THE UNITED REPUBLIC OF TANZANIA
INSTITUTE OF ADULT EDUCATION

ICT POLICY

December, 2020

UNITED REPUBLIC OF TANZANIA

INSTITUTE OF ADULT EDUCATION

ICT POLICY

December, 2020

THE UNITED REPUBLIC OF TANZANIA				
Institute of Adult Education	**ICT Policy**			
	Number: **IAE/NA.246/597/114**			

PPROVAL	Name	Job Title	Signature	Date
Approved by	Dr. Michael W. Ng'umbi	Director		Dec, 2020

Table of Contents

1.0 OVERVIEW

1.1 Introduction

The trend towards a knowledge-based economy has emphasized the importance of ICT in development efforts in Adult Education and Community Development sector. This shift requires a well-developed technology investment plan and intelligent deployment and maintenance management.

For Institute of Adult Education (IAE) 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 IAE's objectives.

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

1.2 Rationale

The Institute of Adult Education needs to meet its objective of improving its services and increasing productivity by leveraging on new technologies. IAE has been investing in ICT to facilitate its internal business operations so as to attain its strategic goals. Its operations are increasingly depending on ICT, making the Institution vulnerable to ICT related risks. In this regard, it is evident that, IAE 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 IAE. The main purpose of this document is to ensure that IAE's ICT related investments, operations and maintenance processes and usage are well directed. Thus, the specific objectives of this policy are to ensure that;

i) ICT governance is integral part of the institutional governance.

ii) ICT services provisions are in line with IAE'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) Members of the Institution use ICT facilities and services in an appropriate and responsible manner and that other persons do not misuse the facilities and services.

1.4 Scope

This policy is applicable to all IAE staff and its associates, all users of ICT equipment owned or leased by the Institution as well as all equipment connected to IAE's ICT related infrastructure. This policy applies to all IAE'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 IAE 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 There shall be an ICT Steering Committee to determine prioritisation of ICT-enabled investment programmes in line with the IAE Rolling Strategic Plan (RSP).

2.1.1.2 IAE shall establish a strong ICT department/unit capable of supporting strategic objectives of the institution.

2.1.1.3 IAE 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.

2.1.1.4 IAE 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 IAE shall ensure that individuals and groups within the Institution understand and accept their responsibilities for ICT.

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

2.1.2.3 IAE shall ensure that ICT policy and related documents are known and adhered to by staff.

2.1.3 ICT Resources Management

2.1.3.1 IAE 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 IAE 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 IAE 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 IAE shall ensure that ICT is fit for its purpose in supporting the changing business requirements.

2.1.4.2 IAE shall ensure that ICT Services are defined, e.g. Email services, Printing services.

2.1.4.3 IAE 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 IAE shall ensure that ICT conforms to eGovernment 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 IAE 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 IAE shall 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 IAE management shall implement the necessary controls to ensure that all ICT procurements are done in line with requirements of Public Procurement Act (PPA)

2.1.7.2 User Departments shall establish and submit, in writing, any ICT related requirement weather ad-hoc or planned, to ICT Unit who will provide technical advice prior to procurement processes.

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

2.1.7.4 Procurement unit shall not procure any ICT System, Service, Equipment, Consumable or Accessory without consultation with ICT Unit.

2.2 ICT Infrastructure

ICT infrastructure is the backbone for supporting the IAE 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 IAE 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.

2.2.1.1 **Infrastructure Planning and Design**

2.2.1.1 IAE shall ensure that ICT infrastructure is in line with the Institution's current and future requirements.

2.2.1.2 IAE shall ensure that appropriate ICT infrastructure is setup and well managed.

2.2.2   Data Management and Storage

2.2.2.1 IAE shall ensure that all official data are stored and back up maintained.

2.2.3   ICT Equipment and Hosting

2.2.3.1 The IAE shall acquire desktop computers, laptops, servers, printers, networking equipment and other ICT facilities from authorized suppliers.

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

2.2.3.3 IAE shall ensure that hosting and storage systems and equipments is done based on acceptable standards and best practices.

2.2.4   Infrastructure Maintenance and Support

2.2.4.1 IAE shall ensure that all ICT infrastructure components are maintained at reasonable and secure operational environment.

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

2.2.4.3 IAE shall procure maintenance services from an authorized organization with technical capabilities.

2.2.4.4 IAE 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 the Institute's operational processes.

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

2.3.1 Applications Acquisition and Deployment

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

2.3.1.2 User departments shall consult ICT Unit regarding their system requirements for specifications outline and budgeting purposes

2.3.1.3 All applications supplied shall be checked by ICT Unit to verify if specifications established are met.

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

2.3.1.5 ICT Unit shall ensure appropriate configuration to systems 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 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 eGovernment Standards and Guidelines relating to the ICT Service Management.

2.4.1 Management of Service Levels

2.4.1.1 IAE shall ensure that for every ICT service outsourced, a Service Level Agreement or Contract between the providers and the Institute is established.

2.4.1.2 IAE shall ensure that issues raised by users on service quality are reviewed periodically in order to determine things that could be improved in service delivery and support.

2.4.2 ICT Service Requests, Incidents and Problems Management

2.4.2.1 IAE shall set up a contact service point for end users where issues will be reported to, recorded and resolved as quickly as possible.

2.4.2.2 IAE shall ensure that ICT service catalogue is prepared and approved.

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

2.4.2.4 IAE management shall review all reports about problems that resulted to systems downtime in order to identify root causes of problems.

2.4.3 Change Management

2.4.3.1 IAE 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.

2.4.4   ICT Service Availability

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

2.4.5   ICT Service Continuity

2.4.5.1 IAE shall conduct a Business Impact Analysis to identify critical Business functions to be supported by ICT.

2.4.5.2 IAE shall ensure ICT service continuity and data recovery plans.

2.4.5.3 IAE shall ensure that data recovery plans are regularly reviewed and tested and key staff are appropriately trained.

2.4.6   Data Management

2.4.6.1 IAE 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 IAE 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 Institute's ICT resources from accidental or malicious act while preserving the open information sharing requirements of the Government; and

ii) Making the Institute's stakeholders aware of their responsibilities with respect of ICT security.

2.5.1 ICT Security Management

2.5.1.1 IAE 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 IAE 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 highlighting 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 IAE systems shall be responsible for protecting the institute's information resources.

2.5.1.5 IAE shall retain overall responsibility and ownership for all Institution's information assets.

2.5.2 Monitoring

2.5.2.1 IAE 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 IAE 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 approved by the ICT Steering Committee of the Institute. The approved document, once signed by the Committee Chairperson shall be considered mandatory for all IAE business operations.

3.1.2 All employees and other authorised users of IAE shall comply with requirements of this policy.

3.1.3 The head responsible for ICT shall enforce compliancy by using audit trails and triggering access denial to IAE systems and networks.

3.1.4 IAE 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 IAE administrative regulations.

3.1.5 This document shall be reviewed within three years, or whenever business environment of IAE 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 IAE Director

3.1.1 Shall 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;

3.3.1.1 Appoint an ICT Steering Committee and determine its terms of reference [the Committee could be the Management Team Sitting with a focus on ICT Matters]; and

3.3.1.2 Ensure implementation of the ICT Policy.

3.3.2 ICT Steering Committee

3.3.2.1 Shall coordinate the establishment of, review and approve IAE's ICT Policy and other related documents;

3.3.2.2 Shall ensure that the ICT Strategy is aligned with IAE's Corporate Plan;

3.3.2.3 Shall advice the Managing Council of the Institute in making appropriate decisions regarding ICT infrastructure of IAE;

3.3.2.4 Shall review all ICT services and applications including IAE's website and infrastructure with the view to advice the Institute on required improvements; and

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

3.3.3   IAE Management Members

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 IAE's ICT resources.

3.3.3.5 Shall be custodian of "Data and Information" for their respective administrative areas.

3.3.4   Head of ICT Unit

Subject to directives from the IAE Director and advice from the ICT Steering Committee, the Head of ICT Unit 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 Monitor adherence to the ICT Policy and the presence of potential threats and risks by ensuring periodic ICT security reviews are conducted

3.3.4.3 Keep abreast of ICT developments in respect of ICT industry in General and IAE's systems in particular.

3.3.4.4Initiate and recommend proposals to change, modify or improve this policy; and

3.3.4.5Recommend procedures, standards and policies for effective implementation of this policy in line with eGovernment Standards and Guidelines.

3.3.4.6Be the custodian of all ICT resources of the Institute including those centrally stored in server room(s) and data centre(s).

3.3.5   Head of Internal Audit Unit

3.3.5.1Shall audit the ICT Function of the Institute and ensure compliancy with the policy.

3.3.6   Users of ICT Systems

3.3.6.1Shall be responsible to safeguard ICT assets of the Institute in their custody.

3.3.6.2Shall comply with this policy.

3.4 Monitoring and Evaluation

3.4.1.1ICT Steering Committee shall meet at least quarterly to monitor and evaluate the achievements in ICT initiatives against IAE Rolling Strategic Plan (RSP).

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

· IAE – Institute of Adult Education

5. RELATED DOCUMENTS

5.1 e-Government Act, 2019

5.2 Guidelines for operationalization of Institutional ICT Steering Committees

5.3 The e-Government General Regulations, 2020

6. PARTICULARS

VERSION	DEPARTMENT/ UNIT	COMMENT	Date
Ver. 2.0	ICT Unit	ICT Policy Review	30th Dec. 2020