic documents management system to facilitate to full migration to paperless office and strengthen documents management controls. Despite the focus on digital solutions for core government business, all the various systems implemented by the FGS institutions are not integrated and exist as stand-alone systems. The Government is keen on addressing the fragmentation issue and has started implementing integration process though at a slower pace. The integration between the IFMIS with the banking systems enabling digital payments such as mobile government payments-to-person (G2P) have been piloted for civil servants pay and emergency payments.

B. Shared Services and Infrastructure

The FGS lacks critical enablers needed to support further expansion, including shared services and infrastructure. Moreover, the FGS lacks shared and secure data hosting and management solutions, including guidelines. Different government institutions are saving government data on individual servers, and sensitive personal and government data is not being shared and stored securely, thus there exist large gaps to fill on the back-end of e-government and in terms of adoption of technology. With expansion of digitization of government business, it is critical to develop relevant data protection and privacy policies and regulation. Moreover, the FGS institutions still lack the necessary IT equipment, hardware and software needed to address increase in expected demand. The FGS also lacks many of the foundational platforms and services needed to support gradual movement towards increased front-end secure transactional government services delivery, and unique and verifiable digital Identification.

2. Objective of the Assignment

The FGS sees as critical in establishing a national Data Center to support and strengthen the digital transformation taking place in the public sector as well as the private sector. Thus, the MoCT is implementing a national Data Center that will bring together the FGS digital infrastructure in particular data hosting. The center will bring together the existing individual data hosting facilities existing in various FGS institutions. The center will strengthen the efficiency, security and sustainability of the overall FGS data management infrastructure.

The objective of this assignment is to recruit a Data Center Facility engineer for operations and maintenance of Data Center facilities (this covers the infrastructure including Power, Cooling, Access Control, Surveillance and Fire Suppression systems, etc). The recruited engineer will be accountable for the smooth operation and maintenance of all electrical and mechanical components of the Data Center.

3. Scope of Services

The Data Center Facility Engineer is responsible for the following;

- Design, develop, secure and maintain the entire physical infrastructure of the Data Center
- Ensure adequate power to maintain target environment for all IT hardware in the Data Center
- Perform reliability testing and assists in planning emergency and disaster recovery procedures
- Maintain asset inventory of the Data Center
- Operate and maintain Data Center infrastructure management system
- Monitor and ensure Data Center condition is maintained according to preset level
- Perform preventive maintenance activities
- Ensure that all system functional requirements such as Access control, Fire Suppression, Environmental Control , Voltage protection are successfully acquired and tested
- Provide Support for generation, review, approval, and implementation of change modification proposals for accuracy, completeness, and remediation
- Follow documented daily procedures and policies; monitoring tools and response guidelines, escalation and notification processes; and trouble management processes and guidelines
- Oversee day-to-day Data Center Operations
- Provide infrastructure support to the Security and IT teams
- Support project management activities through risk mitigation and critical operation activities
- Orient and train Data Center Facilities Staff

4. Deliverables

4.1 Data Center Infrastructure Facility Plan: Develop and submit a detailed plan for the secure and efficient operation of the Data Center's facilities. This plan should address power, cooling, access control, surveillance, and fire suppression systems. Include maintenance schedules and a risk management framework.

4.1.1 Emergency and Disaster Recovery Procedures:

- Document emergency response protocols and disaster recovery plans for critical systems to ensure operational continuity during unforeseen events.

4.1.2 Asset Inventory:

- Maintain and update a comprehensive inventory of all Data Center assets, including electrical, mechanical, and IT equipment.

4.2 Operational Reports

4.2.1 Daily Operational Logs:

- Record daily system performance, incidents, and maintenance activities to monitor Data Center conditions and operations.

4.2.2 Preventive Maintenance Reports:

- Provide periodic reports summarizing preventive maintenance activities, highlighting key findings, actions taken, and recommendations for improvement.

4.2.3 Environmental Monitoring Reports:

- Submit regular updates on temperature, humidity, and other environmental factors to ensure optimal operating conditions.

4.2.4 Incident Reports:

- Prepare detailed reports for all operational incidents, including root cause analysis and mitigation steps taken.

4.3 Compliance & Testing

4.3.1 System Functional Testing Reports:

- Ensure and document the critical systems, including access control, fire suppression, environmental controls, and voltage protection, meet required functionality and safety standards.

4.3.2 Change Management Documentation:

- Review, approve, and document change modification proposals, ensuring accuracy and completeness of implementations.

4.3.3 Compliance Reports:

- Maintain records to demonstrate adherence to industry standards and regulatory requirements.

4.4 Infrastructure Support

4.4.1 Infrastructure Support Plans:

- Provide detailed support documentation for collaboration with Security and IT teams.
- Include troubleshooting guides, escalation procedures, and response guidelines.

4.4.2 Risk Mitigation Plans:

- Submit plans identifying vulnerabilities and proposing mitigation strategies to ensure system reliability and security.

4.5 Training & Staff Capacity Support

4.5.1 Training Materials:

- Develop and provide training materials for Data Center Facilities Staff, covering daily operations, maintenance protocols, and emergency response procedures.

4.5.2 Training Reports:

Document and evaluate the effectiveness of training sessions conducted.

4.6 General Reporting

4.6.1 Monthly Performance Reports:

- Summarize key performance metrics, operational activities, resolved issues, and priorities for the upcoming month.

4.6.2 Annual Review Document:

- Provide a comprehensive review of the Data Center operations over the year, highlighting achievements, challenges, and proposed improvements.

4.7 Infrastructure Upgrade Proposals

4.7.1 Upgrade Proposals:

- Submit proposals for infrastructure upgrades, focusing on improving power efficiency, cooling systems, and overall Data Center performance.

4.7.2 Budget Justifications:

- Provide cost-benefit analyses for proposed upgrades and maintenance activities.

4.8 Compliance & Audit Readiness

4.8.1 Audit Preparedness Documentation:

- Ensure systems and processes are audit-ready and compliant with industry standards, such as ITIL and Uptime Institute guidelines.

4.8.2 Compliance Gap Analysis:

- Identify and document areas requiring improvement to meet compliance standards and organizational goals.

5. Qualifications Requirements

- i. Minimum bachelor's degree in electrical/mechanical engineering
- ii. Minimum five (5) years of experience in Data Center facility operations required
- iii. Strong background in Data Center Infrastructure projects is required
- iv. Professional Certification preferred
- v. Current knowledge of Data Center facility systems, procedures and processes
- vi. Working knowledge of electrical, mechanical and life safety monitoring and control
- vii. Computer Skills: i.e Microsoft Office Suite
- viii. Excellent communication skills