

THE UNITED REPUBLIC OF TANZANIA


| Applicable Public Institution | | Document Title | | |
|--|--------------------------|--------------------------------|---|--------------|
| | | ICT Strategy | | |
| Ministry of Works and Transport (Works) | | Document Number | | |
| | | MoWT (Works) / ICTST/01 | | |
| APPROVAL | Name | Job Title/ Role | Signature | Date |
| Approved by | Amb. Eng. Aisha S. Amour | Permanent Secretary |  | August, 2023 |

Table of Contents

| | |
|--|-----------|
| 1 INTRODUCTION..... | 3 |
| 1.1. Overview..... | 3 |
| 1.2. Rationale..... | 3 |
| 1.4. Purpose..... | 4 |
| 1.5. Scope..... | 4 |
| 2. ICT STRATEGY..... | 5 |
| 2.1 Background of the ICT Strategy..... | 5 |
| 2.2. ICT Strategy - Vision, Mission and Objectives..... | 7 |
| 2.3. ICT Strategic Plan Guiding Principles..... | 8 |
| 2.4 Situational Analysis..... | 9 |
| 2.4.1 Analysis of the Efforts Undertaken to Strengthen ICT Function at the Ministry (Works)..... | 9 |
| 2.4.2 SWOC Analysis..... | 11 |
| 2.4.3 Stakeholders Analysis..... | 11 |
| 2.4.4 Critical Issues..... | 12 |
| 2.5 ICT Strategy Focus Areas..... | 12 |
| 2.6 ICT Strategic Formulation:..... | 15 |
| 2.6.1 Key Results Area 1: ICT Governance..... | 16 |
| 2.6.6 Key Results Area 6: ICT Security and Risk Management..... | 25 |
| 2.6.9 Summary of the Key Result Areas..... | 28 |
| 2.7 ICT Strategy Implementation..... | 28 |
| 2.8 ICT Strategy Implementation Budget..... | 38 |
| 4. GLOSSARY AND ACRONYMS..... | 41 |

4.1 GLOSSARY:..... 41

5. RELATED DOCUMENTS..... 42

Appendix I: SWOC Analysis..... 43

Appendix II: Stakeholders, Services offered and their expectations 46

1 INTRODUCTION

1.1. Overview

The adoption of Information Communication Technologies is increasingly a prerequisite for the provision of effective organizational and individual services around the world. In that light, the organizations across the globe, including the Ministry of Works and Transport (Works), are keen to take advantage of ICT to achieve efficiencies in their internal operations as well as to improve access and timeliness in delivering services.

To pursue this, MoWT(W) needs to have comprehensive framework that provides appropriate guidance to harness ICT in order to achieve internal efficiency and effectiveness as well as improving delivery of service. Thus, the Ministry (Works) has realized the importance of having ICT as a supporting tool to fulfil its established mandate and consequently developing its ICT strategy aimed at aligning ICT with its objectives and ambitious as articulated in the Ministry (Works)'s Five-Year Strategic Plan.

Therefore, this Strategy is intended to provide MoWT (W) a high-level direction on the design, control and use of information and communication technology in order to support the attainment of MoWT (W)'s objectives contained in the MoWT (W) Strategic Plan. The strategies presented here and developed in consultation with various key stakeholders are expected to steer MoWT (W) closer to its vision: "To have modern and suitable public infrastructure that facilitate socio-economic development of Tanzania".

1.2. Rationale

In this strategy, the wider context of technology that encompasses Information and Communication Technology (ICT) as well as Information Systems (IS) is adopted in order to serve the purpose of systematic deployment of the Information and Communication Technologies and IT systems in particular. The use of ICT in the Ministry (Works) therefore intended to optimize performance, improve cost effectiveness; and enhance quality and speed in services delivery. The Ministry (Works) will endeavor to provide the following:

- (a) Planning strategically the ICT investment;
- (b) Managing scarce ICT resources optimally;
- (c) Prioritizing ICT processes and projects based on what provides the most value;
- (d) Measuring how well the Works sector is managing the portfolio to meet the Ministry's needs; and
- (e) Instituting standards and minimize risks in ICT deployment in the Ministry.

1.3 Purpose

The purpose of developing ICT Strategy Plan is to provide guideline, plans, objectives, targets and Key Performance Indicators (KPIs) in order to facilitate implementation and evaluation of the objectives and policy statements outlined in the 2023 ICT Policy. Also, it sets standards and improve performance, establish priorities for efficient and effective resource utilization, operationalization of organization structure, increase level of the Works Sector and to support its sectoral policies and strategies by use of ICT. Its development is based on the required alignment with Ministry's 2023 ICT Policy and Strategic Plan.

The interventions outline in this Strategy focuses on the effective implementation of the identified activities to address the five ICT Policy Issues namely; ICT Governance, ICT Infrastructure, ICT applications management, ICT service management and ICT Security as outlined in the 2023 ICT Policy. In order to effectively implement the strategy, all Ministry (Works) Staff and Management will assume different roles and responsibilities in order to achieve the goal of the strategy. The implementation of this Strategy will lead to effective ICT systems which will contribute to the effort towards achieving objectives outlined in the Ministry of Works and Transport (Works) Five Years Strategic Plan 2021/22 - 2025/26.

1.4. Scope

This Strategy applies to all MoWT (Works) employees, including all officers, support staff, temporary staff, partner agency staff, contractors and all users from MDA's/LGA's using MoWT(W) computer services. All staffs are required

to adhere to these Strategies to ensure that desired level of ICT Policy Implementation Strategy plan is achieved and maintained. The Strategy will be reviewed from time to time and when the need arises in order to address new technological challenges and operational environment.

2. ICT STRATEGY

2.1 Background of the ICT Strategy

The Ministry of Works and Transport (Works) aims to develop its ICT strategy based on the Ministry strategic objectives as well as the objectives of the e-Government Act, 2019 and its Regulations. Having an ICT strategy in place will assist MoWT (W) to improve innovation and investment in Information and Communication Technology. The ICT strategy will support and enable MoWT (W) to meet its regulatory and legal responsibilities, effectively manage and monitor organizational risks.

Likewise, ICT strategy will ensure measurable and achievable ICT related outcomes that support the planning and management of ICT services, asset management and procurement of ICT goods.

2.1.1 Alignment with National e-Government Strategy

The e-Government Strategy in Tanzania aims to "Deliver quality services to the public through technology". With that intention, e-Government involves using ICT to support processes within the government (G2G) as well as for the delivery of services to beneficiaries, such as citizens, businesses and other organizations in all sectors.

The e-Government Strategy specifies seven guiding principles for developing initiatives and services. These are:

- (a) **Service Innovation:** The use of e-Government must be geared towards introducing new work methods by creating new operational processes and changing current processes, as well as by changing the government's relationship with the public. Any such innovations must clearly identify resource requirements for sustainable operations. It requires continuous research, development and M&E;
- (b) **Equal Access:** The implementation of ICT in government processes must

ensure that all citizens will have equal access; for this purpose, factors such as geographic location, time, and diversity must be taken into account. It requires developing shared internal facilities that will enable service delivery channels to be available across the general public;

- (c) **Ease of use:** Applications that are to be implemented must be oriented towards citizens and, hence, be user friendly. It requires providing user-friendly Citizen-Care and Business-Centric services for all;
- (d) **Benefit Realization:** Applications should ensure that the benefits obtained by citizens from using e-Government services will be greater than those from visiting government offices in person. Therefore, e-Government investments need to be justifiable in terms of how they help citizens and taxpayers. It requires ensuring services are aligned to client expectations and address pertinent needs;
- (e) **Security and privacy:** When implementing applications, consideration should be given to using security and privacy mechanisms to ensure the proper use and handling of personal information and transactions. It requires assuring security, legality, protection of privacy, prevention of intrusion and detection of attempts at unauthorized access;
- (f) **Partnership and Involvement of all stakeholders:** The private sector can assist the State in providing e-Government solutions, as well as in training government employees. It requires building strategic partnership with private sector stakeholders and encouraging private-sector led innovations in delivering public services; and
- (g) **Interoperability:** Each government department will be responsible for maintaining its electronic services and data sets, as well as for ensuring that newly implemented systems leverage existing systems and are aligned to the principle of Open Access. This requires holistic oversight and management of systems with broad participatory design processes for new systems.

The implication of these principles on the ICT strategy for the Ministry of Works and Transport (Works) is that the ICT infrastructure for the Works sector will be designed to:

- (a) Streamline business processes through use of technology to improve service delivery;
- (b) Systems are designed as part of the government-wide information systems in terms of inter-operability; and
- (c) The information is shared within the Ministry for decision-making.

2.1.2. Alignment with Ministry's (Works) related Strategies and Policies

The Ministry of Works and Transport (Works) has prepared this ICT Strategic basing on the National Development Vision 2025, the National Five Years Development Plan Phase III (2021/2022 – 2025/2026), the Construction Industry Policy (2003), Ruling Part Manifesto (2020), Sustainable Development Goals (2030), Ministry's Instrument (2021), National Transport Policy (2003), Road Safety Act (2009), other National Policy objectives and initiatives. This ICT Strategic Plan covers a period of three (3) years from 2023/24-2025/26.

The coverage of this ICT Strategic Plan involved stakeholder's analysis, performance review, SWOT analysis which assessed the internal and external environment in order to determine the Ministry's Strengths and Weaknesses, Opportunities and Threats existing in the environment as well as identification of critical issues.

2.2. ICT Strategy - Vision, Mission and Objectives

Vision:

To be effective and efficiency in delivering ICT services that can foster staff innovation, economic growth and Social advancement.

Mission:

To empower efficiency of Ministry (Works) through seamless ICT Infrastructure excellence.

Objectives:

The ICT Strategy Plan provides the highest-level ICT directives for Ministry of Works and Transport (Works). The main objective of this document is to ensure that the Ministry of Works and Transport (Works)'s ICT related investment, operations and

maintenance processes and usage are well directed. The specific objectives of this strategy are as follows:

- i. To ensure ICT governance is integral part of the Ministry governance structure;
- ii. To ensure that ICT infrastructure operations are optimized;
- iii. To ensure that ICT applications are managed to address Service requirements and to maximize service delivery;
- iv. To ensure that ICT services provisions are in line with Ministry of Works and Transport (Works)'s service requirements;
- v. To ensure that the Ministry information resources and services are well secured using appropriate controls;
- vi. To ensure that the Ministry employees uses ICT facilities and services in an appropriate and responsible manner;
- vii. To ensure that the standard and approved software used by professionals such as Engineers, Architects, Quantity Surveyors, Technicians etc ;
- viii. To ensure adequate training (in house) are provided to the users on ICT application;
- ix. To ensure e – Government Act, Guidelines and Standards issued by authoritative institution are complied.

2.3. ICT Strategic Plan Guiding Principles

To achieve and enlighten the stated goals and the proposed ICT strategies respectively, nine guiding principles centered on beyond MoWT (W)'s core values. These principles require a commitment from the beyond MoWT (W)'s ICT professionals but from all employees.

- i. **Functionality:** Drive ICT initiatives beyond MoWT (W)'s operational needs, goals, and objectives, and develop a sound business case before making any new investment;

- ii. **Interoperability:** Deploy systems that are flexible and interoperable to respond quickly and efficiently to changing operational needs;
- iii. **Simplicity:** ICT systems must be easy to use in order to win user acceptance. Supporting procedures for hardware and systems should be clear enough to simplify usage of ICT resources;
- iv. **Affordability:** Acquire, manage, and use ICT resources economically and efficiently through standardized selection and implementation processes to provide maximum benefit to MoWT (W) as a whole;
- v. **Business Continuity:** MoWT (W)'s operations must be provided with the capability to continue regardless of disruptive events;
- vi. **Customer Care:** MoWT (W)'s stakeholders shall be treated with courtesy and due respect;
- vii. **Maintainability:** all the technology acquired by MoWT (W) should observe the following; Sustainability, reliability, upgradability and ease of repair in the event of failure sustain;
- viii. **Collaboration and Knowledge Exchange:** Develop knowledge management mechanism and process for sharing and reusing knowledge easily within MoWT (W) and with external stakeholders to help improve MoWT (W)'s effectiveness and quality service delivery;
- ix. **Scalability:** Develop reliable and scalable systems infrastructure with adequate capacity and speed.

2.4 Situational Analysis

This chapter examines the development of MoWT (W)'s ICT environment by providing a brief account of the Ministry (Works)'s performance concerning ICT with a view of portraying important lessons. It briefly presents analysis of the current ICT status at MoWT (W) by evaluating upon the Strengths, Weaknesses, opportunities as well as challenges in order to extract issues that need to be addressed. The results of the Situation Analysis will form the basis of interventions to be carried out under this Strategy.

2.4.1 Analysis of the Efforts Undertaken to Strengthen ICT Function at the Ministry (Works)

In facilitating the use of ICT at the Ministry (Works) a number of initiatives were undertaken in the areas of ICT in Governance, Infrastructure, Human Resources,

Applications Management and Security Management. Notable achievements identified include:

- a) Availability of qualified ICT staff;
- b) Designing, installation and maintenance of both Local Area Network (LAN) and Wide Area Network (WAN);
- c) Exchange programs between the Ministry and other stakeholders;
- d) Training programs to ICT staff and Ministry's staff in order to increase awareness;
- e) Development of several Systems like Special Load Permit System, Monitoring and Evaluation System;
- f) Facilitate Procurement and installed modern ICT equipment for use by Ministry (Works)'s staff;
- g) Provision of user supports on ICT related matters;
- h) Fast, reliable and secured Government mail services (GMS) and other systems e.g., e-office;
- i) Repair and maintenance of hardware resources and ICT infrastructure;
- j) Existence of e-government standards and guidelines has enabled the formulation of MoWT(W)'s ICT Policy, Security Policy, ICT Acceptable Use Policy and ICT Service Management Procedures and

The above-mentioned initiatives resulted in a number of benefits, including: -

- a) Increasing collection and control of revenue from special load permits;
- b) Increased staff efficiency in undertaking day-to-day operations;
- c) Reduced paper works and operational costs;
- d) Improve Service delivery to Transporters and Ministry's Staff;
- e) Cash handling risk reduced into the Ministry through online payment by Special Load Permit System users;
- f) Retrieval and storage of data;
- g) Availability of sustainable internet connection;
- h) Improved coordination of ICT related matters.

While the aforementioned benefits have largely resulted in an increase in the use of ICTs in core and non-core functions, however, there are number of challenges

remain, including: -

- a) Inadequate number of ICT staff;
- b) Inadequate training of ICT staff to cope with new technologies;
- c) Inadequate knowledge on use of ICT application among staff;
- d) Under-utilization of currently invested ICT resources;
- e) Increased security risks and threats due to technology changes;
- f) Inadequate of funds to facilitate ICT related activities;
- g) Inadequate and obsolete ICT infrastructure and
- h) Unreliable power supply.

2.4.2 SWOC Analysis

The Strengths, Weaknesses, Opportunities and Challenges (SWOC) analysis has assessed the internal environment (strengths and weaknesses) and the external environment (opportunities and challenges) in which the MoWT (W) ICT function operates. Refer attached **Appendix I**.

2.4.3 Stakeholders Analysis

The Stakeholders Analysis involved identifying various stakeholders' of MoWT (W)'s services to be offered, their expectations in terms of quality of the services to be offered and the potential impact of not meeting these expectations. This is covered in detail in the attached **Appendix II**.

2.4.3.1. Issues arising from stakeholder analysis

Based on the stakeholder analysis as explained in **Appendix II**, the following factors were identified as issues, which affect the quality of e-services offered to internal and external stakeholders:

- a) Inadequate funds to carryout ICT projects/activities;
- b) Inadequacy of Human capacity to deliver efficient services;
- c) Vulnerability to security risks;
- d) Inadequacy of ICT equipment;
- e) Lack of ICT Awareness to internal and external stakeholders

2.4.4 Critical Issues

From the internal and external analysis, stakeholder analysis, situation analysis, and findings of various ICT studies at MoWT (W), the following are the critical issues that need to be addressed:

- a) Strengthening internal ICT policy framework;
- b) An increasing number of ICT staff to provide support for e-services;
- c) Increasing the budget for carrying out ICT projects/activities;
- d) Undertaking training and security awareness to users;
- e) Untimely maintenance of ICT hardware and network infrastructure;
- f) Establish, develop and operationalize ICT documents and Guidelines;
- g) Increasing ICT awareness and capacity in the organization;
- h) Capacity to cope with a rapid technological change;

2.5 ICT Strategy Focus Areas

There are several issues needed to be addressed in order to improve operational deficiencies on ICT operation situation from the above analysis:

2.5.1 ICT Governance

Effective ICT governance is a critical factor for successful ICT operations in an organization. It ensures that the organization's ICTs are harmonised and supports its goals. ICT Governance covers leadership, organizational structures and processes that ensure that ICT meets the strategic objectives of the institution.

Issues:

- i. Absence of Risk Management Framework (RMF)
- ii. Absence of Change Management Framework
- iii. Absence of ICT Enterprise Architecture

2.5.2 ICT Human Resources Capacity Management

ICT personnel need to be equipped with knowledge and skills in their different specializations to deal with the dynamic changes in the ICT Industry at the global level. The focus is also on encouraging ICT staff to be more productive and to improve innovation.

Issues:

- i. Inadequate working facilities
- ii. Inadequate ICT professional training
- iii. Inadequate incentives to attract and retain ICT professionals
- iv. Inadequate number of ICT Professionals

2.5.3 Business Systems and Applications

ICT systems consist of the setup of hardware, software, data and people who use them. Reliable ICT systems help to improve operational efficiency, increase customer satisfaction, ensure timely and accurate data for decision-making and ultimately reduce operational costs. Innovative ICT systems will effectively support the operations of the Ministry of ICT by maximizing efficient work outcomes and accessibility.

Issues:

- i. High investment cost;
- ii. Rapid change of technology; and
- iii. Control over installation of non-approved applications.

2.5.4 Infrastructure and Technology

The proper ICT functioning and implementation of ICT often involves the investment of new hardware and software. This investment of ICT infrastructure is mainly due to technological requirement, and finally results in network efficiently operation, high-quality systems delivery and user satisfaction.

Issues:

- i. High investment costs for ICT facilities;
- ii. Rapid technological advancement/changes, which demand to acquire equipment that is more modern and new skills; and
- iii. Insufficient and ineffective use of modern equipment and software.

2.5.5 ICT Business Continuity

This means an organization's level of readiness to maintain critical functions after an emergency or disruption. The most basic business continuity requirement is to keep essential functions up and running during a disaster and to recover with as

little downtime as possible. It considers various unpredictable events, such as natural disasters, fires, disease outbreaks, cyber-attacks and other external threats.

Issues:

- i. Data loss protection;
- ii. Determining essential business functions; and
- iii. Ability to maintain essential functions during and after disaster.

2.5.6 ICT Security and Risk Management

ICT Security is an integral part of the IT governance. MoWT (W) shall integrate ICT security risk management that includes risk identification, risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and evaluation into the Enterprise Risk Management Framework.

Issues:

- i. Inadequate ICT security resources;
- ii. Inadequate ICT security awareness to staff; and
- iii. Inadequate knowledge and skills to fight against threats and risk.

2.5.7 ICT Project Management

ICT project Management is an integral part of ICT governance. MoWT shall implement all ICT project in line with e-Government standards and guidelines in order to attain objectives of the Ministerial Strategic plan 2021/2022 -2025/26.

Issues:

- i. Absence of Institutional Project Management Framework; and
- ii. Inadequate funds to facilitate ICT project.

2.5.8 Information Management

Information Management involves collecting, storing, and organizing data in a way that allows for efficient retrieval and use. Its purpose is to ensure that the right information is available to the right people at the right time in order to facilitate decision-making and support the efficient operation of an organization.

Issues:

- i. Controlling expanding volume;
- ii. Securing information access;
- iii. Data quality preservation and
- iv. Automating the operational processes.

2.5.9 ICT Services, Delivery and Support

This is the manner in which organization provides internal or external customers with access to ICT services, which include applications, data storage and other business resources. It covers design, development, deployment, operation and retirement. ICT service, delivery and support are often tied to user satisfaction and business reputation, therefore plays a high priority for the organization.

Issues:

- i. High customers' expectations; and
- ii. Increased dependency on technology.

2.6 ICT Strategic Formulation:

Outcomes of this ICT Strategy which were derived from the situation analysis as areas of improvement from the critical issues have been grouped into nine Key Result Areas (KRAs). The KRAs which will be covered in detail in chapter 2.5 should be seen as interactive interventions that work together towards a common Objective, Vision and Mission indicated in 2.2 above.

The KRAs are:

- (i) KRA 1: ICT Governance;
- (ii) KRA 2: ICT Human Resource capacity management;
- (iii) KRA 3: ICT Business Systems and Applications;
- (iv) KRA 4: ICT Infrastructure and Technology;
- (v) KRA 5: ICT Business Continuity;
- (vi) KRA 6: ICT Security and Risk Management;
- (vii) KRA 7: ICT Project Management;
- (viii) KRA 8: ICT Information Management;

- (ix) KRA 9: ICT Services, Delivery and Support.

2.6.1 Key Results Area 1: ICT Governance

ICT Governance is a strategic framework, which includes overarching leadership framework, organizational structures and processes or procedures that oversee and provide guidance in the development of strategies, implementation, monitoring and evaluation of ICT interventions in the organization and ensuring compliance to ICT standards and guidelines.

Faces challenges in ICT Governance including absence of an effective framework to oversee operations and implementation, secure ICT environment, ICT investment decisions, accountability, monitoring and evaluation of ICT initiatives; limited adoption of ICT Standards and Guidelines to guide ICT interventions; absence of ICT Management Framework for management, maintenance and support of ICT resources; and absence of clear structure/guideline to manage ICT resources among others.

In order to ensure that there is an effective framework to oversee operations and implementation of ICT initiatives, a number of measures and interventions are undertaken to address above issues and challenges, emerging issues which will arise in the course of implementation of this Strategy and achieve the goals and intermediate outcomes under this KRA.

2.6.1.1 Strategic Objectives:

- A.** A well-functioning ICT Management established.

2.6.1.2 Intermediate Outcomes:

The overall goal of this KRA is to implement interventions that lead to development and operationalization of ICT Governance that will provide proper leadership, structure, guidelines and processes that will guide ICT interventions. It is expected that achievement of the interventions under this KRA will lead to the following intermediate outcomes:

- (i) Improved leadership in ICT interventions;

- (ii) Improved monitoring and evaluation of ICT initiatives;
- (iii) Improved service delivery;
- (iv) Increased customer satisfaction;
- (v) Informed decision making in ICT intervention; and
- (vi) Increased use of ICT in internal operations and service delivery.

2.6.1.3 Strategies

The achievement of the above intermediate outcomes is dependent on commitment of resources in implementation of the following strategies:

- (i) To establish and operationalize ICT Steering Committee;
- (ii) To review ICT Structure to cope with extended/expanding functions;
- (iii) To develop and operationalize ICT Management documents (ICT policies, ICT Security Guidelines, ICT Acceptable use guideline, backup/restore plans, etc.) in conformity to e-Government Standards and Guidelines;
- (iv) To developed Enterprise Architecture.

2.6.1.4 Expected Outputs/Targets

To realize the above strategies, the following expected outputs will be delivered:

- (i) ICT steering committee established and sustained by June, 2026;
- (ii) Assessment report on ICT structure produced by June, 2026;
- (iii) At least 9 ICT Management documents which like ICT Policy, ICT Strategy, ICI disaster recover, ICT service management procedure e.t.c in place by June, 2024;
- (iv) ICT Management documents reviewed by June, 2026;
- (v) Enterprise Architecture developed by June, 2024.

2.6.1.4 Outcome Indicators

The realization of the outputs will lead to achievement of the intermediate outcomes indicated in 2.6.1.2 that will be measured using the following outcome indicators.

- (i) Number of ICT Steering Committee meetings conducted;
- (ii) Assessment report produced;
- (iii) Number of ICT management documents developed.

It is expected that effective implementation and realization of the strategy output and intermediate outcomes will enhance ICT Governance therefore achieve the main goal of this KRA.

B. Capacity, innovative and strategic use of ICT enhanced

2.6.1.6 Intermediate Outcomes:

- (i) Improve ministerial competences;
- (ii) Improve working skills;
- (iii) Improved efficiency and effectiveness;
- (iv) Increased expertise;
- (v) Improve working environment.

2.6.1.7 Strategies:

The achievement of the above intermediate outcomes is dependent on commitment of resources in implementation of the following strategies:

- i. ICT awareness to staff created;
- ii. ICT Management documents such as standard operating procedures developed and reviewed.

2.6.1.8 Expected Outputs/Targets

To realize the above strategies, the following expected outputs will be delivered:

- (i) ICT awareness to staff created by June, 2025;
- (ii) ICT Management documents such as standard operating procedures developed and reviewed by June, 2025.

2.6.1.9 Outcome Indicators

- (i) Level of customer satisfaction;
- (ii) Audit rating.

2.6.2 Key Results Area 2: ICT Human Resource capacity management

ICT Human Resource covers the collective skills, knowledge, professional ethics, wisdom and other intangible assets possessed by individuals that can be used to

achieve the Unit's ICT operational goals, needs qualified and multi-skilled ICT human resources with leadership, managerial and specialized skills to achieve its operational goals.

On the other hand, other non-ICT personnel need to be well versed on proper ICT resources utilization, in order for ICT to bring a meaningful contribution to achieve goals. Regular training and awareness for non-ICT personnel needs to be provided in line with technological development and change of business processes.

In the area of ICT human resource is facing a number of challenges including shortage of specialized ICT technical staff, inadequate capacity building and training interventions to both technical and non-technical staff, inadequate incentives to attract, and encourage ICT creativity and innovations.

In order to enhance the ICT HR capacity at a number of measures and interventions will have to be undertaken to address above issues and challenges, emerging HR issues that will arise in the course of implementation of this Strategy to achieve the goals and intermediate outcomes under this KRA.

2.6.2.1 Strategic Objective

To equip with adequate, multi-skilled ICT professionals and skilled ICT users.

2.6.2.2 Intermediate Outcomes

The overall goal of this KRA is to implement interventions that will ensure has adequate number and quality of ICT professionals. This KRA also intends to ensure that staff are well versed on the use of ICT services and resources as well as being aware of vulnerable security risks. It is expected that achievement of the interventions under this KRA will lead to the following intermediate outcomes:

- (i) Increased staff competence in ICT matters;
- (ii) Increased staff productivity;
- (iii) Increased availability of ICT expertise;
- (iv) Reduction in ICT outsourcing cost and risks;
- (v) Increased e-Government initiatives;

- (vi) Increased ICT literacy level;
- (vi) Increased ICT creativity and innovations.

2.6.2.3 Strategies

The achievement of the above intermediate outcome is dependent on commitment of resources in implementation of the following strategies:

- (i) To enhance ICT HR capacity;
- (ii) To encourage ICT creativity and innovations.

2.6.2.4 Expected Outputs/Targets

To realize the above strategies, the following expected outputs will be delivered:

- (i) At least five (5) ICT Professional trainings facilitated by June, 2026;
- (ii) Recruitment of competent ICT Professionals facilitated by June, 2026;
- (iii) Two ICT staff provided with long course training by June, 2026;
- (iv) Basic ICT Awareness training to employees conducted by June, 2026;
- (v) Two (2) ICT staff recruited by June, 2025;
- (vi) ICT creativity and innovations supported by June, 2026.

2.6.2.5 Outcome Indicators

The realization of the above outputs will lead to achievement of the intermediate outcomes indicated in 2.6.2.2 that will be measured using the following outcome indicators:

- (i) Number of certified ICT staff;
- (ii) Number of ICT staff graduated;
- (iii) Number of employees trained;
- (iv) Number of ICT staff recruited;
- (v) Number of internal systems developed.

2.6.3 Key result Area 3: Business Systems and Applications

Reliable and ICT systems result in improving operational efficiency, increase customer satisfaction, ensure timely and accurate data for decision-making consequently, better, quality, timely and more accessible services to the Ministry's stakeholders to be realised.

2.6.3.1 Strategic Objectives

Ensure business system and applications are properly utilized and maintained

2.6.3.2 Strategies

- i. Monitoring and Evaluation System developed and maintained
- ii. Integration of Monitoring and evaluation System with the associated Institutional Information systems
- iii. Improved Special Load Permit System.

2.6.3.3 Expected Outputs/Targets

To realize the above strategies, the following expected outputs will be delivered:

- i. Monitoring and Evaluation System developed and maintained by June, 2023;
- ii. Integration of Monitoring and evaluation System with the associated Institutional Information systems by June, 2025;
- iii. Improved Special Load Permit System by June, 2024.

2.6.3.4 Outcome Indicators

The overall goal of this KRA is to implement the interventions that will enhance information System and application security at offices. It is expected that achievement of the interventions under this KRA will lead to the following intermediate outcomes:

- (i) Increased Integrity of information;
- (ii) Increased confidentiality of information;
- (iii) Increased availability of information;
- (iv) Increased reliability of information;
- (v) Increased security controls;
- (vi) Increased staff awareness on ICT security matter; and
- (v) Reduced information security risks

2.6.4 Key Results Area 4: Infrastructure and Technology

ICT infrastructure consists of all hardware such as network devices, servers, workstations, laptops, desktops, storage devices, back-up, operating facilities and supporting platform like operating systems and databases. ICT infrastructure is the backbone for supporting the business operations as it enables information exchange and providing secure access to different software applications and services. Reliable ICT infrastructure is imperative for supporting and facilitating the achievement of strategic goals.

The main Challenges facing in this area include insufficient unstable power supply which interrupts service provisioning and work operations; absence of connectivity between National Business Portal Infrastructure and backup storage at National Internet Datacentres; and inadequate backup infrastructure for systems.

In order to ensure that has adequate and reliable infrastructure, a number of measures and intervention will have to be taken in order to address above issues, challenges, and other emerging issues that may arise in the course of implementation of this Strategy and the achievement of the goals and intermediate outcomes under this KRA.

2.6.4.1 Strategic Objective

To have in place an optimized ICT infrastructure that supports 's business operations.

2.6.4.2 Intermediate Outcomes

The overall goal of this KRA is to implement interventions which will ensure there is adequate and up and running infrastructure which will facilitate to use ICT effectively in internal operations and service delivery to its customers and stakeholders. It is expected that achievement of the interventions under this KRA will lead to the following intermediate outcomes:

- (i) Increased staff efficiency in undertaking day-to-day operations;
- (ii) Improved administration on ICT systems;
- (iii) Reliable and uninterrupted service delivery;
- (iv) Improved communication systems within and outside;

- (v) Increased Public access to information on;
- (vi) Efficiency of service, which is based on the average time to complete a specific service;
- (vii) Maximized Customer satisfaction;
- (viii) Reduced paperwork and operational costs.

2.6.4.3 Strategies

The achievement of the above intermediate outcome is dependent on commitment of resources in implementation of the following strategy:

- To strengthen ICT Infrastructure
- Scale up and maintain ICT infrastructure

2.6.4.3 Expected Outputs/Targets

To realize the above strategies, the following expected outputs will be delivered:

- (i) ICT equipment acquired by June, 2026;
- (ii) Computer software and licenses procured by June 2026;
- (iii) 90% of ICT equipment maintained by June, 2026;
- (iv) Storage equipment capacity upgraded to 80% by June, 2026;
- (v) Storage equipment capacity upgraded to 80% by June, 2026;

2.6.4.4 Outcome Indicators

The realization of the above outputs will lead to achievement of the intermediate outcomes indicated in 2.6.4.1 which will be measured using the following outcome indicators;

- (i) Number of ICT equipment acquired;
- (ii) Number of Computer Software and licenses procured;
- (iii) Number of sites upgraded;
- (iv) 80% of equipment maintained;
- (v) 80% of storage equipment upgraded.

It is expected that effective implementation and realization of the strategy, output and intermediate outcomes will ensure availability reliable services and adequate hardware, software, and network services for both internal operations and service delivery therefore achieve the main goal of this KRA.

2.6.5 Key Results Area 5: ICT Business Continuity

It is a capability of the organization to continue the use of ICT in the delivery of services at acceptable predefined levels following a disruptive incident or disaster. Business continuity encompasses a set of planning, preparatory and related activities which are intended to ensure that the Ministry (Works)'s critical business functions and services are protected against circumstances that could hamper the delivery of services and plan to reduce the likelihood of occurrence of interrupting incidents and disasters and prepare for or respond to, and recover from disruptive incidents and disasters when they arise.

In the case of an incident or disaster ensure that critical services are recovered to an operational state within a reasonable period of time.

2.6.5.1 Strategic Objectives

To support key Ministry (Works)'s activities operation during crisis

2.6.5.2 Strategies

- i. Potential threat recognized;
- ii. Assess potential impact on the Ministry's daily activities;
- iii. Identifying measures of the possible threats.

2.6.5.3 Expected Outputs/Targets

- i. Potential threat recognized;
- ii. Assess potential impact on the Ministry's daily activities;
- iii. Identifying measures of the possible threats by June, 2026.

2.6.5.4 Outcome Indicators

- i. Increased security controls by June, 2026
- ii. Increased staff awareness on ICT security matter by June, 2026

2.6.6 Key Results Area 6: ICT Security and Risk Management

ICT Security covers all the processes which ensure computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction throughout an organization. In modern world of technology, the security of networks, data and all ICT resources are very important.

Management of ICT Security at faces a number of challenges including inadequate protection of the ICT resources from accidental or malicious acts; inadequate knowledge of advanced ICT security appliances such as firewalls; limited ICT security awareness to staff and other stakeholders in the course of undertaking their responsibilities; inadequate ICT security resources; capacity to manage and keep in pace with rapid technological advances in ICT.

In order to enhance the ICT Security at a number of measures and interventions will have to be undertaken to address above issues, challenges and emerging Security issues in the course of implementation of this Strategy so as to achieve the goals and intermediate outcomes under this KRA.

2.6.6.1 Strategic Objective

To protect 's ICT resources from accidental, intended or malicious acts.

2.6.6.2 Intermediate Outcomes

The overall goal of this KRA is to implement the interventions that will enhance physical, information, hardware and network security at offices. It is expected that achievement of the interventions under this KRA will lead to the following intermediate outcomes:

- (vii) Increased Integrity of information;
- (viii) Increased confidentiality of information;
- (ix) Increased availability of information;
- (x) Increased reliability of information;
- (xi) Increased security controls;
- (xii) Increased staff awareness on ICT security matter; and
- (xiii) Reduced information security risks.

2.6.6.3 Strategies

The achievement of the above intermediate outcome is dependent on commitment of resources in implementation of the following strategies:

- (i) To operationalize ICT security policy;
- (ii) To build capacity on ICT Security (Technical staff and users).

2.6.6.4 Expected Outputs/Targets

To realize the above strategies, the following expected outputs will be delivered:

- i. Increased availability of information by June, 2026;
- ii. Increased reliability of information by June, 2026;
- iii. Increased ICT security awareness to Ministry (Works)'s staff by June, 2026.
- iv. Reduce information security risks by June, 2026

2.6.7 Key Results Area 7: ICT Project Management

ICT project Management is an integral part of ICT governance. MoWT(Works) shall implement all ICT projects in line with e-Government standards and guidelines in order to attain objectives of the Ministerial Strategic plan.

2.6.7.1 Strategic Objective

To ensure ICT project implementation follow the e- Government standards and Guidelines.

2.6.7.2 Strategies:

- (i) Allocate adequate funds for implementation of ICT project;
- (ii) Keep updated with drastic change in technology advancement for ICT equipment and software annually.

2.6.8 Key Results Area 8: Information Management

Information Management is a key component of organization's success by ensuring that the right people have access to the right data at the right time and making sure that data is not lost and exposed to unauthorized users.

2.6.8.1 Strategic Objectives:

To ensure timely provision of information to the intended users

2.6.8.2 Strategies:

- i. Preventing information and data;
- ii. Providing better information and data;
- iii. Speeding up and improving access to more, better quality, centralised information and data.

2.6.8.3 Expected Outputs

- i. Data safely stored by June, 2026;
- ii. Digitized data for ease access by June, 2026;
- iii. Automated processes for speedy output by June, 2026;
- iv. Increased data quality by June, 2026;
- v. Timely Information availability by June, 2026.

2.6.8.4 Outcome Indicators

- (i) Availability of information;
- (ii) Percentage of intended customer have information access;
- (iii) Number of processes automated.

2.6.9 Key Results Area 9: ICT Services, Delivery and Support

The services and support data entry, data storage, data processing, reporting services, monitoring, business and decision support services that are provided and delivered to one or more internal or external stakeholders.

2.6.9.1 Strategic Objectives:

Delivering of quality services to customer

2.6.9.2 Strategies:

- i. Improved quality of service;
- ii. Increased number of services delivered;
- iii. Deployment of new equipment and maintaining hardware and software upgrade.

2.6.9.3 Expected Outputs/Targets

- i. Improved quality of service by June, 2026;
- ii. Increased number of services delivered by June, 2026;
- iii. Deployment of new equipment and maintaining hardware and software upgrade by June, 2026.

2.6.9 Summary of the Key Result Areas

The above nine KRAs form the basis of interventions that will be implemented during the three years' period i.e., 2023/24 - 2025/26 of this ICT strategy. The ICT strategy matrix which summarizes the Key Result Areas, Strategies, Targets and Activities is covered in table 3. The implementation of the interventions and results under this ICT Strategy will be tracked and assessed using a comprehensive Monitoring and Evaluation plan which is covered in chapter 2.7.4

2.7 ICT Strategy Implementation

2.7.1 Strategy Implementation Plan

The ICT Strategy Implementation Plan needs to be prepared in order to provide initiatives in terms of critical areas required to realize the strategies identified. While ICT is a strategic enabler affecting all aspects in MoWT (W) operation, the ICT unit shall be the focal point in the implementation of this strategy and responsible for working very closely with all other departments/units in initiating, implementing and monitoring of ICT projects.

The ICT unit role also shall include among other things management, control and maintenance of the network, ICT systems and security, end user support and

training. The implementation plan will be implemented phase wise based on priority and shall be reviewed once in every three (3) years or whenever such a need arises.

2.7.2 ICT Strategy Implementation Critical Success

The successful deployment of ICT in the Ministry (Works) requires a high level of coordination, a constant demand of tangible results, proactive leadership and strong management. There are always a number of critical success factors and risks associated with ICT implementation. Some of the key ones are highlighted on the following table (Table no. 1)

Table 1: Analysis of Critical Success Factors (CSF)

| S/NO | Critical Success Factors | Impact | Requirements |
|------|--|---|---|
| 1. | Management support and management commitment | <ul style="list-style-type: none"> Increased customer satisfaction Increased use of ICT in operations | <ul style="list-style-type: none"> Strategy acceptance in the Ministry (Works) Continuing engagement of management at all levels of implementation |
| 2. | ICT steering Committee | Improved service delivery | <ul style="list-style-type: none"> Consolidate IT structures to ensure responsiveness and accountability Clear and adequate roles and responsibilities for ICT Unit/people and ICT related coordinating committees. |
| 3. | Human Resource capacity | <ul style="list-style-type: none"> Availability of adequate ICT professionals | <ul style="list-style-type: none"> Continuous capacity development Continuous public involvement |

| | | | |
|----|----------------------------|---|---|
| | | <ul style="list-style-type: none"> Reduction of ICT expertise dependence | |
| 4. | Financial Resources | Annual budgetary ICT implementation of activities planned. | <ul style="list-style-type: none"> Recognition of ICT as a priority area in the delivery of Ministry services, Cost effectiveness in the allocation and use of available financial resources and avoid duplication of efforts or redundancies |
| 5. | Sustainable Infrastructure | <ul style="list-style-type: none"> Service delivery improved Sharing of available ICT resources Speed up of operations Procured ICT equipment | <ul style="list-style-type: none"> Network and information security Infrastructure to sustain the use of IT systems Reliable infrastructure to support continuous availability of data from fields |

2.7.3 Analysis of Risks

Risk is about uncertainties and constraints. There are a number of risks and dependencies that may affect the successful implementation of this strategy. In this manner, risk management shall be a major concern and will involve activities

undertaken with the intent of providing a plan that minimizes the adverse impacts of risk on project resources. Possible risks and mitigation measures have been identified in the table 2 below:

Table2: Delivery Risks

| Risk Description | Impact | Mitigation |
|--|---------------|---|
| Resource un-availability | Medium | Government funding for ICT projects |
| Management Commitment and support | Medium | Sustain management commitment |
| | | Delivery of electronic services for decision making |
| Resistance to change | High | Raise awareness and continuous ICT training. |
| | | Manage expectations. |
| | | Involve all users. |
| | | Clarity of scope, roles and responsibilities. |
| | | Expose technology and do not underestimate the resistance to change within the Ministry (Works) and their benefits. |
| Technological failure | Medium | Business continuity. |
| | | Disaster recovery plan. |
| | | Do not over trust in technology solutions. |
| Technological Obsolescence | Low | Planning of technological refresh. |
| | | Build internal capacity. |
| Privacy and security | Medium | Information security policy. |
| | | Security measures. |
| | | Effective rules and regulations. |
| Poor data quality | High | <ul style="list-style-type: none"> • Well defined procedures • Non conflicting of objectives for the system |
| Stakeholders with different objectives | Medium | Stakeholders' participation in the process and their interests are considered. Frequent |

| | | |
|---|--------|---|
| | | communication to address stakeholders' uncertainty. |
| IT structure that is not strong enough (e.g. unit instead of Department/division) | Medium | Create a decentralized ICT Structure which is closely coordinated by the Ministry's (Works) ICT Department. |

2.7.4 Monitoring and Evaluation

The MoWT (Works)'s Steering Committee will be embedded as the organizational vehicle to take forward ICT strategies, work very closely with all other departments/units to monitor implementation and measuring performance of all ICT related activities. For each ICT area there are Key Performance Indicators (KPIs) which should be used to monitor and evaluate the progress of each ICT area, achievement of MoWT (W)'s ICT strategy in alignment with MoWT (W)'s strategic objectives.

Table 3: Monitoring and evaluation matrix

| Focus Area | Objective | Strategies | Key Performance Indicators (KPI) |
|-----------------------|--|---|--|
| ICT Governance | <ul style="list-style-type: none"> • A well-functioning ICT Management established. • Capacity, innovative and strategic use of ICT enhanced | <ul style="list-style-type: none"> i. Enterprise Architecture developed by June, 2024 ii. ICT steering committee established and sustained by June, 2026. iii. Assessment report on ICT structure produced by June, 2026. iv. At least 9 ICT Management documents in place by June, 2024. v. ICT Management documents reviewed by June, 2026 vi. ICT awareness to staff created by June, 2025. vii. ICT Management documents such as standard operating procedures developed and reviewed by June, 2025. | <ul style="list-style-type: none"> i. Number of ICT Steering Committee meetings conducted annually. ii. Assessment report produced iii. Number of ICT management documents developed. iv. Number of Staff trained. |

| | | | |
|---|---|---|---|
| <p>ICT Human Resource capacity management.</p> | <p>To equip with adequate, multi-skilled ICT professionals and skilled ICT users.</p> | <p>i. Recruitment of competent ICT Professionals facilitated by June, 2026</p> <p>ii. At least five (5) ICT Professional trainings facilitated by June, 2026</p> <p>iii. Basic ICT Awareness training to employees conducted by June, 2026</p> <p>iv. ICT creativity and innovations supported by June, 2026.</p> | <p>i. Two (2) ICT Staff recruited by June, 2025</p> <p>ii. Five (5) ICT Training attended annually</p> <p>iii. Five (5) employees trained annually</p> <p>iv. New innovation toward improving operational process of the Ministry</p> |
|---|---|---|---|

| | | | |
|--|---|--|--|
| Business Systems and Applications | Ensure applications are properly utilized and maintained. | <ul style="list-style-type: none"> i. Monitoring and Evaluation System developed and maintained by June, 2023 ii. Integration of Monitoring and evaluation System with the associated Institutional Information systems by June, 2025 iii. Improved Special load Permit System by June, 2024 | <ul style="list-style-type: none"> i. System in developed and maintained ii. Integrated system in place iii. System improved |
| Infrastructure and Technology | To have in place an optimized ICT infrastructure that supports business operations. | <ul style="list-style-type: none"> i. ICT equipment acquired by June, 2026. ii. Computer software and licenses procured by June, 2026. iii. 90% of ICT equipment maintained by June, 2026. iv. Storage equipment capacity upgraded to 80% by June, 2026. v. Storage equipment capacity upgraded to 80% by June, 2026. | <ul style="list-style-type: none"> i. Number of ICT equipment acquired annually. ii. Number of Computer Software and licenses procured annually. iii. Number of sites upgraded annually. iv. 80% of equipment maintained annually v. 80% of storage equipment upgraded annually |

| | | | |
|---|--|--|--|
| ICT Business Continuity | To support key Ministry (Works)'s activities operation during crisis. | <p>i. Potential threat recognized by June, 2026.</p> <p>ii. Assess potential impact on the Ministry's daily activities by June, 2026.</p> <p>iii. Identifying measures of the possible threats by June, 2026.</p> | <p>i. Rate of incidents occurred annually.</p> <p>ii. Percentage of incidents taken measures annually.</p> |
| ICT Security and Risk Management | To protect ICT resources from accidental, intended or malicious acts. | <p>i. Increased availability of information by June, 2026.</p> <p>ii. Increased reliability of information by June, 2026.</p> <p>iii. Increased ICT security awareness to Ministry (Works)'s staff by June, 2026.</p> <p>iv. Reduce information security risks by June, 2026</p> | <p>i. Percentage of staff awareness on security issues annually.</p> <p>ii. Percentage of security risks occurred and mitigated annually.</p> <p>iii. Rate of occurrence of security violation incidents annually.</p> |
| ICT Project Management | To ensure ICT project implementation follow the e-Government standards and Guidelines. | <p>i. Allocate adequate funds for implementation of ICT project by June, 2026.</p> <p>ii. Keep updated with drastic change in technology advancement for ICT equipment and software annually.</p> | <ul style="list-style-type: none"> ICT budget increased by 10% annually. |

| | | | |
|---|---|---|---|
| Information Management | To ensure timely provision of information to the intended users | <ul style="list-style-type: none"> i. Data safely stored by June, 2026. ii. Digitized data for ease access by June, 2026. iii. Automated processes for speedy output by June, 2026. iv. Increased data quality by June, 2026 | <ul style="list-style-type: none"> i. Percentage of intended customer have information access annually ii. Number of processes automated annually |
| ICT Services, Delivery and Support | Delivering of quality services to customers. | <ul style="list-style-type: none"> i. Improved quality of service by June, 2026. ii. Increased number of services delivered by June, 2026. ii. Deployment of new equipment and maintaining hardware and software upgrade by June, 2026 | <ul style="list-style-type: none"> i. Time spent to provide feedback to customer. ii. Percentage of customers supported. iii. Percentage of new equipment deployed. iv. Percentage of hardware and software upgraded. |

2.8 ICT Strategy Implementation Budget

The planned expenditure over 3 years' period from 2023/2024 to 2025/2026 is **Tshs. 981,713,500.00**. This is approximately **Tshs. 327,237,833** per annum as follows: -

Table 2: ICT Strategy Action Implementation Budget

| S/No | Focus Area | Initiatives | Costs (TZS) – 2023/2024 | Costs (TZS) – 2024/2025 | Costs (TZS) – 2025/2026 |
|-------------|---|---|--------------------------------|--------------------------------|--------------------------------|
| 1. | ICT Governance | <ul style="list-style-type: none"> Functioning ICT Management established. Capacity, innovative and strategic use of ICT enhanced | 52,237,833.33 | 52,237,833.33 | 52,237,833.33 |
| 2. | ICT Human Resource capacity management. | <ul style="list-style-type: none"> Number of ICT staff increased ICT employees Capacity building enhanced | 15,000,000 | 15,000,000 | 15,000,000 |
| 3. | Business Systems and Applications | <ul style="list-style-type: none"> Ensure business system and applications are properly | 25,000,000 | 25,000,000 | 25,000,000 |

| | | | | | |
|----|------------------------------------|---|----------------------|----------------------|----------------------|
| | | utilized and maintained | | | |
| 4. | Infrastructure and Technology | <ul style="list-style-type: none"> To ensure ICT infrastructure are improved | 100,000,000 | 100,000,000 | 100,000,000 |
| 5. | ICT Business Continuity | <ul style="list-style-type: none"> To assess potential impact on the Ministry's daily. | 8,333,333.33 | 8,333,333.33 | 8,333,333.33 |
| 6. | ICT Security and Risk Management | <ul style="list-style-type: none"> Security risk Management enhanced | 10,000,000.00 | 10,000,000.00 | 10,000,000.00 |
| 7. | ICT Project Management | <ul style="list-style-type: none"> To ensure ICT project implementation follow e-Government standards and Guidelines | 16,666,666.67 | 16,666,666.67 | 16,666,666.67 |
| 8. | Information Management | <ul style="list-style-type: none"> To increase data quality To ensure Data are stored safely | 13,333,333.33 | 13,333,333.33 | 13,333,333.33 |
| 9. | ICT Services, Delivery and Support | <ul style="list-style-type: none"> A well-functioning ICT Management for Ministry's | 86,666,666.67 | 86,666,666.67 | 86,666,666.67 |

| | | | | | |
|--|--|--|--|--|--|
| | | <p>ICT Services, Delivery and Support established.</p> <ul style="list-style-type: none"> • Capacity, innovative and strategic use of ICT for ICT Services, Delivery and Support enhanced | | | |
|--|--|--|--|--|--|

3. IMPLEMENTATION, REVIEWS AND ENFORCEMENT

3.1 Implementation and Reviews

- 3.1.1 This document shall come into operation once tabled and agreed in management meeting, and approved in its first page, and then shall be considered mandatory for all MoWT(W)'s operations.
- 3.1.2 The strategies in this document provide top level issues for common understanding of adoption and usage of ICT and delivery of ICT services at the Ministry (Works) based on e-Government standards and guidelines and therefore detailed procedures are necessary.
- 3.1.3 MoWT(W) management shall use this strategy in conjunction with other Ministry's ICT related policies and guidelines, processes and procedures to ensure that it is operated within a well geared ICT governance ecosystem.
- 3.1.4 All employees and other authorized users of Ministry (Works)'s ICT services shall comply with requirements of this strategy.
- 3.1.4 This document shall be reviewed after every three years or whenever business environment of MoWT(W) changes in a way that affects the existing strategy.

3.1.5 Any exception to this strategy must be thoroughly documented and taken through a proper channel of authorization using the same authority which approved this document.

3.2 Exceptions

Any exception to this strategy must be thoroughly documented and taken through a proper channel of authorization using the same authority which approved this document.

3.3 Monitoring and Evaluation

ICT Steering Committee shall meet at least quarterly to monitor and evaluate the achievements in ICT initiatives against MoWT(W) ICT Strategic Plan.

4. GLOSSARY AND ACRONYMS

4.1 GLOSSARY:

- **ICT Strategy** – A document created as an approach to create ICT capability for maximum and sustainable value for a public institution.
- **ICT Security Policy**- is a set of policies issued by an organization that identifies the rules and procedures that all persons accessing computer resources must adhere to in order to ensure the confidentiality, integrity, and availability of data and resources.
- **e-Government standards and guidelines** - A set of detailed guidelines that provide directives to public institutions on the implementation of e-Government. The guidelines are aimed at improving government operations that ultimately result into improved public service delivery.
- **Disaster Recovery Plan (DRP)**- A master plan specifically developed for an organization describing how to deal with the potential disaster to its information systems.

4.2 ACRONYMS:

| | |
|-----------------|--|
| ICT | Information and Communication Technology |
| KRAs | Key Result Areas |
| KPIs | Key Performance Indicators |
| MoWT (W) | Ministry of Works and Transport (Works) |
| SWOC | Strength, Weaknesses, Opportunities and Challenges |
| M&E | Monitoring and Evaluation |
| HR | Human Resource |
| LAN | Local Area Network |
| WAN | Wide Area Network |
| PPPA | Public and Private Partnership Authority |
| PPRA | Procurement Regulatory Authority |

5. RELATED DOCUMENTS

- 5.1 ICT Policy
- 5.2 ICT Security Policy
- 5.3 Acceptable ICT Use Policy
- 5.4 Disaster Recovery Plan
- 5.5 ICT Management Services Procedure
- 5.6 Operational Level Agreement

Appendix I: SWOC Analysis

| | STRENGTHS | WEAKNESSES | OPPORTUNITIES | CHALLENGES |
|--|---|---|--|--|
| Human Resources Capacity management | <ul style="list-style-type: none"> i. Availability of qualified ICT staff. ii. MoWT(W)'s management willingness to support ICT. iv. Ability of ICT staff to cope with advanced technology. | <ul style="list-style-type: none"> i. Inadequate ICT Staff ii. Inadequate incentives to attract and retain ICT professionals. iii. Inadequate ICT professional training iv. Absence of succession plan for ICT staff. | <ul style="list-style-type: none"> i. Availability of local and International ICT training Institutions. ii. Availability of ICT partners. | <ul style="list-style-type: none"> i. Limited funds to facilitate ICT capacity building. ii. Centralized remuneration and incentive scheme |
| ICT Governance | <ul style="list-style-type: none"> i. Existence of ICT Unit ii. Availability of ICT Policy iii. Management support for ICT activities | Absence of ICT Service Level Agreements. | <ul style="list-style-type: none"> i. Existence of e-government standards and guidelines ii. Existence of eGA to support ICT initiative iii. Presence of e-Government Act, 2019 and its Regulations of 2020 | Compliance with e-Government standards and Guidelines. |

| | STRENGTHS | WEAKNESSESS | OPPORTUNITIE S | CHALLENGES |
|---------------------------|--|---|--|---|
| | | | iv. Availability of Government network (Govnet). | |
| ICT Infrastructure | <p>i. Existence of Basic ICT infrastructures.</p> <p>ii.Strong relationship with vendors</p> | <p>i. Obsolete ICT equipment.</p> <p>ii. Low quality of technology used.</p> <p>iii. Inadequate number of ICT equipment</p> | <p>i. Availability of Government network (Govnet)</p> <p>ii. Presence of ICT Shared resources, such as Government Data Centre and NIDC</p> | <p>i. High investment costs for ICT facilities.</p> <p>ii. Rapid technological advancement /changes, which demand to acquire modern equipment and new skills.</p> <p>iii. Security Risk</p> |

| | STRENGTHS | WEAKNESSES | OPPORTUNITIES | CHALLENGES |
|-------------------------------------|---|--|--|--|
| Applications | Development in-house Monitoring and Evaluation systems (M&E System) | Absence of e-services applications. | Availability of modern technology and technological systems in the market. | i. Partial ownership of ICT applications. ii. Inadequate budget to support the application. |
| ICT Security | Existence of ICT security appliances. | Sharing of credentials between users. | i. Availability of Government ICT Security Standards and Guidelines. ii. Presence of Cyber Crime Act, 2015 | i. Reluctance of ICT users and Stakeholders in implementing security measures. ii. Cyber-attack and data theft. |
| Operational Process Analysis | Operational process reviewed | Absence of disaster recovery and operational continuity plan | Existence of training programs that enhance appropriate technology transfer, knowledge sharing and capacity building | High cost of technology transfer |
| Stakeholders Analysis | i. Existence of MoWT(W) website. | Inadequacy of ICT resources. | i. Existence of Government | i. Availability of sustainable power supply. |

| | STRENGTHS | WEAKNESSES | OPPORTUNITIES | CHALLENGES |
|--|---|------------|--|--|
| | ii.Existence of LAN and internet service. iii.Availability of shared network resources | | network (GovNet) ii. Existence of Government Mailing System (GMS) to facilitate communication | ii. Misuse of ICT resources by stakeholders. |

Appendix II: Stakeholders, Services offered and their expectations

| S/N | Stakeholder | Expected Services | Stakeholders' Expectations | Potential Impacts of not meeting their expectations |
|-----|---------------------------|--|--|--|
| 1. | Finance and Accounts Unit | i. Finance Management Information System. ii. Internet services iii. Email services iv. Hardware and software maintenance services. v. Day-to-day user support | i. Reliable and timely support services ii. Fast and reliable, secured internet services iii. Timely notification. | i. Poor services delivery ii. Poor performance iii. Increasing Complaints iv. Increasing Complaints v. Vulnerability to security risks |

| S/N o | Stakeholder | Expected Services | Stakeholders' Expectations | Potential Impacts of not meeting their expectations |
|----------|------------------------------|---|---|---|
| 2. | Procurement Management Unit | i. Procurement Management Information Systems. ii. Internet services iii. Email services iv. Hardware and software services. v. Day-to-day user support | i. Reliable and timely support services ii. Fast, reliable and secured internet services iii. Timely notification | i. Poor contract management ii. Poor services delivery iii. Poor performance iv. Increasing Complaints v. Poor Image and bad reputation of the Unit vi. Non-Compliance with PPA and PPRA |
| 3. | Policy and Planning Division | i. Planning, Monitoring and Evaluation Management Information system. ii. Internet services iii. Hardware and software maintenance services. iv. Network maintenance services. | i. Fast and reliable internet services ii. Fast, reliable and secured Intranet services. iii. Prompt and quality services. iv. Timely notification. v. Timely communication | i. Poor services delivery ii. Poor performance iii. Increasing Complaints iv. Poor Image and bad reputation of the Unit v. Vulnerability to security risks |

| S/N | Stakeholder | Expected Services | Stakeholders' Expectations | Potential Impacts of not meeting their expectations |
|-----|-----------------------------|---|--|--|
| | | v. Day-to-day user support | | |
| 4. | Roads Division | i. Roads Networks and project monitoring and Evaluation systems. ii. Hardware and software maintenance services. iii. Network maintenance services. iv. e-Meetings facilities v. Day-to-day user support. | i. Reliable, secured and timely services enabled by ICT. ii. Fast and reliable internet services iii. Fast, reliable and secured Intranet services. iv. Prompt and quality services. v. Timely notification. vi. Timely communication | i. Poor services delivery ii. Poor performance iii. Increasing Complaints iv. Loss of Public Trust v. Vulnerability to security risks vi. Upload Contractor and Consultancy Claims. vii. Delay in implementation of development projects |
| 5. | Technical Services Division | i. Motor vehicle, Electrical, Electronics Management Information System. ii. Internet services iii. Hardware maintenance services. | i. Reliable, secured and timely services enabled by ICT. ii. Fast and reliable internet services. | i. Poor services delivery ii. Poor performance iii. Increasing Complaints |

| S/N o | Stakeholder | Expected Services | Stakeholders' Expectations | Potential Impacts of not meeting their expectations |
|----------|---|--|--|---|
| | | iv. Software maintenance services. v. Network maintenance services. vi. Intranet services vii. e-notifications viii. Day-to-day user support | iii. Prompt and quality support services. iv. Timely notification. | iv. Poor Image and bad reputation of the Department v. Loss of Public Trust vi. Vulnerability to security risks |
| 6. | Administration and Human Resources Management Division. | i. Administration and Human Resource Management Information Systems. ii. Internet services iii. Intranet services iv. Hardware maintenance services. v. Software maintenance services. vi. Network maintenance services. vii. e-notifications viii. Day-to-day user support | i. Fast and reliable internet services ii. Timely notification. iii. Prompt and quality support services | i. Poor services delivery ii. Poor performance iii. Increasing Complaints iv. Poor Image and bad reputation of the Department v. Loss of Public Trust vi. Vulnerability to security risk |

| S/N o | Stakeholder | Expected Services | Stakeholders' Expectations | Potential Impacts of not meeting their expectations |
|----------|---------------------|---|--|---|
| 7. | Legal Services Unit | <ul style="list-style-type: none"> i. Legal services management Information system ii. Intranet services iii. Internet Services iv. Hardware maintenance services. v. Software maintenance services. vi. Network maintenance services. vii. e-notifications viii. Day-to-day user support | <ul style="list-style-type: none"> i. Reliable, secured and timely services enabled by ICT. ii. Fast and reliable internet services iii. Fast, reliable and secured Intranet services. iv. Prompt and quality services. v. Timely notification. | <ul style="list-style-type: none"> i. Poor services delivery ii. Poor performance iii. Increasing Complaints iv. Poor Image and bad reputation of the Unit v. Loss of Trust vi. Vulnerability to security risks |
| 8. | Internal Audit Unit | <ul style="list-style-type: none"> i. Internal Audit Management Information Systems ii. Internet Services iii. Intranet services iv. Hardware maintenance services. v. Software maintenance services. | <ul style="list-style-type: none"> i. Reliable, secured and timely services ii. Fast and reliable internet services iii. Prompt and quality support services. iv. Timely notification. | <ul style="list-style-type: none"> i. Under performance ii. Time consuming in extracting data iii. Poor Image and bad reputation of the Unit iv. Loss of Public Trust v. Vulnerability to security risks |

| S/N o | Stakeholder | Expected Services | Stakeholders' Expectations | Potential Impacts of not meeting their expectations |
|----------|-----------------------------|--|--|---|
| | | vi. Network maintenance services. vii. Email services viii. e-notifications ix. Day-to-day user support | | |
| 9. | Safety and Environment Unit | i. Safety and environment Information Systems ii. Internet services iii. Intranet Services iv. Hardware maintenance services. v. Software maintenance services. vi. Network maintenance services. vii. Email services, viii. e-notifications ix. Day-to-day user support | i. Reliable, secured and timely services ii. Fast and reliable internet services iii. Prompt and quality support services. iv. Timely notification. | i. Under performance ii. Time consuming in extracting data iii. Poor Image and bad reputation of the Unit iv. Loss of Public Trust v. Vulnerability to security risks |
| 10 | Airports Construction Unit | i. Airport Construction | i. Reliable, secured and timely services | i. Under performance |

| S/N o | Stakeholder | Expected Services | Stakeholders' Expectations | Potential Impacts of not meeting their expectations |
|----------|-------------------------------|--|---|---|
| | | Information Systems ii. Internet services iii. Intranet services iv. Hardware maintenance services. v. Software maintenance services. vi. Network maintenance services. vii. Email services, viii. e-notifications ix. Day-to-day user support | ii. Fast and reliable internet services iii. Prompt and quality support services. iv. Timely notification. | ii. Time consuming in extracting data iii. Poor Image and bad reputation of the Unit iv. Loss of Public Trust v. Vulnerability to security risks |
| 11. | Government Communication Unit | i. Government Communication Information Systems ii. Intranet services iii. Internet services iv. Hardware maintenance services. v. Software maintenance services. | i. Reliable, secured and timely services ii. Fast and reliable internet services iii. Prompt and quality support services. iv. Timely notification | i. Under performance ii. Time consuming in extracting data iii. Poor Image and bad reputation of the Unit iv. Loss of Public Trust v. Vulnerability to security risks |

| S/N o | Stakeholder | Expected Services | Stakeholders' Expectations | Potential Impacts of not meeting their expectations |
|----------|-------------|---|----------------------------|---|
| | | vi. Network maintenance services. vii. Email services, viii. e-notifications ix. Day-to-day user support | | |