THE REVOLUTIONARY GOVERNMENT OF ZANZIBAR				
Applicable Public Institution **<<insert the name of the Institution >>**	**Document Name** ICT Policy			
	Document Number <<Insert your own document reference code>>			

PPROVAL	Name	Job Title/ Role	Signature	Date
Approved by	<<Name of Accounting Officer >>	<<Title e.g. CEO>>	<<Signature>>	<<Date>>

Table of Contents

1. INTRODUCTION

1.1. Overview

The trend towards a knowledge-based economy has emphasized the importance of ICT in development efforts in **<< include the institution's business operations sector >>** sector. This shift requires a well-developed technology investment plan and intelligent deployment and maintenance management.

For **<< include the name of the institution >>** to realize the value out of ICT investment, ICT must be deployed to improve efficiency and effectiveness in internal and external services delivery. This means that, a comprehensive framework established by ICT Policy to provide appropriate directives to harness ICT, is necessary for achievement of **<< include the name of the institution >>**'s objectives.

Establishment of ICT Policy is the important step toward ensuring that ICT will assist **<< include the name of the institution >>** to attain its objectives. The ICT Policy will ensure that the ICT infrastructure and capacity are utilized effectively and are in alignment with the **<< include the name of the institution >>**'s strategic objectives, National ICT Policy, National e-Government Strategy and the e-Government Standards and Guidelines.

1.2. Rationale

<< Include the name of the institution >> need to meet its objective of improving its services and increasing productivity by leveraging on new technologies. **<< include the name of the institution >>** has been investing in ICT to facilitate its internal business operations so as to attain its strategic goals. **<< include the name of the institution >>** operations are increasingly depending on ICT, making the Institution vulnerable to ICT related risks. In this regard, it is evident that, **<< include the name of the institution >>** needs to develop and operationalize comprehensive ICT Policy to direct ICT adoption and usage within the Institution.

1.3. Purpose

This document provides the highest level ICT directives for **<< include the name of the institution >>**. The main purpose of this document is to ensure that **<< include the name of the institution >>**'s ICT related investment, operations and maintenance processes and usage are well directed. The specific objectives of this policy are;
  i.   To ensure ICT governance is integral part of the institutional governance.

ii.   ICT services provisions are in line with **<< include the name of the institution >>**'s business requirements based on existing e-Government standards and best practices.

iii.   All the Institution information resources and services are well secured using appropriate controls.

iv.   To ensure the members of the Institution use ICT facilities and services in an appropriate and responsible manner and to ensure that other persons do not misuse those ICT facilities and services.

1.4.   Scope

This policy is applicable to all **<< include the name of the institution>>**'s staff and its associates, all users of ICT equipment owned or leased by the Institution as well as all equipment connected to **<<include the name of the institution>>**'s ICT related infrastructure. This policy applies to all **<< include the name of the institution >>**'s ICT related resources and services.

2.   ICT POLICY STATEMENTS

2.1.   ICT Governance

ICT Governance is an integral part of corporate governance and consists of the leadership, organisational structures and processes that ensure that the organisation's ICT sustains and extends the organisation's strategies and objectives.

The general objective of ICT Governance is to put the strategic and operational management of ICT within the principles of ICT Governance and within the context of **<<include the name of the institution>>** strategic directions. Specific objectives are:

i.   Establishing a framework for ICT investment decisions, accountability, monitoring and evaluation; and

ii.   Ensuring there is formal ICT governance process that is consistent across the enterprise and has strong accountability.

2.1.1.   ICT Processes and Organisation

2.1.1.1.   **<< Include the name of the institution >>** will set up an ICT governance model so that it have the right structure to manage ICT operations and a secure ICT environment that complies with e-Government standards.

2.1.1.2.   There shall be an **ICT Steering Committee** (or equivalent) to determine prioritisation of ICT-enabled investment programmes in line with the Institution's

business strategy and priorities, track status of ICT initiatives, resolve resource conflicts and monitor ICT services.

2.1.1.3.   **<<Include the name of the institution>>** shall establish a strong ICT department/unit capable of supporting strategic objectives of the institution.

2.1.1.4.   **<<Include the name of the institution>>** shall ensure that ICT strategic plan and Enterprise Architecture are established and operationalized.

2.1.1.5.   **<<Include the name of the institution>>** shall ensure that ICT plans fit the current and on-going needs of the institute and that the ICT plans support the institute strategic plans.

2.1.1.6.   **<<Include the name of the institution>>** shall ensure that ICT Risk Management periodically done, where ICT risk assessment is conducted and reviewed, likelihood and occurrence identified, mitigation strategy established and risks treated, accepted, transferred or avoided.

2.1.2.   Roles and Responsibilities for ICT

2.1.2.1.   **<<Include the name of the institution>>** shall ensure that individuals and groups within the Institution understand and accept their responsibilities for ICT.

2.1.2.2.   **<<Include the name of the institution>>** shall ensure that clear and well understood contracts exist for external suppliers.

2.1.2.3.   **<<Include the name of the institution>>** shall ensure that acceptable use and related policy are known and adhered to by staff.

2.1.3.   ICT Resources Management

2.1.3.1.   **<<Include the name of the institution>>** shall define a set of policies for ICT security, which shall be approved by management, published and communicated to employees and relevant external parties.

2.1.3.2.   **<<Include the name of the institution>>** shall ensure that ICT acquisitions are made for approved reasons in an approved way; on the basis of appropriate and on-going analysis.

2.1.3.3.   **<<Include the name of the institution>>** shall ensure that there is appropriate balance between costs, risks, long-term and short-term benefits.

2.1.4.   ICT Performance Management

2.1.4.1.   **<<Include the name of the institution>>** shall ensure that ICT is fit for its purpose in supporting the Institution, is kept responsive to changing business requirements.

2.1.4.2.   **<<Include the name of the institution>>** shall ensure that ICT Services are defined, e.g. Email services, Printing services.

2.1.4.3.   **<<Include the name of the institution>>** shall establish mechanism for evaluating and monitoring ICT services (E.g. Service availability, staff satisfaction / feedback system).

2.1.5.   Conformance

2.1.5.1.   **<<Include the name of the institution>>** shall ensure that ICT conforms to e-Government standards and guidelines and all external regulations and complies with all internal policy, procedures and practices.

2.1.5.2.   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.

2.1.6.   ICT Projects Management

2.1.6.1.   **<<Include the name of the institution>>** shall ensure that ICT conforms to the Government ICT projects management procedures and complies with all internal developed procedures for managing projects.

2.1.6.2.   **<< Include the name of the institution>>** management team will monitor the key ICT projects undertaken and provide regular progress reports on risks identified and preventive/detective actions taken.

2.1.7.   Procurement of ICT Equipment and Services

2.1.7.1.   **<< Include the name of the institution>>** management will implement the necessary controls to ensure that all ICT procurements are done in line with requirements of Public Procurement and disposal of public Asset Act.

2.1.7.2.   User Departments shall establish and submit, in writing, all ICT related requirements weather ad-hoc or planned, to ICT **<<section/unit/department>>,** who will process and submit them to procurement unit.

2.1.7.3.   ICT **<<section/unit/department>>,** shall ensure that all requirements for ICT procurements comply with e-Government Standards and Guidelines.

2.1.7.4.   Procurement unit shall not procure any ICT System, Service, Equipment, Consumable or Accessory if the request is not originating from ICT **<<section/unit/department>>.**

2.2.   ICT Infrastructure

ICT infrastructure is the backbone for supporting the **<<include the name of the institution>>** business operations by enabling information exchange and providing secure access to different applications. This consists of all hardware devices such as network devices,

servers, workstations, laptop, storage, back-up, operating facilities and supporting platform like operating systems and databases.

The objective managing ICT Infrastructure is to ensure that the **<<include the name of the institution>>**'s ICT infrastructure operations are optimized in order to deliver higher level service quality and support business-relevant operations based on ICT planning and management best practices.

2.2.1. Infrastructure Planning and Design

2.2.1.1.   **<<Include the name of the institution>>** shall ensure that ICT infrastructure architecture is in place and in line with the Institution's current and future requirements.

2.2.1.2.   **<<Include the name of the institution>>** shall ensure that appropriate ICT infrastructure is setup and well managed.

2.2.2. Data Management and Storage

2.2.2.1.   **<<Include the name of the institution>>** shall ensure that all business related data shall be stored in a way to facilitate back up procedures and access.

2.2.3. ICT Equipment and Hosting

2.2.3.1.   **<<Include the name of the institution>>** shall acquire desktop computers, laptop, servers, printers and networking equipment from authorized suppliers.

2.2.3.2.   All ICT resources shall be acquired in consultation with ICT **<<section/unit/department>>**.

2.2.3.3.   **<<Include the name of the institution>>** shall ensure that approved Government environment for hosting computing and storage equipment based on standards and best practices is used.

2.2.4. Infrastructure Maintenance and Support

2.2.4.1.   **<<Include the name of the institution>>** shall ensure that all ICT infrastructure components are maintained at a reasonable operational and secure level.

2.2.4.2.   **<<Include the name of the institution>>** shall ensure that standard software list including the operating system to be installed into the Institution's equipment is established.

2.2.4.3.   **<<Include the name of the institution>>** shall procure maintenance services from organization that have technical capabilities.

2.2.4.4.   **<<Include the name of the institution>>** shall ensure that maintenance services are procured in consultation with ICT **<<section/unit/department>>**.

2.3. Applications

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

The general objective of managing applications is to ensure that ICT applications that are in use or are to be acquired to address the business requirements of the Institute and provide reasonable return on investment. Specific objectives are:

i. To ensure system acquired follow proper procedures set by institution responsible for e-Government implementation;
ii. To establish controls for efficient acquisition and administration of applications; and
iii. To enhance accountability on the management and usage of ICT Applications.

2.3.1. Applications Acquisition and Deployment

2.3.1.1. There shall be clear understandable business and system requirements before any application acquisition.

2.3.1.2. User departments shall submit to ICT **<<section/unit/department>>** their ICT requirements to be included in ICT resource budget.

2.3.1.3. All applications supplied shall be checked by ICT **<<section/unit/department>>** to verify the technical if requirements established are met and approved.

2.3.1.4. ICT **<<section/unit/department>>** shall establish appropriate software standards to facilitate acquisition/development in line with e-Government technical standard.

2.3.1.5. ICT **<<section/unit/department>>** shall ensure the best configuration is adopted for the system acquired.

2.3.2. Applications Maintenance and Support

2.3.2.1. Administration and maintenance of applications shall be an on-going process that will last throughout the life cycle of the application.

2.3.2.2. Every application acquired by the Institute shall have documentation in place and updated regularly.

2.3.2.3. Installation of additional applications or overriding existing one shall follow change management procedures as described under *ICT service Management Procedure.*

2.4. ICT Service Management

ICT Service management deals with 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.

The objectives of ICT Service Management are:

i. To improve internal and external stakeholder's satisfaction.
ii. To assist in defining meaningful metrics to measure service results and using the metrics to drive continuous service improvement.
iii. To enable the monitoring and improvement of service quality through the effective application of processes.
iv. To ensure compliance with all e-Government Standards and Guidelines relating to the ICT Service Management.

2.4.1. ICT Service Desk

2.4.1.1.   **<<Include the name of the institution>>** shall operate an ICT service and support function which will ensure that business disruptions are minimised, users' queries are responded to and ICT problems are resolved. An ICT Service Management document shall be developed accordingly.

2.4.2. Management of Service Levels

2.4.2.1.   **<<Include the name of the institution>>** shall ensure that for every ICT services provided, Service Level Agreements between the providers and the recipients are established.

2.4.2.2.   **<<Include the name of the institution>>** shall ensure that reports on service quality are reviewed periodically with customers along in order to determine things that could be added or changed to improve service delivery and support.

2.4.3. Management of Third Party Services

2.4.3.1.   **<<Include the name of the institution>>** shall ensure proper processes and procedures for managing vendors are in place.

2.4.3.2.   **<<Include the name of the institution>>** shall ensure that services procured from third parties (suppliers, vendors and partners) meet business requirements.

2.4.3.3.   **<<Include the name of the institution>>** shall ensure that it builds good relationships with the business and third party providers to ensure that ICT services delivered continue to meet evolving Institution's business needs.

2.4.4. ICT Service Requests, Incidents and Problems Management

2.4.4.1.   **<<Include the name of the institution>>** shall set up a single point of contact i.e. service desk 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.

2.4.4.2.   **<<Include the name of the institution>>** shall ensure that ICT service catalogue is prepared and approved.

2.4.4.3.   **<<Include the name of the institution>>** shall ensure that Service Requests and Incidents Management processes and procedures are established to ensure minimal adverse impacts on customers.

2.4.4.4.   **<<Include the name of the institution>>** management shall review all reports about problems that resulted to systems downtime in order to identify root causes of problems.

2.4.5. Change Management

2.4.5.1.   **<<Include the name of the institution>>** shall ensure that a process for recording, assessing and authorizing all changes prior to implementation, including changes procedures, processes, systems and service parameters is established.

2.4.6. ICT Service Availability

2.4.6.1.   **<<Include the name of the institution>>** shall implement an availability management process to ensure that services are available, when needed, and as defined in approved Service Level Agreements.

2.4.7. ICT Service Continuity

2.4.7.1.   **<<Include the name of the institution>>** shall conduct a Business Impact Analysis to identify critical Business functions to be supported by ICT.

2.4.7.2.   **<<Include the name of the institution>>** shall ensure that a robust business continuity and service recovery plans are in place and that these plans are regularly reviewed and tested and key staff are appropriately trained.

2.4.8. Configuration Management

2.4.8.1.   All information regarding ICT assets, Service Level Agreements, End User documentations version control and change requests shall be loaded into the configuration management system.

2.4.9. Capacity Management

2.4.9.1.   **<<Include the name of the institution>>** shall establish a capacity plan to monitor ICT resources usage for existing and planned systems in order to assist in time and cost effective purchase of additional resources so as to avoid panic purchase when resources run out.

2.4.10. Data Management

2.4.10.1.   **<<Include the name of the institution>>**'s business requirements for data management shall be determined and data shall conform to the Government data and metadata standards.

2.4.10.2.   **<<Include the name of the institution>>** shall develop procedures for effective and efficient data storage, retention and archiving to meet business objectives, the Institution's ICT Security Policy and regulatory requirements.

2.5.   ICT Security

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.

The general objective of managing ICT Security is to provide **<<include the name of the institution>>** with information security mechanism to support the Institution to achieve its strategic goals based on best practices. The specific objectives are:

i.   Protection of the **<<include the name of the institution>>**'s ICT resources from accidental or malicious act while preserving the open information sharing requirements of the Government; and

ii.   Making the **<<include the name of the institution>>**'s stakeholders aware of their responsibilities with respect of ICT security.

2.5.1.   ICT Security Management

2.5.1.1.   **<<Include the name of the institution>>** shall actively support ICT security within the Institution through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of ICT security responsibilities.

2.5.1.2.   **<<Include the name of the institution>>** shall ensure 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.

2.5.1.3.   ICT security Policy shall be established to highlight the implemented ICT security controls that ensures 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.

2.5.1.4.   All users of **<<include the name of the institution>>** systems shall be responsible for protecting the institute's information resources.

2.5.1.5.   **<<Include the name of the institution>>** shall retain overall responsibility and ownership for all Institution's information assets.

2.5.2. Monitoring

2.5.2.1.   **<<Include the name of the institution>>** will monitor use of its ICT facilities and premises. This includes, but is not restricted to, accessing and reviewing the contents of servers, email accounts, hard drives, text messages, the telephone system, voicemail and mobile telephone logs, access control logs and CCTV recordings. This is to ensure that the institution's business interests are protected, for quality control purposes, to detect abuse of the systems, or to detect or prevent crime or misconduct.

2.5.3. Continuity Management

2.5.3.1.   **<< Include the name of the institution >>** will maintain its ICT environment so that it remains in a running state and does not affect the business performance or services. A disaster recovery plan will be developed accordingly.

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, approved in its first page, and then shall be considered mandatory for all **<<include the name of the institution>>** business operations.

3.1.2.   The policies described below provide top level issues for common understanding of adoption and usage at the Institution based on e-Government standards and guidelines and where necessary detail procedures could be developed.

3.1.3.   **<<Include the name of the institution>>** management will use this policy in conjunction with the documents in Section 5, below to ensure that it operated within a well geared ICT ecosystem.

3.1.4.   All employees and other authorised users of **<<include the name of the institution >>** shall comply with requirements of this policy.

3.1.5.   The head responsible for ICT shall enforce compliancy by using audit trails and triggering access denial to **<<include the name of the institution >>** systems and networks.

3.1.6.   **<<Include the name of the institution >>** staff found to have violated this policy may be subject to withdrawal and or suspension of systems and network privileges or disciplinary action in accordance with rules defined by **<<include the name of the institution >>** administrative regulations.

3.1.7.   This document shall be reviewed within three years, or whenever business environment of **<<include the name of the institution >>**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 through a proper channel of authorization using the same authority which approved this document.

3.3. Roles and Responsibilities

3.3.1. <<board of directors or accounting officer, whichever applies>>

3.3.1.1. Review and approve General ICT Policy, and provide strategic directives on utilisation of ICT in order to enhance productivity by ensuring effective and efficient systems ;

3.3.1.2. Appoint an ICT Steering Committee (or equivalent) and determine its terms of reference [Could be the Management Team Sitting with a focus on ICT Matters]; and

3.3.1.3. Ensure implementation of the ICT Policy.

3.3.2. ICT Steering Committee (or equivalent)

3.3.2.1. Shall review and provide ICT policy and strategy of the **<<include the name of the institution>>**;

3.3.2.2. Shall review and provide advice on ICT investment portfolio and priorities;

3.3.2.3. Shall ensure alignment of ICT with the **<<include the name of the institution>>**'s business needs;

3.3.2.4. Shall ensure e-Government guidelines and standards are implemented by the **<<include the name of the institution>>**;

3.3.2.5. Shall ensure continuous monitoring and evaluation of **<<include the name of the institution>>** ICT project;

3.3.2.6. Shall review and approve **<<include the name of the institution>>** disaster recovery plan and ensure its effective implementation;

3.3.2.7. Shall approve any other **<<include the name of the institution>>** e-Government sub-committee as may, from time to time, be constituted and address specific ICT related matters;

3.3.2.8. Shall prepare and submit quarterly Ministerial e-Government progress report to the Authority; and

3.3.2.9. Shall perform such other functions as may be directed by the accounting officer or the Authority.

3.3.2.10. Shall perform such other functions as may be directed by the **<<include the title of the Accounting Officer>>**.

3.3.3. Directors/ Managers/Head of Sections/Units

3.3.3.1.   Shall ensure that all users under their supervision are aware and comply with this policy;

3.3.3.2.   Shall provide adequate and appropriate protection of ICT assets and resources under their control;

3.3.3.3.   Shall ensure availability, integrity and confidentiality of information produced by systems under their areas of functional responsibilities and thereby ensure continuity of operations; and

3.3.3.4.   Shall review and approve procedures, standards, policies and guidelines developed from this policy for the purpose of maintaining business continuity and security of **<<include the name of the institution>>**'s ICT resources.

3.3.3.5.   Shall be custodian of "Data and Information" for their respective Departments/sections/Units.

3.3.4. Head of ICT **<<section/unit/department>>**

Subject to general oversight of **<<board of directors or accounting officer, whichever applies>>** and advice of the ICT Steering Committee, the Head responsible for ICT shall oversee the overall implementation of this policy; and in particular he/she shall;

3.3.4.1.   Coordinate the review and amendment of this policy, as and when required in order to accommodate new technologies or services, applications, procedures and perceived dangers;

3.3.4.2.   Plan and develop ICT Strategy and **<<include the name of the institution>>**'s Enterprise Architecture and ensure its implementation.

3.3.4.3.   Monitor adherence to the ICT Policy and the presence of potential threats and risks by ensuring periodic ICT security reviews are conducted

3.3.4.4.   Keep abreast of ICT developments in respect of ICT industry in General and **<<include the name of the institution>>**'s systems in particular.

3.3.4.5.   Initiate and recommend proposals to change, modify or improve this policy; and

3.3.4.6.   Recommend procedures, standards and policies for effective implementation of this policy in line with e-Government Standards and Guidelines.

3.3.4.7.   Be the custodian of all ICT resources of **<<include the name of the institution>>** including those centrally stored in server room/data centre.

3.3.5. Head of Internal Audit Unit

3.3.5.1.   Shall audit the ICT Function of **<<include the name of the institution>>** and ensure compliancy with the policy.

3.3.6.   Users of ICT Systems

3.3.6.1.   Shall be responsible to safeguard ICT assets of **<<include the name of the institution>>** in their custody.

3.3.6.2.   Shall comply with this policy.

3.4. Monitoring and Evaluation

3.4.1.1.   ICT Steering Committee or equivalent shall meet at least quarterly to monitor and evaluate the achievements in ICT initiatives against **<<include the name of the institution >>**ICT Policy, Strategic Plan and Enterprise Architecture.

4.   GROSSARY AND ACRONYMS

4.1. Glossary

ICT Policy – A document that elaborate on the Public Institution's ICT Management Philosophy by providing general statements of purpose, direction and required activities for the entire ICT Management Framework, commonly known as ICT Policy of an Institution.

4.2. Acronyms

- **CCTV** – Closed Circuit Television
- **ICT** – Information & Communication Technology

5.   RELATED DOCUMENTS

5.1.   ICT Strategy

5.2.   ICT Security Policy

5.3.   ICT Service Management Guidelines

5.4.   Disaster Recovery Plan

5.5.   Acceptable ICT Use Policy

5.6.   ICT Project Management Guidelines

5.7.   ICT Acquisition, Development and Maintenance Guidelines

6.   DOCUMENT CONTROL

VERSION	NAME	COMMENT	DATE
Ver. 1.0	Responsible Section	<<What has been done>>	<<Date>>

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

Sample Name: **ICT Policy**

Sample Reference: **eGAZ/EXT/SMP/006**
Sample Version: **1.0**
Sample Effective Date: **March 2022**
Sample Creation: **Zanzibar e-Government Agency**
Sample Changes: **None**