THE UNITED REPUBLIC OF TANZANIA

PRIME MINISTER’S OFFICE
TANZANIA COMMISSION FOR AIDS (TACAIDS)
ICT POLICY

Publisher

Tanzania Commission for AIDS (TACAIDS)
Nanenane Ground
S. L. P 2904
Dodoma
Phone: (026) 2190600
Email: ed@tacaids.go.tz / info@tacaids.go.tz
Website: www.tacaids.go.tz

ISBN 978-9987-519-33-0

ICT POLICY

Document Controls

Document Title	ICT Policy	Document Storage	TACAID/ICT/Doc/01/2023
Approved By	ACTING EXECUTIVE DIRECTOR	Approved Date	1/July/2023
Approver Name	DR. JEROME KAMWELA	Signature	
Document validity		Permanent Document, Until Major updates	
Document Version		02	

Table of Contents

1. OVERVIEW

1.1. Introduction

The trend towards a knowledge-based economy has emphasized the importance of ICT in development efforts at Tanzania Commission for AIDS (TACAIDS). This shift requires a well-developed technology investment plan and intelligent deployment and maintenance management.

For TACAIDS to realize the value of ICT investment, ICT must be deployed to improve efficiency and effectiveness in internal and external service delivery. This means that a comprehensive framework established by ICT Policy to provide appropriate directives to harness ICT is necessary for the achievement of TACAIDS objectives.

The establishment of an ICT Policy is an important step toward ensuring that ICT will assist TACAIDS to attain its objectives. The ICT Policy will ensure that the ICT infrastructure and capacity are utilized effectively and are in alignment with the TACAIDS strategic objectives, National ICT Policy, National e-Government Strategy, and e-Government Standards and Guidelines.

TACAIDS needs to meet its objective of improving its services and increasing the level of service delivery by leveraging new technologies. TACAIDS has been investing in ICT to facilitate its internal business operations to attain its strategic goals. TACAIDS operations are increasingly dependent on ICT, making the Institution vulnerable to ICT-related risks. In this regard, it is evident that TACAIDS needs to develop and operationalize a comprehensive ICT Policy to direct ICT adoption and usage within the Institution.

1.2. Purpose

This document provides the highest-level ICT directives for TACAIDS. The main purpose of this document is to ensure that TACAIDS 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 an integral part of institutional governance.

ii. ICT services provisions are in line with TACAIDS business requirements based on existing e-Government standards and best practices.

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

iv. To ensure the members of the Institution use ICT facilities and services appropriately and responsibly and to ensure that other persons do not misuse those ICT facilities and services.

1.3. Scope

This policy applies to all TACAIDS staff and its associates, all users of ICT equipment owned or leased by the Commission as well as all equipment connected to TACAIDS ICT-related infrastructure. This policy applies to all TACAIDS 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, organizational structures, and processes that ensure that the organization's ICT sustains and extends the organization'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 the context of TACAIDS strategic directions. 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 enterprise and has strong accountability.

2.1.1. ICT Processes and Organization

2.1.1.1. TACAIDS will set up an ICT governance model so that it has 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 to determine the prioritization of ICT-enabled investment programmed in line with the Institution's business strategy and priorities, track the status of ICT initiatives, resolve resource conflicts, and monitor ICT services.

2.1.1.3. TACAIDS shall establish a strong ICT unit capable of supporting the strategic objectives of the institution.

2.1.1.4. TACAIDS shall ensure that ICT strategic plan and Enterprise Architecture are established and operationalized.

2.1.1.5. TACAIDS shall ensure that ICT plans fit the current and ongoing needs of the institution and that the ICT plans support the commission's strategic plans.

2.1.1.6. TACAIDS shall ensure that ICT Risk Management is 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. TACAIDS shall ensure that individuals and groups within the Institution understand and accept their responsibilities for ICT.

2.1.2.2. TACAIDS shall ensure that clear and well-understood contracts exist for external suppliers.

2.1.2.3. TACAIDS 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. TACAIDS 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. TACAIDS shall ensure that ICT acquisitions are made for approved reasons in an approved way; based on appropriate and ongoing analysis.

2.1.3.3. TACAIDS shall ensure that there is an appropriate balance between costs, risks, and long-term and short-term benefits.

2.1.4. ICT Performance Management

2.1.4.1. TACAIDS shall ensure that ICT is fit for its purpose in supporting the Institution, and is kept responsive to changing business requirements.

2.1.4.2. TACAIDS shall ensure that ICT Services are defined, e.g. Email services, and printing services.

2.1.4.3. TACAIDS shall establish a mechanism for evaluating and monitoring ICT services (E.g. Service availability, staff satisfaction/feedback system).

2.1.5. Conformance

2.1.5.1. TACAIDS shall ensure that ICT conforms to e-Government standards, guidelines, and all external regulations and complies with all internal policies, 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. TACAIDS shall ensure that ICT conforms to the Government ICT projects management procedures and complies with all internally developed procedures for managing projects.

2.1.6.2. TACAIDS 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. TACAIDS management will implement the necessary controls to ensure that all ICT procurements are done in line with the requirements of the Public Procurement Act (PPA)

2.1.7.2. User Departments shall Consult ICT Unit in regard of requirements specifications before submitting their purchase requests to Management Procurement Unit.

2.1.7.3. ICT Unit shall ensure that all requirements for ICT procurements comply with e-Government Standards and Guidelines.

2.2. ICT Infrastructure

ICT infrastructure is the backbone for supporting the TACAIDS 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, laptops, storage, backup, operating facilities, and supporting platforms like operating systems and databases.

The objective of managing ICT Infrastructure is to ensure that the TACAIDS ICT infrastructure operations are optimized to deliver high-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. TACAIDS shall ensure that ICT infrastructure architecture is in place and align with the Institution's current and future requirements.

2.2.1.2. TACAIDS shall ensure that appropriate ICT infrastructure is set up and well managed.

2.2.2. Data Management and Storage

2.2.2.1. TACAIDS shall ensure that all business-related data shall be stored in a way to facilitate backup procedures and access.

2.2.3. ICT Equipment and Hosting

2.2.3.1. TACAIDS shall acquire desktop computers, laptops, servers' printers

and networking equipment from authorized suppliers.

2.2.3.2. All ICT resources shall be acquired in consultation with ICT Unit.

2.2.3.3. TACAIDS shall ensure that an appropriate environment for hosting computing and storage equipment based on standards and best practices is established.

2.2.4. Infrastructure Maintenance and Support

2.2.4.1. TACAIDS shall ensure that all ICT infrastructure components are maintained at a reasonable operational and secure level.

2.2.4.2. TACAIDS shall ensure that a standard software list including the operating system to be installed into the Institution's equipment is established.

2.2.4.3. TACAIDS shall procure maintenance services from an organization that has technical capabilities.

2.2.4.4. TACAIDS shall ensure that maintenance services are procured in consultation with ICT Unit.

2.3. Applications

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

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

i. To ensure the system acquired follow proper procedures;

ii. To establish controls for the 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 Unit their ICT requirements to be included in the ICT resource budget.

2.3.1.3. All applications supplied shall be checked by ICT Unit to verify whether the technical requirements established are met and approved.

2.3.1.4. ICT Unit shall establish appropriate software standards to facilitate acquisition/development.

2.3.1.5. ICT Unit 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 ongoing process that will last throughout the life cycle of the application.

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

2.3.2.3. Installation of additional applications or overriding existing ones shall follow change management procedures.

2.3.2.4. Software acquired for installation into the Institute equipment shall be licensed.

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 stakeholders' 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 and Support

2.4.1.1. TACAIDS shall operate an ICT service and support function, which will ensure that business disruptions are minimized, 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 TACAIDS shall ensure that for every ICT service provided, Service Level Agreements between the providers and the recipients are established.

2.4.2.2 TACAIDS shall ensure that reports on service quality are reviewed periodically with customers to determine things that could be added or changed to improve service delivery and support.

2.4.3 Management of Third Party Services

2.4.3.1 TACAIDS shall ensure proper processes and procedures for managing vendors are in place.

2.4.2.1. TACAIDS shall ensure that services procured from third parties (suppliers, vendors, and partners) meet business requirements.

2.4.2.2. TACAIDS 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 TACAIDS 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.

2.4.2.3. TACAIDS shall ensure that the ICT service catalog is prepared and approved.

2.4.2.4. TACAIDS shall ensure that Service Requests and Incidents Management processes and procedures are established to ensure minimal adverse impacts on customers.

2.4.2.5. TACAIDS management shall review all reports about problems that resulted in systems downtime to identify the root causes of problems.

2.4.5 Change Management

2.4.2.6. TACAIDS shall ensure that a process for recording, assessing, and authorizing all changes before implementation, including changes in procedures, processes, systems, and service parameters is established.

2.4.3. ICT Service Availability

2.4.3.1. TACAIDS shall implement an availability management process to ensure that services are available when needed, and as defined in approved Service Level Agreements.

2.4.4. ICT Service Continuity

2.4.4.1. TACAIDS shall conduct a Business Impact Analysis to identify critical business functions to be supported by ICT.

2.4.4.2. TACAIDS shall ensure that robust business continuity and service recovery plans are in place, that these plans are regularly reviewed and tested, and that key staffs are appropriately trained.

2.4.5. Configuration Management

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

2.4.6. Capacity Management

2.4.6.1. TACAIDS shall establish a capacity plan to monitor ICT resource usage for existing and planned systems to assist in the time and cost-effective purchase of additional resources to avoid panic purchases when resources run out.

2.4.7. Data Management

2.4.7.1. TACAIDS business requirements for data management shall be determined and data shall conform to the Government data and metadata standards.

2.4.7.2. TACAIDS 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 TACAIDS with an information security mechanism to support the Institution to achieve its strategic goals based on best practices. The specific objectives are:

i. Protection of the TACAIDS ICT resources from accidental or malicious activity while preserving the open information sharing requirements of the Government; and

ii. Making the TACAIDS stakeholders aware of their responsibilities concerning ICT security.

2.5.1. ICT Security Management

2.5.1.1. TACAIDS 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. TACAIDS shall ensure information systems are designed, acquired, and implemented with effective ICT security controls to safeguard 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 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.

2.5.1.4. All users of TACAIDS systems shall be responsible for protecting the institution’s information resources.

2.5.1.5. TACAIDS shall retain overall responsibility and ownership for all Institution’s information assets.

2.5.2. Monitoring

2.5.2.1. TACAIDS will monitor the 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. TACAIDS will maintain its ICT environment so that it remains running 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 its first page, and then shall be considered mandatory for all TACAIDS business operations.

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

3.1.3. TACAIDS 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 authorized users of TACAIDS shall comply with the requirements of this policy.

3.1.5. The head responsible for ICT shall enforce compliance by using audit trails and triggering access denial to TACAIDS systems and networks.

3.1.6. TACAIDS staff found to have violated this policy may be subject to withdrawal and or suspension of systems and network privileges or disciplinary action following rules defined by TACAIDS administrative regulations.

3.1.7. This document shall be reviewed within three years, or whenever the business environment of TACAIDS 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 followed through a proper channel of authorization using the same authority which approved this document.

3.3. Roles and Responsibilities

3.3.1. Executive Director

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

3.3.1.2. Appoint an ICT Steering Committee and other sub committees and determine its terms of reference; and

3.3.1.3. Ensure implementation of the ICT Policy.

3.3.2. ICT Steering Committee

3.3.2.1. Shall propose TACAIDS ICT Policy for the consideration of the ED.

3.3.2.2. Shall coordinate the establishment and continuos review of TACAIDS ICT Policy, ICT Strategy, and Enterprise Architecture;

3.3.2.3. Shall ensure that the ICT Strategy is aligned with TACAIDS ‘s Corporate Plan;

3.3.2.4. Shall advise the Executive Director in making considered decisions about the focus of ICT resources;

3.3.2.5. Shall approve review of all ICT services and applications including the TACAIDS website and infrastructure with the view to advise TACAIDS on required improvements; and

3.3.2.6. Shall ensure that risks associated with ICT are managed appropriately.

3.3.3. Directors/Head of Sections/Units

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

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

3.3.3.3. Shall ensure compliance with procedures, standards, policies and guidelines developed from this policy for maintaining business continuity and security of TACAIDS ICT resources.

3.3.3.4. Shall be the custodian of Data and Information for their respective Departments/sections/Units.

3.3.4. Head of ICT Unit

Subject to general oversight of the ED 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. Shall ensure that all TACAIDS staff are capacitated and being aware of this policy;

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

3.3.4.3. Plan and develop ICT Strategy and TACAIDS Enterprise Architecture and ensure its implementation.

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

3.3.4.5. Keep abreast of ICT developments in respect of the ICT industry in General and TACAIDS systems in particular.

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

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

3.3.4.8. Be the custodian of all ICT resources of TACAIDS including those centrally stored in the Server room/Government Data Centre.

3.3.5. Users of ICT Systems

3.3.5.1. Shall be responsible to safeguard the ICT assets of TACAIDS in their custody.

3.3.5.2. Shall comply with this policy.

3.4. Monitoring and Evaluation

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

4. GLOSSARY AND ACRONYMS

4.1. Glossary

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, commonly known as the ICT Policy of an Institution.

4.2. Acronyms

- **CTV** – Closed Circuit Television
- **ED** – Executive Director
- **ICT** – Information and Communication Technology
- **TACAIDS** – Tanzania Commission for AIDS

5. RELATED DOCUMENTS

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