



UNITED REPUBLIC OF TANZANIA
MINISTRY OF EDUCATION, SCIENCE AND TECHNOLOGY
MOSHI CO-OPERATIVE UNIVERSITY (MoCU)
CHUO KIKUU CHA USHIRIKA MOSHI



INFORMATION AND COMMUNICATION TECHNOLOGY
POLICY AND GUIDELINES

THIRD EDITION

APRIL, 2026

FOREWORD

Moshi Co-operative University (MoCU) was established in 2014 following the upgrading of the then Moshi University College of Co-operative and Business Studies (MUCCoBS). The University formulated its first Information and Communication Technology Policy in 2015 to provide guidance on the identification, promotion, and effective use of ICT services and products. The policy aimed at ensuring that ICT applications are systematically integrated into academic, research, consultancy and administrative functions of the university. The issues covered in the Policy were mainly pertained to ICT infrastructure development, connection to and usage of ICT facilities, software development, procurement of ICT tools, facilities and services, ICT training, Website Contents as well as ICT security and Internet. The 2015 policy was revised in 2019.

Nevertheless, since then, significant changes have taken place at national, regional and international levels. Changes in technologies, structures and processes have impacted the development and usage of ICT at the University. Pursuant to that, the need arises to review and update the ICT Policy to accommodate the new developments and help the University to implement its mandated functions. The revised Policy has captured various issues related to ICT governance, ICT infrastructure and facilities, applications, ICT service management and ICT security.

It is anticipated that this Policy will guide the University towards its Vision to become an eminent academic institution committed to supporting co-operative and business development. It is the responsibility of every member of the university to adhere to this ICT Policy and Guidelines to meet the envisioned dream.

Prof. Alfred Said Sife

VICE CHANCELLOR

TABLE	OF	CONTENTS
FOREWORD		i
TABLE OF CONTENTS		ii
LIST OF ABBREVIATION AND ACRONYMS		v
INTERPRETATIONS		vi
PART ONE:		1
POLICY FRAMEWORK		1
1.1 Background Information		1
1.2 University Vision, Mission and Core Values		1
1.2.1 Vision		1
1.2.2 Mission		2
1.2.3 Core Values		2
1.2.4 Motto		2
2.0 POLICY JUSTIFICATION, OBJECTIVES AND GUIDING PRINCIPLES		3
2.1 Justification for Policy Review		3
2.2 Situational analysis		4
2.3 Policy Objectives		5
2.3.1 Main Objective		5
2.3.2 Specific Objective		5
2.4 Guiding Principles		5
2.5 Scope of the Policy and Guidelines		6
2.6 Rationale for the ICT Policy and Guidelines		6
3.0 POLICY ISSUES, STATEMENTS, AND STRATEGIES		8
3.1 ICT Governance		8
3.1.1 Policy Statement		8
3.1.2 Policy Strategies		8
3.2 ICT Infrastructure and Facilities		8
3.2.1 Policy statement		9
3.2.2 Policy Strategies		9

3.3 Applications	9
3.3.1 Policy statement	10
3.3.2 Policy Strategies	10
3.4 ICT Service Management	10
3.4.1 Policy statement	10
3.4.2 Policy Strategies	10
3.5 ICT Security	11
3.5.1 Policy statement	11
3.5.2 Policy Strategies	11
3.6 ICT Innovations.....	12
3.6.1 Policy statement	12
3.6.2 Policy Strategies	12
3.7 Systems Integration	13
3.7.1 Policy statement	13
3.7.2 Policy Strategies	13
PART TWO:.....	14
POLICY GUIDELINES	14
4.1 ICT Governance, Risk and Compliance.....	14
4.2 ICT Systems, Infrastructure and Facilities	14
4.3 ICT Service Management and Operations.....	15
4.4 ICT Security and Data Protection	15
5.0 ROLES OF STAKEHOLDERS IN MANAGING ICT RELATED ACTIVITIES	16
5.1 ICT Steering Committee	16
5.2 Dean/Directors/Head of Departments/Section/Units	16
5.3 Department of ICT Services.....	16
5.4 Internal Audit Unit	17
5.5 Quality Assurance Unit	17
5.6 Users	17
5.7 Conformance	17

6.0 MONITORING AND EVALUATION	18
6.1 Monitoring.....	18
6.2 Evaluation.....	18
7.0 OPERATION AND REVIEWS.....	20
7.1 Operational Date.....	20
7.2 Policy Review	20

LIST OF ABBREVIATION AND ACRONYMS

AI	:	Artificial Intelligence
CCTV	:	Close Circuit Television
DVC-PFA	:	Deputy Vice Chancellor - (Planning, Finance and Administration)
e-GA	:	Electronic Government Authority
E-learning	:	Electronic Learning
EAC	:	East African Community
ICT	:	Information and Communication Technology
ICTS	:	ICT Services
IP	:	Intellectual Property
KPI	:	Key Performance Indicator
KICoB	:	Kizumbi Institute of Co-operative and Business Education
MoCU	:	Moshi Co-operative University
MUCCoBS	:	Moshi University College of Co-operative and Business Studies
SDGs	:	Sustainable Development Goals
SDLC	:	Software Development Life Cycle
SLA	:	Service Level Agreements

INTERPRETATIONS

In this policy and guidelines, unless the context requires otherwise;

- “Applications”** means software designed for end users to use in their daily operations to support the enterprise business processes.
- “e-Learning platform”** means online system that enables the delivery, management, and access of educational content and learning activities over the internet.
- “ICT Steering Committee”** means a governance body responsible for providing strategic oversight on ICT investment portfolio and priorities and alignment of ICT with the University’s goals, ensuring and continuous monitoring and evaluation of the University’s ICT initiatives and projects
- “Infrastructure and Facilities”** means physical equipment, digital systems and networks that enable the use, management and delivery of ICT services within the University.
- “Open-source software”** means software whose source code is freely available for anyone to use.
- “University community”** means all individuals affiliated with the University, including students, staff and other authorized users of University’s ICT resources and services.
- “University”** means Moshi Co-operative University, which includes Kizumbi Institute of Co-operative and Business Education and regional offices.
- “Service Level Agreements”** means a documented contract between ICT service providers and the University as well as defined level of service, including performance metrics and responsibilities between the department responsible for ICT Services and the University
- “Change Management”** means approach taken to allow smooth transition of users of ICT services at the University from a current state to a desired future state.
- “ICT Assets”** means the hardware, software, and network components that support the University functions, including computers, servers, mobile devices, and applications

“Social media”

means a collection of web and mobile applications that allow the University community to connect, create, and share content such as text, photos, and videos within and outside the University community.

PART ONE:

POLICY FRAMEWORK

1.1 Background Information

The history of the Moshi Co-operative University (MoCU) dates way back to 5th January, 1963 when the then Co-operative College Moshi was established. The College's primary responsibility was training of human resources in the co-operative sector under the then Ministry of Co-operatives and Community Development. The College was subsequently established through the Co-operative College Act No. 32 (Repealed) of 1964 as an autonomous institution with its own Governing Board. In 2004, the Co-operative College Moshi was transformed into the Moshi University College of Co-operative and Business Studies (MUCCoBS), a Constituent College of Sokoine University of Agriculture, through the Government Declaration Order No. 22 of 2004. MoCU came into being as a result of transforming Moshi University College of Co-operative and Business Studies (MUCCoBS) to a full-fledged University in September, 2014. The University is governed by its own Charter, made under the Universities Act No. 7 of 2005 (Cap 346) of Tanzania laws.

MoCU is located in Moshi Municipality, on the foot of Mount Kilimanjaro along Sokoine Road. MoCU has a teaching centre located in Shinyanga Region along Tabora Road, namely Kizumbi Institute of Co-operative and Business Education (KICoB). In addition, the University operates 13 Regional Offices catering for all the regions in Tanzania Mainland. These offices are located in Mtwara (serving Mtwara and Lindi Regions), Mbeya (serving Mbeya, Katavi and Rukwa), Kilimanjaro (serving Kilimanjaro, Arusha and Manyara Regions), Shinyanga (serving Shinyanga and Simiyu Regions), Mwanza (serving Mwanza, Geita and Kagera), Iringa (serving Iringa and Njombe Regions), Dodoma (serving Dodoma and Morogoro Regions), Coast (serving Coast, Dar-es-Salaam and Zanzibar), Singida, Ruvuma, Tanga, Tabora and Kigoma.

In recognition of the central role that Information and Communication Technology (ICT) plays in enabling the University's academic, research, consultancy, and administrative functions, MoCU formulated its first ICT Policy in 2015. The Policy was developed to provide a guiding framework for the identification, promotion, acquisition, and effective utilisation of ICT services and resources across the University. It established the basis for systematically integrating ICT across all institutional operations, covering areas such as ICT infrastructure development, access to and use of ICT facilities, software development and procurement, ICT training, website content management, and ICT security and internet governance.

The first ICT Policy was revised in 2019 to reflect the developments and emerging needs of the University at that time. However, since then, significant changes have continued to take place at national, regional, and international levels. Rapid advancements in technology including cloud computing, data analytics, cybersecurity, and artificial intelligence together with changes in

institutional structures, service delivery models, and regulatory requirements, have considerably influenced the development and use of ICT Services within the University.

As a result of these developments, several gaps have emerged in the existing ICT framework. These include limited systems integration and interoperability, inadequate data management and security practices, insufficient ICT governance and service management mechanisms, and emerging constraints on users' capacity to adopt new technologies. In addition, evolving national frameworks including e-Government standards and digital transformation agendas require institutional compliance and alignment.

It is against this background that the University has undertaken a comprehensive review and update of its ICT Policy, resulting in this Third Edition (2026). The revised ICT Policy and Guidelines address seven key policy areas: ICT Governance, ICT Infrastructure and Facilities, Applications, ICT Service Management, ICT Security, ICT Innovations, and Systems Integration. The Policy is aligned with the National ICT Policy 2023, the Tanzania Digital Economy Framework, the e-Government Authority (e-GA) standards, the African Union Digital Transformation Strategy (2020–2030), and global frameworks such as the Sustainable Development Goals (SDGs), particularly SDG 4 (Quality Education) and SDG 9 (Industry, Innovation and Infrastructure).

1.2 University Vision, Mission and Core Values

1.2.1 Vision

To be an eminent academic institution committed to supporting co-operative and business development.

1.2.2 Mission

To promote sustainable co-operative and business development through quality training, research, and advisory services.

1.2.3 Core Values

Cooperation, objectivity, pursuit of excellence in service delivery, integrity, accountability, courtesy to all, and social responsibility.

1.2.4 Motto

The motto of the University is "Ushirika ni Biashara".

2.0 POLICY JUSTIFICATION, OBJECTIVES AND GUIDING PRINCIPLES

2.1 Justification for Policy Review

The use of ICT at the University is increasing in response to the demand of students, staff and other stakeholders. As a result, the University has invested in a strong ICT base, which supports teaching, learning, research, outreach and administration. It is for this reason that the University has taken initiatives to develop the ICT policy to guide the design, development, implementation, and effective utilization of ICT infrastructure and services. The first ICT Policy was developed in 2015 and revised in 2019.

However, since then, significant developments have taken place at national, regional, and international levels. Rapid advancements in technology including cloud computing, data analytics, cybersecurity and artificial intelligence; together with changes in institutional structures, service delivery models and regulatory requirements, have considerably influenced the development and use of ICT within the University.

As a result of these developments, several gaps have emerged. The gaps include fragmented ICT infrastructure, limited systems integration and interoperability, inadequate data management and security practices, insufficient ICT governance and service management mechanisms, weak alignment between ICT investments and institutional priorities, and emerging constraints on users' capacity to adopt new technologies. In addition, evolving national frameworks, including e-Government standards and digital transformation agendas, require institutional compliance and alignment.

Considering these developments and gaps, it has become necessary to review and update the ICT Policy to reflect current and emerging technological trends, strengthen governance and security, enhance service delivery, and support innovation and digital transformation across the University. The revised ICT Policy and Guidelines covering seven (7) policy issues shall, therefore, focus on strengthening institutional capacity, improving efficiency of ICT systems and supporting the advancement of teaching, learning, research, outreach services and innovation in line with the University's mandate.

2.2 Situational analysis

Moshi Co-operative University (MoCU) has a strong foundation of expertise that supports the development and use of ICT within the institution. The University hosts professionals in diverse fields, including information technology, finance, banking, law, co-operation, marketing, and procurement and supply management. This multidisciplinary capacity provides an enabling environment for integrating ICT into teaching, learning, research, consultancy, and administrative functions. In addition, the University operates through various centres across Tanzania, creating the need for reliable ICT systems to enhance communication, coordination, and service delivery.

As a recognized centre of excellence in co-operative and business management training within the East African Community (EAC), MoCU has accumulated more than 55 years of experience in training, research, and consultancy within and outside Tanzania. The University also maintains collaborative links with higher learning institutions and experts locally and internationally. These networks provide opportunities for knowledge sharing, technological collaboration, and capacity building which can be easily fostered through ICT development and application.

Despite these strengths, the effective utilization of ICT at the University faces several challenges, including limited ICT infrastructure, variations in digital literacy among staff and students, and the need to modernize existing systems to match rapid technological developments. At the same time, the increasing digital transformation of higher education presents opportunities for the University to expand the use of e-learning platforms, digital libraries, electronic learning resources and various information systems.

Given these opportunities and challenges, there is a need to review and strengthen the ICT Policy to guide the strategic development, management, and effective utilization of ICT in supporting the University's core functions and goals as stipulated in the Corporate Strategic Plan.

2.3 SWOT Analysis

A SWOT analysis was conducted to assess the internal and external factors influencing ICT development and utilization at the University. The analysis informed the policy review process and provides the basis for the strategic directions adopted in this Policy.

STRENGTHS	WEAKNESSES
• Comprehensive coverage of twelve ICT policy areas • Clear implementation strategies defined for each policy area • Wide scope covering staff, students, contractors and outsourced providers • Dedicated provisions for inclusive access for people with special needs • Defined enforcement mechanisms with graduated consequences • Alignment with National ICT Policy 2016, Vision 2025 and SDGs	• No ICT governance body to oversee strategic alignment and investments • No systems integration or interoperability provisions • No data protection and privacy framework • No Service Level Agreements or service performance monitoring • No provisions for cloud computing, AI or data analytics • ICT innovation and digital entrepreneurship not addressed
OPPORTUNITIES	THREATS
• Expansion of e-learning and digital library services • Growing national digital transformation and e-Government agenda • Increasing availability of open-source and affordable ICT solutions • Regional and international networks for ICT collaboration and benchmarking • Rising demand for ICT skills is driving structured capacity building	• Evolving cybersecurity threats beyond the scope of 2019 security provisions • Rapid technological obsolescence outpacing maintenance guidelines • Data privacy risks from the absence of a data governance framework • Emergence of Artificial Intelligence and cloud computing without governance guidance • Vendor dependency with inadequate contract and performance management

2.4 Policy Objectives

2.4.1 Main Objective

The main objective of this policy is to ensure effective ICT services to support the University's teaching, learning, research, consultancy, and administrative activities.

2.4.2 Specific Objective

The following are the specific objectives of the revised ICT Policy and procedures;

- (i) To establish an ICT governance environment that ensures strategic alignment, effective oversight, and informed decision making for optimal utilisation of ICT resources;
- (ii) To develop a reliable and scalable ICT infrastructure and facilities environment capable of supporting systems and evolving institutional needs;
- (iii) To achieve a standardized and coordinated application ecosystem which ensure proper software development and acquisition;
- (iv) To establish a responsive and efficient ICT service management environment that ensures quality and reliable delivery of ICT services;
- (v) To establish a secure ICT environment that safeguards institutional information, ensures system integrity and availability and supports continuous institutional operations;
- (vi) To enhance the University's capacity for ICT-driven innovation; and
- (vii) To improve interoperability and information exchange across institutional systems.

2.5 Guiding Principles

All ICT undertakings at the university shall be governed by the following principles:

- (i) ICT initiatives and investments shall align with the University's vision, mission, and strategic objectives to support teaching and learning, research, consultancy, and administrative activities;
- (ii) ICT resources shall be used to enhance operational efficiency, improve service delivery, and ensure value for money;
- (iii) The University shall promote the adoption of emerging technologies and continuous improvement of ICT services to support institutional development;
- (iv) ICT users have a responsibility of ensuring safety and care of the ICT facilities; and

- (v) Users have a duty of reporting to the relevant authority any mishandling, damage, theft, tempering or any other act which is detrimental to the wellbeing of the ICTS department.
- (vi) The use of Artificial Intelligence (AI) within the University shall be guided by principles of ethical use, transparency, accountability, and compliance with institutional policies and applicable regulations.
- (vii) The use of AI in academic work and official documents shall adhere to established guidelines and restrictions, including appropriate disclosure, avoidance of academic misconduct and respect for intellectual property rights.

2.6 Scope of the Policy and Guidelines

This policy applies to any person accessing, developing, implementing and/or using ICT-based information and resources owned, managed, supported or operated by, or on behalf of, the University. These include all University staff and students; any other organizations accessing services using the University ICT resources; persons contracted to develop, repair or maintain the University's ICT resources; and suppliers of outsourced ICT services and any other relevant parties when accessing, interacting or using ICT equipment, software or other facilities owned or leased by the University.

2.7 Rationale for the ICT Policy and Guidelines

This policy outlines various courses of action that the University will adopt in addressing matters related to ICT both within and outside the institution. It is intended to guide the entire process regarding the provision and use of ICT services. The development of this policy and guidelines has been necessitated by the increasing access to and reliance on ICT services among the University community. In addition, the expansion of ICT services to accommodate a growing number of students and staff requires proper coordination in the acquisition, maintenance, and utilization of ICT resources.

The policy is also aligned with the National ICT Policy 2023, which encourages public, private, and community sectors to invest in ICT infrastructure for national development. The policy promotes the development of ICT networks, human capital, legal and regulatory frameworks, leadership, and universal access to ICT services. It is further aligned with the Tanzania Digital Economy Framework, which emphasizes

digital transformation, data-driven governance, innovation ecosystems, and inclusive access to digital services as key drivers of socio-economic development.

In addition, the policy is consistent with the Government's electronic government (eGa) initiatives and digital transformation agenda, which advocate for interoperability of systems, improved ICT service delivery, enhanced cybersecurity and efficient public service management through digital platforms. It also draws guidance from regional and international commitments, including the African Union Digital Transformation Strategy (2020–2030), which promotes digital integration, innovation, and the strengthening of digital infrastructure across member states.

The policy is further informed by global development frameworks such as the Sustainable Development Goals (SDGs), particularly SDG 4 (Quality Education) and SDG 9 (Industry, Innovation and Infrastructure), which underscore the role of ICT in advancing inclusive education, innovation, resilient infrastructure, and effective institutions. It also aligns with emerging global priorities on cybersecurity, artificial intelligence governance and digital inclusion, which require institutions to adopt secure, ethical, and innovative ICT practices.

In this context, the University requires a coherent policy framework to guide ICT development, integration and utilization, in support of institutional effectiveness and transformation. The policy will facilitate the effective implementation of the University's Corporate Strategic Plan while ensuring alignment with national, regional and global development priorities, including the Tanzania Development Vision 2050 and the Sustainable Development Goals.

3.0 POLICY ISSUES, STATEMENTS, AND STRATEGIES

3.1 ICT Governance

The growing applications of ICT in supporting teaching, learning, research, and administrative functions require effective governance to ensure alignment with institutional priorities and optimal utilisation of resources. The benefits of ICT investments are limited by challenges related to coordination, accountability, compliance and performance monitoring. In this context, the University seeks to strengthen its ICT governance approach to enhance decision-making, ensure compliance with applicable standards and improve oversight of ICT investments and services.

3.1.1 Policy Statement

The University shall establish and strengthen ICT governance to ensure effective oversight, alignment with institutional priorities, and compliance with applicable standards and regulations.

3.1.2 Policy Strategies

The University will:

- (i) Strengthen ICT governance structures to oversee ICT operations guide investment decisions and align ICT functions with institutional priorities and applicable standards;
- (ii) Develop and periodically review ICT policies, guidelines, and standards to support consistent, secure, and compliant use of ICT resources;
- (iii) Develop and institutionalise ICT risk management approaches to support systematic identification, assessment and mitigation of risks affecting ICT systems and services;
- (iv) Establish and implement mechanisms for monitoring and evaluating ICT services, including service performance, availability, and user satisfaction; and
- (v) Develop and enhance institutional capacity to support effective ICT governance, utilisation of systems and the adoption of relevant and emerging technologies.

3.2 ICT Infrastructure and Facilities

Continuous expansion of systems and services has increased demand for reliable, scalable and secure infrastructure and facilities such as network devices, servers, workstations, laptops, storage, back-up, operating facilities, CCTV and supporting

platforms like operating systems and databases. However, challenges such as capacity limitations, uneven access, maintenance constraints, and evolving technology requirements have affected the efficiency and reliability of these infrastructure and facilities. The University aims to strengthen its infrastructure to ensure sustainability, resilience and access for all users.

3.2.1 Policy statement

The University shall develop and maintain reliable, secure, and scalable ICT infrastructure and facilities to support institutional operations and future technological advancements.

3.2.2 Policy Strategies

The University will:

- (i) Develop and expand an integrated ICT infrastructure architecture aligned with current institutional needs and future technological developments to support teaching, research, consultancy and administrative functions;
- (ii) Implement data management practices that support secure storage, reliable backup, and controlled access to institutional data;
- (iii) Develop sustainable mechanisms for lifecycle management of ICT infrastructure, including maintenance, upgrading, and continuous improvement of existing resources;
- (iv) Develop inclusive ICT infrastructure and access platforms that expand connectivity, availability, and usability of ICT services for all user groups; and
- (v) Establish and enforce governance mechanisms for ICT usage, including compliance monitoring and regulation of user access rights in line with institutional requirements.

3.3 Applications

Applications developed internally or acquired from external providers, play a critical role in enabling institutional business processes and service delivery. However, the absence of coordinated and standardized approaches to their development, acquisition and management has resulted in inconsistencies, duplication of functionalities and operational inefficiencies. The University therefore seeks to strengthen the management of applications to enhance efficiency and alignment with institutional priorities.

3.3.1 Policy statement

The University shall adopt standardized procedures for the development, acquisition, implementation and management of application software to ensure standardization, efficiency and alignment with institutional needs.

3.3.2 Policy Strategies

The University will:

- (i) Standardize software development and acquisition practices to enhance quality, interoperability, and efficient utilization of institutional resources;
- (ii) Maintain structured software lifecycle management practices, including design, documentation, maintenance, support, and controlled change management throughout the application lifecycle;
- (iii) Apply software governance measures to promote compliance with licensing requirements, intellectual property regulations, and the use of authorized and secure software solutions;
- (iv) Promote collaboration and the adoption of appropriate technologies, including open-source and emerging solutions such as Artificial Intelligence (AI), based on institutional needs and risk considerations; and
- (v) Enhance institutional digital platforms, including the university website and students' systems, to ensure security, scalability, usability, and alignment with emerging technology trends.

3.4 ICT Service Management

As ICT services increase, the demand for timely support, service reliability and user satisfaction continues to grow. However, challenges such as inconsistent service levels, limited monitoring mechanisms and evolving user needs have highlighted the need for more structured ICT service management practices. The University aims to enhance ICT service management in alignment with best practices and national standards.

3.4.1 Policy statement

The University shall implement and strengthen ICT service management to ensure efficient, reliable and continuous improvement of ICT services.

3.4.2 Policy Strategies

The University will:

- (i) Strengthen ICT service delivery processes for timely, reliable, and user-centred support services;
- (ii) Implement service performance management mechanisms, including the use of service level arrangements and quality monitoring processes;
- (iii) Regulate digital communication practices to support effective, secure, and information sharing which comply with policy across institutional platforms; and
- (iv) Establish resilient ICT service environments, including business continuity, service recovery capabilities, and digital learning platforms to support core University functions.

3.5 ICT Security

The increasing use of ICT systems and digital platforms exposes the University to a wide range of security threats, including unauthorized access, data breaches, system disruptions and cyberattacks. While measures have been implemented to secure ICT resources, evolving threats and increased complexity in University's ICT systems require a more comprehensive and proactive approaches to security. The University therefore intends to enhance its ICT security strength to ensure confidentiality, integrity and availability of institutional information and systems.

3.5.1 Policy statement

The University shall establish and strengthen ICT security measures to protect its information systems and data from unauthorized access, misuse, alteration, or destruction.

3.5.2 Policy Strategies

The University will:

- (i) Develop and strengthen ICT security capabilities through deployment of appropriate technologies, tools and practices to protect ICT facilities, information assets, and services against evolving threats;
- (ii) Establish and operationalise ICT security governance structures to support coordinated management of security functions, roles, and accountability across the institution;

- (iii) Integrate security requirements across the lifecycle of information systems from design and acquisition to deployment and maintenance, to ensure confidentiality, integrity, and availability; and
- (iv) Develop and enhance continuous monitoring and assurance capabilities including auditing, and controlled use of ICT resources to support proactive detection, response and improvement of security measures.

3.6 ICT Innovations

The rapid evolution of digital technologies presents significant opportunities for universities to transform teaching, learning, research, and service delivery. However, universities are largely consumers of externally developed ICT solutions with limited institutional mechanisms to support innovation, incubation, and commercialization of digital solutions. The University aspires to transition from passive consumption of ICT technologies to active participation in the innovation ecosystems. This shift will enhance institutional competitiveness, strengthen linkages with industry, and contribute to national priorities on industrialization, digital transformation, and knowledge-based economic growth.

3.6.1 Policy statement

The University shall promote and support ICT innovation to enhance institutional performance, advance research and development, and contribute to national and global digital transformation and socio-economic development.

3.6.2 Policy Strategies

The University will:

- (i) Develop an enabling environment for ICT innovation to support research, local solution development and knowledge commercialization in alignment with national digital economy priorities;
- (ii) Establish mechanisms for supporting innovation activities to facilitate transformation of ideas into practical solutions;
- (iii) Support the adoption and integration of emerging technologies to improve teaching, learning, research, and administrative functions;
- (iv) Establish strategic partnerships with industry, government, and research institutions to support collaborative innovation, resource sharing, and knowledge exchange; and

- (v) Implement capacity development initiatives to equip staff and students with skills required for ICT innovation, entrepreneurship, and digital solution development.

3.7 Systems Integration

The increasing adoption of digital systems across university functions has led to the deployment of multiple standalone applications supporting teaching, learning, research, finance, human resources, and administration. While these systems have improved operational efficiency in specific areas, limited integration and interoperability have resulted in data differences, duplication of effort, inconsistent information and inefficiencies in decision-making and service delivery. The University aspires to establish a cohesive and interoperable ICT ecosystem where systems are effectively integrated, data is shared securely and efficiently, and services are streamlined across functional areas. This will improve operational efficiency, data quality and alignment with national e-Government interoperability standards.

3.7.1 Policy statement

The University shall promote and implement systems integration to enhance interoperability, data sharing, and efficiency in service delivery in alignment with institutional and national requirements.

3.7.2 Policy Strategies

The University will:

- (i) Develop and adopt standards and frameworks for systems integration and data exchange to support consistency, compatibility and secure information sharing;
- (ii) Strengthen technical and organizational capacity for systems integration through appropriate skills development, tools, and integration platforms; and
- (iii) Design and implement integrated ICT solutions and interfaces to enable interoperability and efficient exchange of information across institutional systems.
- (iv) Develop and maintain a coordinated integration environment that supports continuous improvement, scalability, and alignment with institutional and national interoperability requirements.

PART TWO:

POLICY GUIDELINES

Implementation shall be guided by the following key steps:

4.1 ICT Governance, Risk and Compliance

- (i). Governance structures and processes established by operationalizing the ICT Steering Committee, defining roles and responsibilities, and adopting clear decision making and reporting procedures.
- (ii). ICT planning and oversight are conducted through structured processes for needs assessment, investment prioritization, resource allocation, and performance monitoring aligned with institutional priorities.
- (iii). Compliance and policy management are implemented by aligning ICT operations with national laws, e-Government standards, and institutional policies, including periodic review and dissemination of relevant guidelines.
- (iv). ICT risk management activities are undertaken through systematic identification, assessment, mitigation, documentation and continuous monitoring of ICT related risks.
- (v). Monitoring, audit, and lifecycle control are carried out by tracking governance performance, conducting periodic audits and managing ICT assets throughout their lifecycle, including disposal in accordance with applicable regulations.

4.2 ICT Systems, Infrastructure and Facilities

- (i). ICT systems and infrastructure are managed through a lifecycle approach covering planning, design, implementation, maintenance and periodic upgrades, guided by approved ICT architecture and technical standards.
- (ii). System changes, upgrades, and enhancements are managed through a structured change management process comprising request initiation, impact and risk assessments, approval by designated authorities, controlled deployment and post-implementation evaluation to ensure system integrity and performance.
- (iii). Systems integrations are implemented through defined interoperability standards and interface specifications to enable secure data exchange across systems.

- (iv). Artificial Intelligence (AI) solutions are adopted through structured assessment, controlled adoption, ethical review and compliance checks aligned with institutional and national regulations.

4.3 ICT Service Management and Operations

- (i). ICT service delivery is implemented through service desk operations, incident management and structured user support processes guided by service levels.
- (ii). Service quality and performance are managed through continuous monitoring, evaluation of availability, user satisfaction and performance reporting.
- (iii). External ICT services are managed through procurement, contract enforcement, performance monitoring and evaluation of service providers.
- (iv). ICT capacity development is implemented through training needs assessment, delivery of programmes and evaluation of user competence improvement.
- (v). Institutional communication through digital and social media platforms follows approval, content control and official channel management including user registration, access management and termination of accounts where applicable.

4.4 ICT Security and Data Protection

- (i). ICT security is implemented through a structured process of risk assessment, control implementation, monitoring and continuous improvement aligned with security standards.
- (ii). Access control and system protection are managed by user authentication, authorization, activity logging, and periodic review of access rights.
- (iii). Data protection is implemented following a lifecycle approach covering classification, secure storage, encryption, backup and recovery testing.
- (iv). Security incident management is implemented following a cycle of detection, reporting, response, recovery, and post-incident review.
- (v). ICT security awareness is promoted through continuous training, communication, and compliance reinforcement programmes.

5.0 ROLES OF STAKEHOLDERS IN MANAGING ICT RELATED ACTIVITIES

5.1 ICT Steering Committee

The steering committee shall:

- (i) Review and provide advice on ICT investment plans and priorities.
- (ii) Ensure alignment of ICT with the University's needs.
- (iii) Ensure e-Government guidelines and standards are complied with.
- (iv) Ensure continuous monitoring and evaluation of ICT projects in the University.
- (v) Review and approve the disaster recovery plan and ensure its effective implementation.
- (vi) Perform such other functions as may be directed by the appointing authority
- (vii) Meet quarterly to monitor and evaluate the achievements in ICT initiatives against the University's Strategic plan, ICT Policy, ICT Strategy and ICT Security Policy and Procedures.
- (viii) Assess progress, approve, provide guidance and make recommendations where necessary.

5.2 Dean/Directors/Head of Departments/Section/Units

With regard to this policy, these leaders shall:

- (i) Ensure that all users under their supervision are aware and comply with this policy.
- (ii) Enhance adequate and appropriate protection of ICT assets and resources under their control.
- (iii) Ensure availability, integrity and confidentiality of information produced by systems under their areas.
- (iv) Be custodian of data and information for their respective areas of operations.

5.3 Department of ICT Services

In relation to this policy, the department of ICTS shall oversee the overall implementation of this policy, and in particular the department shall:

- (i) Implement ICT policies, strategies and standards.
- (ii) Form and prepare relevant guidelines and procedures towards the implementation of this policy.
- (iii) Be custodian of all ICT resources of the University.

- (iv) Prepare and present a quarterly ICT performance and implementation report to the ICT Steering Committee.

5.4 Internal Audit Unit

The internal audit unit shall audit ICT functions of the University and ensure compliance/compliance with this policy and guidelines.

5.5 Quality Assurance Unit

The Quality Assurance Unit shall be responsible for:

- (i) Monitoring and evaluating ICT governance and service delivery practices
- (ii) Assessing the quality and performance of ICT services and systems to ensure efficiency, reliability, user satisfaction, and continuous improvement.
- (iii) Providing independent reports and recommendations to University management on ICT performance gaps, risks, and areas for improvement to support decision making.

5.6 Users

All users of University's ICT systems shall be responsible for safeguarding ICT assets in their custody and complying with this policy.

5.7 Conformance

- (i). The University shall ensure that ICT conforms to e-Government standards and guidelines and all external regulations and complies with all internal policy, procedures and practices.
- (ii). 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.

6.0 MONITORING AND EVALUATION

6.1 Monitoring

The overall monitoring of this ICT Policy and Guidelines shall be undertaken by the Department of ICT Services in consultation with the Deputy Vice Chancellor (Planning, Finance and Administration). Monitoring shall involve continuous assessment of the implementation and effectiveness of the Policy in not only supporting the University's objectives but also responding to technological advancements and emerging ICT needs.

Specifically, the Department of ICT Services shall:

- (i) Be responsible for advising and assisting all institutional entities including units, departments, faculties, directorates, bureaus, institutes and other stakeholders across the University on ICT matters.
- (ii) Work and be advised by the ICT Steering Committee in monitoring and evaluating policy activities.
- (iii) Develop and maintain key performance indicators to assess the efficiency, effectiveness, and impact of ICT services and systems on a regular basis.
- (iv) Track the performance, usage, and reliability of ICT infrastructure, systems and applications.
- (v) Record and respond to user feedback, complaints, and service issues, and implement corrective measures to improve ICT service delivery.

6.2 Evaluation

The Policy shall be evaluated based on data and evidence generated through monitoring processes including defined Key Performance Indicators (KPIs), performance reports, audit findings, and user feedback data. Evaluation shall focus on the extent to which policy objectives have been achieved as well as the efficiency, effectiveness, and impact of ICT services in supporting the University's core functions.

The evaluation shall be conducted every three (3) years, unless deemed necessary, by a team appointed by the Deputy Vice Chancellor (Planning, Finance and Administration). The evaluation process shall be guided by clearly defined performance indicators, including but not limited to: ICT service availability, system downtime trends, security incident frequency, compliance levels, user satisfaction index, ICT resource utilization efficiency, level of system interoperability and

integration, data consistency and exchange effectiveness across systems, number and adoption rate of ICT innovation initiatives and extent of implementation of emerging technologies in institutional processes.

The terms of reference for the evaluation shall be developed in consultation with the Head of the Department of ICT Services. The evaluation process shall be participatory, involving key stakeholders to ensure a comprehensive assessment and practical recommendations. Findings from the evaluation shall be used to inform policy review, strengthen ICT governance, improve service performance and enhance the overall effectiveness and impact of ICT services within the University.

7.0 OPERATION AND REVIEWS

7.1 Operational Date

This ICT Policy and Guidelines shall come into force upon its approval by the Council.

7.2 Policy Review

This Policy shall be reviewed every five (5) years or earlier where necessary to ensure continued relevance and alignment with institutional and national priorities. The review process shall involve key stakeholders across the University. The Department of ICT Services shall coordinate the review in consultation with the relevant governance bodies, including the ICT Steering Committee. The process should include stakeholder consultations and consideration of feedback received.

Proposed revisions shall be subjected to technical review and formal approval in accordance with the University's governance procedures. Members of the University community and other stakeholders may submit recommendations for policy improvement to the Department of ICT Services at any time for consideration in the review process.