

THE UNITED REPUBLIC OF TANZANIA

MINISTRY OF WATER

**RURAL WATER SUPPLY AND SANITATION
AGENCY**



RUWASA ICT POLICY

Version 1

AUGUST, 2022

THE UNITED REPUBLIC OF TANZANIA

RUWASA

Document Title

ICT Policy

Document Number

RUWASA ICT POLICY 2022

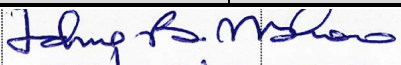
APPROVAL	Name	Job Title/ Role	Signature	Date
Approved by	Prof. IDRISSA BILALI MSHORO	BOARD CHAIRMAN	 25/08/2022	

Table of Contents

1. INTRODUCTION	1
1.1. Background.....	1
1.2. Rationale	1
1.3. Purpose.....	2
1.4. Scope.....	2
2. ICT POLICY STATEMENTS	2
2.1. ICT Governance.....	2
2.1.1. Objectives	2
2.1.2. ICT processes and organisation	3
2.1.3. Dissemination of roles and responsibilities of stakeholders for ICT	3
2.1.4. ICT resources management	4
2.1.5. ICT performance management.....	4
2.1.6. Compliance.....	4
2.1.7. ICT projects management	5
2.1.8. Procurement of ICT equipment and services	5
2.2. ICT Infrastructure	5
2.2.1. Objectives	5
2.2.2. Infrastructure planning and design.....	6
2.2.3. Data management and storage.....	6
2.2.4. ICT equipment and hosting.....	6
2.2.5. Infrastructure maintenance and support	6
2.3. Applications	7
2.3.1. Objectives	7
2.3.2. Applications acquisition and deployment	7
2.3.3. Applications maintenance and support	8
2.4. ICT Service Management.....	8
2.4.1. Objectives	8
2.4.2. ICT service desk.....	9
2.4.3. Management of service levels	9
2.4.4. Management of third-party services	9
2.4.5. ICT service requests, incidents and problems management	10
2.4.6. Change management	10
2.4.7. ICT service availability.....	10

2.4.8.	<i>ICT service continuity</i>	10
2.4.9.	<i>Configuration management</i>	11
2.4.10.	<i>Capacity management and development</i>	11
2.4.11.	<i>Data management</i>	11
2.5.	ICT Security	11
2.5.1.	<i>Objectives</i>	11
2.5.2.	<i>ICT security management</i>	12
2.5.3.	<i>Monitoring</i>	12
2.5.4.	<i>Continuity management</i>	13
3.	IMPLEMENTATION, REVIEWS, AND ENFORCEMENT	13
3.1.	Implementation and Reviews	13
3.2.	Exceptions	14
3.3.	Organisation Structure	14
3.4.	Roles and Responsibilities	15
3.4.1.	<i>RUWASA Board of Directors</i>	15
3.4.2.	<i>Director General</i>	16
3.4.3.	<i>ICT Steering Committee</i>	16
3.4.4.	<i>Heads of departments and units</i>	16
3.4.6.	<i>Chief Internal Auditor</i>	18
3.4.7.	<i>Users of ICT systems</i>	18
3.5.	Monitoring and Evaluation	18
4.	GLOSSARY AND ACRONYMS	18
4.1.	Glossary	18
4.2.	Acronyms	18
5.	ICT RELATED DOCUMENTS	18
6.	DOCUMENT CONTROL	19

1. INTRODUCTION

1.1. Background

The Rural Water Supply and Sanitation Agency (RUWASA) was established on 01st July, 2019 by the Water Supply and Sanitation Act No. 5 of 2019. Specifically, the Act has mandated RUWASA to plan, develop, maintain and manage the provision of reliable water supply and sanitation services in Tanzania Mainland. The mandate is to be realised under the overall guidance and oversight of the Ministry of Water, and in liaison with the local government authorities and the regional and district administrations. It is also provided by the Act to cooperate with the private sector, where applicable. Considering the apparent and critical importance of clean and safe water for livelihood and economic development, the Tanzania rural community has high expectations of better services from RUWASA, and which the Agency has to realise, as anticipated. At the time of RUWASA's inception, the access to rural water supply was 64.8% of the population while the national policy perspectives require the coverage to at least reach 85% by the year 2025. The magnitude of the statutory undertaking of RUWASA, stakeholders' expectations and their diversity require the Agency to maintain certain core organizational and operational values for attaining the purposes of its establishment. Such values include professionalism, integrity, creativity, team-work and unity of purpose, customer focus and good governance and management.

1.2. Rationale

Information and Communication Technology (ICT) if properly harnessed can indeed facilitate RUWASA to realise its statutory obligations and stakeholders' expectations with the desired core values. Most of the undertakings of the Agency, and especially for sustenance of service delivery operations are increasingly dependent on ICT for efficiency and effectiveness. The anticipated benefits from ICT however, cannot be attained if the technology is applied in an *ad hoc* manner. Various ICT-related risks exist and which need to be mitigated. In this regard, RUWASA has developed this ICT Policy in a consultative manner and in line with best practice. The Policy directs ICT adoption and usage by the Board of Directors, Management and Staff. It is generally intended to provide guidance, consistency, accountability, efficiency, and clarity on all RUWASA's ICT-mediated operations.

1.3. Purpose

The main purpose of this policy is to assist RUWASA handle its ICT needs as per its mandate and strategic vision. The specific objectives of this policy are;

- (a) To ensure ICT governance is an integral part of RUWASA governance.
- (b) ICT service provisions are aligned with RUWASA's business requirements based on existing e-Government standards and the best practices.
- (c) All RUWASA information resources and services are well secured using appropriate controls.
- (d) To ensure that members of RUWASA use ICT facilities and services appropriately and responsibly. Also, to ensure that other people do not misuse ICT facilities and services.

1.4. Scope

This policy applies to all RUWASA staff and its associates, all users of ICT equipment owned or leased as well as all equipment connected to RUWASA's ICT-related infrastructure. This policy applies to all RUWASA's ICT-related resources and services.

2. ICT POLICY STATEMENTS

2.1. ICT Governance

2.1.1. Objectives

ICT Governance is an integral part of corporate governance and consists of the leadership, organizational structures, and processes with set objectives.

- (a) The general objective is to put the strategic and operational management of ICT within the principles of ICT Governance and within the context of RUWASA strategic directions.
- (b) The specific objectives are:

- (i) Establishing a framework for ICT investment decisions, accountability, monitoring, and evaluation; and
- (ii) Ensuring there is a formal ICT governance process that is consistent across the Agency, and has strong accountability.

2.1.2. *ICT processes and organisation*

RUWASA shall ensure that,

- (a) An ICT governance model is established, that has the right structure to manage ICT operations and secure an ICT environment that complies with e-Government standards;
- (b) An ICT Steering Committee is appointed to determine prioritization of ICT-enabled investment programmes aligned with RUWASA's business strategy and priorities, track the status of ICT initiatives, resolve resource conflicts and monitor ICT services;
- (c) A strong ICT Unit capable of supporting its strategic objectives is established and operationalised;
- (d) ICT strategic plan and Enterprise Architecture are established and operationalised;
- (e) ICT plans fit the current and ongoing needs of the Agency to support its strategic plans;
- (f) ICT Risk Management is periodically done. Where ICT risk assessment is conducted and reviewed, the likelihood and occurrence identified, mitigation strategy established and risks treated, accepted, transferred, or avoided.

2.1.3. *Dissemination of roles and responsibilities of stakeholders for ICT*

RUWASA shall ensure that,

- (a) All concerned individuals and groups understand and accept their responsibilities for ICT;

- (b) Clear and well-understood ICT contracts exist for external suppliers;
- (c) Related and acceptable documents are known and adhered to by concerned staff.

2.1.4. *ICT resources management*

RUWASA shall ensure that,

- (a) A set of policies for ICT security is defined and approved by the Board of Directors of RUWASA, and subsequently published, and communicated to employees and relevant external parties;
- (b) ICT acquisitions are made with approved reasons in an approved way;
- (c) There is appropriate balance between costs, risks, long-term and short-term benefits.

2.1.5. *ICT performance management*

RUWASA shall ensure that,

- (a) Adopted ICT is fit for its purpose in supporting and keeping responsive to changing business requirements;
- (b) ICT Services are well defined, e.g., email services, printing services;
- (c) A mechanism for evaluating and monitoring ICT services is established (E.g., Service availability, staff satisfaction/feedback system).

2.1.6. *Compliance*

RUWASA shall ensure that,

- (a) ICT Policy conforms to e-Government standards and guidelines, external regulations, and all internal policies, procedures, and practices;
- (b) All employees and third parties have a personal obligation to comply with internal ICT policy, guidelines, and procedures, and must keep abreast of, and comply with any changes. Failure to comply may result in legal or disciplinary actions.

2.1.7. *ICT projects management*

RUWASA shall ensure that,

- (a) ICT projects conform to Government ICT projects management procedures and all internally developed procedures for managing projects;
- (b) RUWASA Management monitors the key ICT projects undertaken and provides regular progress reports on risks identified and preventive actions taken.

2.1.8. *Procurement of ICT equipment and services*

RUWASA shall ensure that,

- (a) RUWASA Management implements the necessary controls to ensure that all ICT procurements are done in line with the requirements of the Public Procurement Act (PPA) and Regulations;
- (b) User Departments establish and submit, in writing, all ICT-related requirements whether ad-hoc or planned, to the ICT unit, who shall process and submit them to Procurement Management Unit;
- (c) ICT Unit ensures that procurement of ICT requirements complies with e-Government Standards and Guidelines;
- (d) Procurement Management Unit does not procure any ICT system, service, equipment, consumables, or accessories if the request has not been endorsed from the ICT Unit.

2.2. *ICT Infrastructure*

2.2.1. *Objectives*

ICT infrastructure is the backbone for supporting the RUWASA business operations by enabling information exchange and providing secured access to different applications. This consists of all hardware devices such as network devices, servers, workstations, computers,

storage, back-ups, operating facilities, and supporting platforms like operating systems and databases.

The objective of managing ICT Infrastructure is to ensure that RUWASA's ICT infrastructure operations are optimized to deliver high-level service quality and support business-relevant operations based on ICT planning and managing best practices.

2.2.2. Infrastructure planning and design

RUWASA shall ensure that,

- (a) ICT infrastructure architecture is in place and line with its current and future requirements;
- (b) Appropriate ICT infrastructure is set up and well managed.

2.2.3. Data management and storage

RUWASA shall ensure that all business-related data is stored in a way that facilitates backup procedures and access.

2.2.4. ICT equipment and hosting

RUWASA shall ensure that,

- (a) All ICT equipment such as computers, servers, printers, and networking equipment are acquired from authorised suppliers;
- (b) All ICT resources are acquired in consultation with the ICT Unit;
- (c) An appropriate environment is established for the hosting, computing, and storage of ICT equipment based on standards and best practices.

2.2.5. Infrastructure maintenance and support

RUWASA shall ensure that,

- (a) All ICT infrastructure components are maintained at a reasonably defined operational and secure level;
- (b) A standard software list is established, which will include operating and application systems to be installed;
- (c) All maintenance services are procured from organisations that comply with the technical requirements of the Agency;
- (d) All ICT maintenance services are procured in consultation with the ICT Unit.

2.3. Applications

2.3.1. Objectives

Applications are software designed for end-users to use in their daily operations to support the enterprise business processes, with set objectives.

- (a) The general objective of managing applications is to ensure that, the ICT applications are in use or are to be acquired to address the business requirements and provide a reasonable return on investment.
- (b) The specific objectives are:
 - (i) To ensure system acquired follow proper procedures;
 - (ii) To establish controls for efficient acquisition and administration of applications; and
 - (iii) To enhance accountability on the management and usage of ICT applications.

2.3.2. Applications acquisition and deployment

RUWASA shall ensure that,

- (a) A clear understandable business and system requirements exist before any application acquisition;

- (b) User departments submit to Planning Department their ICT requirements in order to be included in the respective resource budget;
- (c) All applications supplied are checked by the ICT Unit to verify, if the technical requirements established are met and approved;
- (d) ICT Unit establishes appropriate software standards to facilitate acquisition or development;
- (e) The best configuration is adopted for all acquired systems.

2.3.3. *Applications maintenance and support*

RUWASA shall ensure that,

- (a) Administration and maintenance of applications are ongoing processes that will last throughout the life cycle of the application;
- (b) Every application acquired by RUWASA has requisite documentation in place and updated regularly;
- (c) Installation of additional applications or overriding existing ones follow change management procedures;
- (d) All third-party software packages acquired for installation into RUWASA's equipment are licensed.

2.4. ICT Service Management

2.4.1. *Objectives*

ICT Service management refers to how ICT resources and core business practices altogether are delivered in such a way that the end-user experiences the most desired results from accessing the entire solution stack.

- (a) The main objective of ICT service management is to improve the satisfaction of internal and external stakeholders.
- (b) The specific objectives are:
 - (i) To assist in defining meaningful metrics to measure service results and using the metrics to drive continuous service improvement.
 - (ii) To enable the monitoring and improvement of service quality through the effective application of processes.
 - (iii) To ensure compliance with all e-Government Standards and Guidelines relating to the ICT Service Management.

2.4.2. *ICT service desk*

RUWASA shall ensure that an ICT Service Desk that supports functions is established to minimize business disruptions, respond to user queries and timely resolve ICT problems. An ICT Service Management document shall be developed accordingly.

2.4.3. *Management of service levels*

RUWASA shall ensure that,

- (a) Service Level Agreements between the providers and the recipients are established for every ICT service provided;
- (b) Reports on service quality are reviewed periodically with customers to determine things that could be added or changed to improve service delivery and support.

2.4.4. *Management of third-party services*

RUWASA shall ensure that,

- (a) Proper processes and procedures for managing vendors are in place;
- (b) Services procured from third parties (suppliers, vendors, and partners) meet business requirements;

- (c) A good relationship is built with the business and third-party providers to ensure that ICT services delivered continue to meet its evolving business needs.

2.4.5. *ICT service requests, incidents and problems management*

RUWASA shall ensure that,

- (a) A single point of contact is set i.e. service desk officer for end-users where requests will be recorded, escalated to the correct group, resolved, and closed to ensure restoration of normal service operations as quickly as possible;
- (b) ICT service catalogue is prepared and approved;
- (c) Service requests, incidents management processes, and procedures are established to ensure minimal adverse impacts on customers;
- (d) All reports about problems that resulted in systems downtime are reviewed to identify root causes of problems.

2.4.6. *Change management*

RUWASA shall ensure that processes for recording, assessing and authorizing all changes before implementation, including changes procedures, processes, systems and service parameters are established.

2.4.7. *ICT service availability*

RUWASA shall implement available management processes to ensure that services are available when needed, and as defined in approved Service Level Agreements.

2.4.8. *ICT service continuity*

RUWASA shall ensure that,

- (a) A business impact analysis is conducted to identify critical business functions to be supported by ICT;

- (b) Robust business continuity and service recovery plans are in place, and are regularly reviewed, tested and key staff are appropriately trained.

2.4.9. *Configuration management*

RUWASA shall ensure that all information regarding ICT assets, Service Level Agreements, End User documentation version control, and change requests shall be loaded into the configuration management system.

2.4.10. *Capacity management and development*

RUWASA shall ensure that,

- (a) A capacity plan is established to monitor ICT resources usage for existing and planned systems to assist in the time and cost-effective purchase of additional resources to avoid unplanned purchases when resources run out;
- (b) Staff are regularly trained and capacitated on the use and integrity of ICT systems and infrastructures.

2.4.11. *Data management*

RUWASA shall ensure that,

- (a) The business requirements of the Agency for data management is determined and data conform to the Government data and metadata standards;
- (b) Procedures for effective and efficient data storage, retention, and archiving are developed to meet business objectives, the ICT Security Policy, and regulatory requirements.

2.5. ICT Security

2.5.1. *Objectives*

ICT Security covers all the processes by which computer-based equipment, information, and services are protected from unintended or unauthorized access, change, or destruction throughout an organization.

- (a) The general objective of managing ICT Security is to provide RUWASA with an information security mechanism to support the achievement of its strategic goals based on best practices.
- (b) The specific objectives are:
 - (i) Protection of ICT resources from accidental or malicious activities while preserving the open information-sharing requirements of the Government; and
 - (ii) Making RUWASA stakeholders aware of their responsibilities concerning ICT security.

2.5.2. *ICT security management*

RUWASA shall ensure that,

- (a) ICT security is actively supported through clear direction, demonstrated commitment, explicit assignment, and acknowledgment;
- (b) Information systems are designed, acquired, and implemented with effective ICT security controls to safeguard the integrity, confidentiality, and continual availability throughout the entire life cycle;
- (c) ICT Security Policy is established to highlight the implemented ICT security controls that ensure ICT security risks are mitigated and controlled. The document may be complemented by other ICT security sub-documents that define more specific security policies for individual components of the ICT environment;
- (d) All users of RUWASA systems are responsible for protecting the information resources;
- (e) It retains the overall responsibility and ownership for all information assets.

2.5.3. *Monitoring*

RUWASA shall ensure that,

- (a) The use of all its ICT facilities and premises is adequately monitored. This includes, but is not restricted to, accessing and reviewing the contents of the server, email accounts, hard drives, text messages, telephone systems, voicemail and mobile telephone logs, access control logs, and CCTV recordings;
- (b) Its business interests are protected, for quality control purposes, as well as timely detection or prevention of abuse of the systems, crime or misconduct.

2.5.4. *Continuity management*

RUWASA shall ensure that,

- (a) An ICT environment is established that will remain running without affecting the business performance or services;
- (b) A disaster recovery plan is developed to ensure reliable service in case of service outage or distortion.

3. IMPLEMENTATION, REVIEWS, AND ENFORCEMENT

3.1. Implementation and Reviews

- 3.1.1.** This document shall come into operation once approved by the Board of Directors of RUWASA, and then shall be considered mandatory for all RUWASA business operations.
- 3.1.2.** This policy provides top-level issues for a common understanding of adoption and usage based on eGovernment standards and guidelines and where necessary detailed documents could be developed.
- 3.1.3.** RUWASA Management will use this policy in conjunction with the documents listed in Section 5 below, to ensure that it operates within a well-gearred ICT ecosystem.
- 3.1.4.** All employees and other authorised users shall comply with the requirements of this policy.

- 3.1.5. The Manager responsible for ICT shall enforce compliance by using audit trails and triggering access denial to RUWASA systems and networks.
- 3.1.6. Any staff found to have violated this policy may be subject to withdrawal and or suspension from systems and network privileges or get subjected to disciplinary action by rules defined by RUWASA administrative regulations.
- 3.1.7. This document shall be reviewed within three years, or whenever the business environment changes in a way that affects the current policy.

3.2. Exceptions

- 3.2.1. In case of any exceptions to this policy, it shall be thoroughly documented and follow the proper channel of authorization.

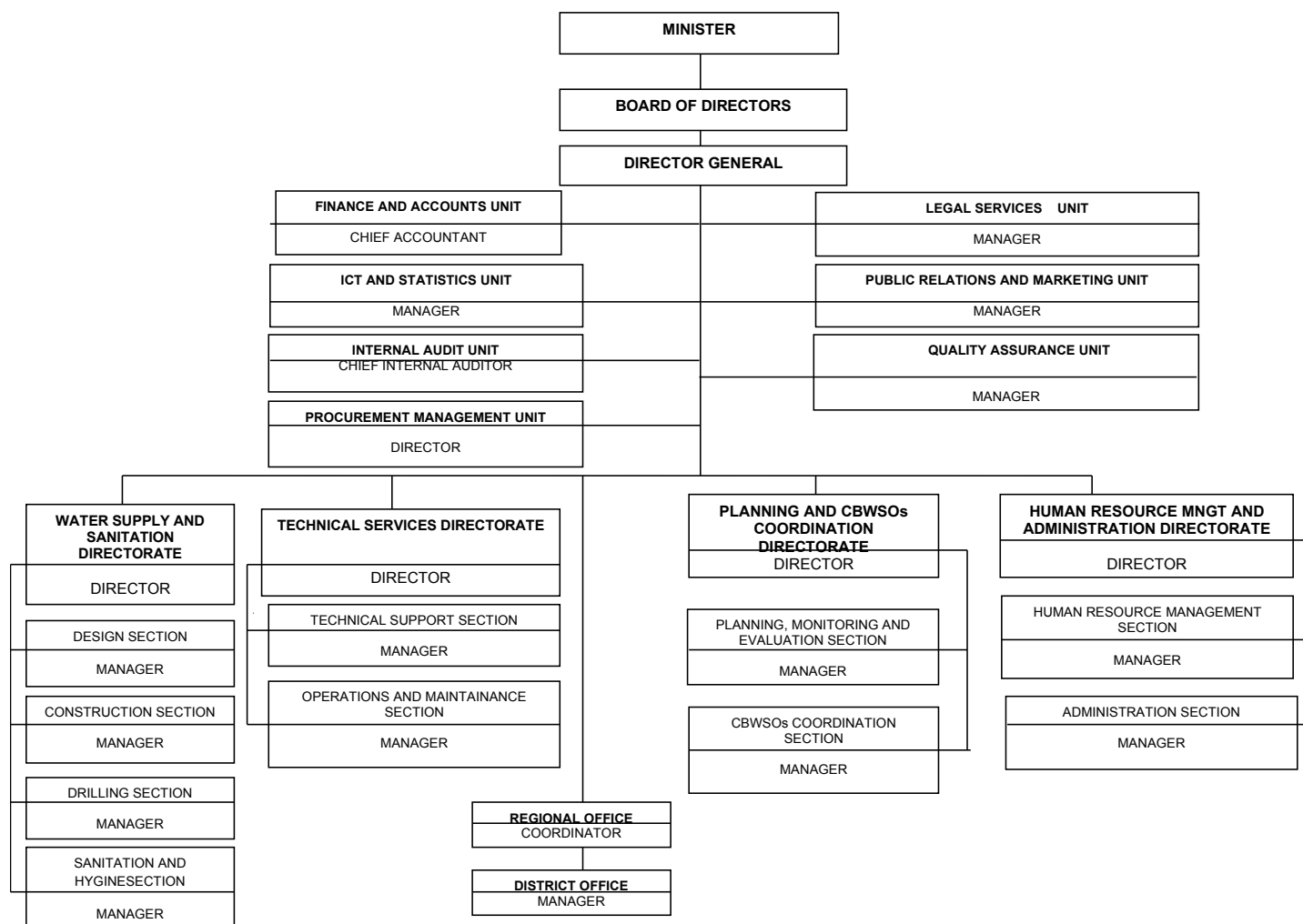
3.3. Organisation Structure

RUWASA organisational structure comprises of four (4) Directorates, seven (7) Units, and 25 Regional Office, which are responsible to the Director General as shown in chart I below. List of departments and units are as follows:

- (i) Water Supply and Sanitation Directorate;
- (ii) Technical Services Directorate;
- (iii) Planning and CBWSOs Coordination Directorate;
- (iv) Administration and Human Resource Management Directorate;
- (v) Quality Assurance Unit;
- (vi) Finance and Accounts Unit;
- (vii) Public Relations and Marketing Unit;
- (viii) Procurement Management Unit;
- (ix) Internal Audit Unit;
- (x) Information and Communication Technology and Statistics Units;
- (xi) Legal Services Unit;
- (xii) Regional Offices; and
- (xiii) District Offices.

Chart I

THE FUNCTIONS AND ORGANIZATIONAL STRUCTURE OF RURAL WATER SUPPLY AND SANITATION AGENCY (RUWASA)



3.4. Roles and Responsibilities

3.4.1. RUWASA Board of Directors

- (a) Approve the ICT Policy and its revisions in line with the RUWASA's business requirements and existing e-Government standards and the best practices.

- (b) Provide strategic direction on the utilisation of ICT.

3.4.2. *Director General*

- (a) Overall in charge for proper implementation of the approved ICT Policy.
- (b) Appoint an ICT Steering Committee and determine its terms of reference.
- (c) Oversee the review of the ICT Policy in line with the strategic directives of the RUWASA Board of Directors on utilisation of ICT in order to enhance productivity of the Agency.

3.4.3. *ICT Steering Committee*

- (a) Coordinate the establishment and continuous review of RUWASA's ICT Policy, ICT Strategy, and all other supporting documents as listed in section 5 of this Policy.
- (b) Advise the Director General on the alignment of the ICT Strategy with RUWASA's Strategic Plan.
- (c) Advise the Director General in making considered decisions about the focus of ICT resources.
- (d) Review all ICT services and applications including website and infrastructure with the view to advise RUWASA on required improvements;
- (e) Ensure that risks associated with ICT are managed appropriately.

3.4.4. *Heads of departments and units*

- (a) Ensure that all users under their supervision are aware and comply with ICT policy.

- (b) Provide adequate and appropriate protection of ICT assets and resources under their control.
- (c) Ensure availability, integrity, and confidentiality of information produced by systems under their areas of functional responsibilities and thereby ensure continuity of operations.
- (d) Review and approve procedures, standards, policies, and guidelines developed from this policy to maintain business continuity and security of RUWASA's ICT resources.
- (e) Be the custodian of "Data and Information" for their respective Departments and Units.

3.4.5. *ICT Manager*

Subject to general oversight of the Accounting Officer and the advice of the ICT Steering Committee, the Manager responsible for ICT shall oversee the overall implementation of the policy; and in particular shall;

- (a) Coordinate the review and amendment of the policy as required to accommodate new technologies or services, applications, procedures, and perceived dangers;
- (b) Plan and develop ICT Strategy, Enterprise Architecture, and ensure its implementation.
- (c) Monitor adherence to the ICT Policy, the presence of potential threats and risks by ensuring periodic ICT security reviews are conducted.
- (d) Keep abreast of ICT developments in respect to the ICT industry.
- (e) Initiate and recommend proposals to change, modify or improve the policy.
- (f) Recommend procedures, standards and policies for effective implementation of the policy in line with e-Government Standards and Guidelines.

- (g) Be the custodian of all RUWASA's ICT resources (infrastructure and data) including those centrally stored in the server room and data centre.

3.4.6. *Chief Internal Auditor*

Shall audit the ICT functions of RUWASA and ensure compliance with the policy.

3.4.7. *Users of ICT systems*

- (a) Shall be responsible to safeguard the ICT assets of RUWASA in their custody.
- (b) Shall comply with RUWASA's ICT policy.

3.5. Monitoring and Evaluation

ICT Steering Committee shall meet at least quarterly to monitor and evaluate the achievements of ICT initiatives against RUWASA ICT Policy, Strategic Plan, and Enterprise Architecture.

4. GLOSSARY AND ACRONYMS

4.1. Glossary

Agency - RUWASA

ICT Policy - A document that elaborates on the Public Institution's ICT Management Philosophy by providing general statements of purpose, direction, and required activities for the entire ICT Management Framework.

4.2. Acronyms

- **CBWSO** - Community Based Water Supply Organisation
- **CCTV** - Closed Circuit Television
- **ICT** - Information & Communication Technology
- **RUWASA** - Rural Water Supply and Sanitation Agency

5. ICT RELATED DOCUMENTS

For proper implementation of this Policy, the following documents shall be developed as listed below;

- 5.1. ICT Strategy
- 5.2. Enterprise Architecture
- 5.3. ICT Security Policy
- 5.4. ICT Service Management Guidelines
- 5.5. Disaster Recovery Plan
- 5.6. Acceptable ICT Use Policy
- 5.7. ICT Project Management Guidelines
- 5.8. ICT Acquisition, Development, and Maintenance Guidelines

6. DOCUMENT CONTROL

VERSION	NAME	COMMENT	DATE
Ver. 1.0	Responsible Section		

-----*For Government Control Only*-----

Document Name: **ICT Policy**

Reference: **RUWASA/ICTP/2022/001**

Version: **1.0**

Effective Date: **August 2022**

Creation: **RUWASA**