UNITED REPUBLIC OF TANZANIA

MINISTRY OF EDUCATION, SCIENCE AND TECHNOLOGY

MOSHI CO-OPERATIVE UNIVERSITY (MoCU)
CHUO KIKUU CHA USHIRIKA MOSHI

ACCEPTABLE INFORMATION COMMUNICATION TECHNOLOGY USE POLICY

FIRST EDITION

APRIL, 2026

FOREWORD

Moshi Co-operative University (MoCU), as an institution of higher learning, relies heavily on Information and Communication Technology (ICT) resources to support its core functions of teaching, research, consultancy, and community service. ICT systems, including computers, networks, email services, and digital platforms, play a vital role in facilitating communication, knowledge sharing, data management, and efficient service delivery within the University. As the use of digital technologies continues to expand in higher education institutions, it has become increasingly important to ensure that these resources are used responsibly, securely, and in accordance with established institutional and legal frameworks.

Over the years, MoCU has made significant investments in ICT infrastructure and services to improve academic delivery, administrative efficiency, and collaboration with stakeholders both within and outside the country. The growing reliance on digital systems, however, also introduces various risks related to information security, misuse of ICT facilities, unauthorized access to institutional data, and exposure to cyber threats. These challenges necessitate that the University establish clear guidelines governing the acceptable use of ICT resources by staff, students, and other stakeholders.

The Acceptable ICT Use Policy has therefore been developed to provide a comprehensive framework that guides responsible and ethical use of ICT facilities at the University. The Policy outlines acceptable and unacceptable behaviour in the use of ICT resources, and provides guidance on areas such as email usage, internet access, password management, protection of ICT equipment, software licensing, mobile device usage, and other aspects related to ICT security and management. The Policy is intended to safeguard the integrity, confidentiality, and availability of the University's ICT systems and information assets while ensuring that users can effectively utilize these resources in support of institutional objectives.

Furthermore, this Policy promotes a culture of accountability and responsible digital conduct within the University community. It emphasizes the importance

of protecting institutional information, respecting intellectual property rights, and ensuring compliance with national ICT regulations and standards. By establishing clear responsibilities and expectations for ICT users, the Policy helps strengthen information security practices and minimize risks associated with technology misuse. It is expected that the effective implementation of this Policy will enhance the secure and efficient use of ICT resources across the University and support the achievement of MoCU's mission of providing quality education, training, research, and advisory services to the co-operative sector and society at large.

I therefore call upon all staff members, students, and other stakeholders of the University to familiarize themselves with this Policy and adhere to its provisions to ensure responsible use of ICT resources and protection of the University's digital assets. Through collective commitment and compliance, the University will continue to strengthen its ICT environment in support of its academic and institutional goals.

Prof. Alfred Said Sife

Vice Chancelor

Table of Content

1. POLICY FRAMEWORK

1.1. Background Information

The history of the Moshi Co-operative University (MoCU) dates 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), becoming the Constituent University College of Sokoine University of Agriculture through the Government Declaration Order No. 22 of 2004. MoCU came into being through the transformation of Moshi University College of Co-operative and Business Studies (MUCCoBS) into 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 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 Teaching Centre. 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.

1.2. University Vision, Mission and Core values

Vision

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

Mission

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

Core Values

In pursuing its mission and achieving its vision, the University is guided by seven core values: co-operation, objectivity, the pursuit of excellence in service delivery, integrity, accountability, courtesy to all, and social responsibility.

Motto

The Motto of the University is "*Ushirika ni Biashara*."

Objects and Functions of the University

The general objectives of the University are to advance knowledge, wisdom, understanding and enhance creativity through teaching, research, extension and consultancy on all matters relating to co-operative development, rural transformation, business studies, information and communication technology, law and any other relevant area of learning and knowledge at national and international levels.

2. POLICY JUSTIFICATION, OBJECTIVES, AND GUIDING PRINCIPLES

2.1. Justification for the Policy

The development of the Acceptable ICT Use Policy is driven by the increasing reliance on Information and Communication Technology (ICT) in supporting the University's academic, administrative, research, and consultancy functions. As digital technologies continue to expand within higher learning institutions, there is a growing need to establish clear guidelines that promote responsible, ethical, and secure use of ICT resources.

The University has made significant investments in ICT infrastructure, including computer systems, networks, internet connectivity, institutional email, digital learning platforms, and other information systems to enhance efficiency and service delivery. While these advancements have improved communication, collaboration, and access to information, they have also introduced risks such as cyber threats, unauthorized access to data, misuse of ICT resources, and breaches of information confidentiality.

In the absence of clearly defined acceptable use guidelines, users may misuse ICT facilities either unintentionally or deliberately leading to operational disruptions, legal exposure, and reputational damage. Common risks include installation of unauthorized software, weak password practices, improper handling of institutional data, and access to inappropriate online content, all of which can compromise system security and integrity.

The increasing use of ICT in teaching, research, and administration, alongside the growth of mobile technologies, cloud services, and online communication platforms, further intensifies the need for strong governance mechanisms. Additionally, limited awareness among some users regarding cybersecurity practices and data protection requirements highlights the necessity for structured guidance and accountability.

This Policy therefore provides a comprehensive framework for regulating the acceptable use of ICT resources within the University. It establishes standards

governing the use of institutional ICT assets, including computers, networks, email systems, internet services, mobile devices, and software applications. It also outlines measures to safeguard institutional information and ensure compliance with relevant national ICT regulations and standards. Ultimately, the Policy aims to protect the confidentiality, integrity, and availability of the University's ICT systems and data, while enabling users to effectively leverage digital technologies in achieving the University's mission and strategic objectives.

2.2. Situational Analysis

Moshi Co-operative University (MoCU) has progressively integrated Information and Communication Technology (ICT) into its academic and administrative functions across its expanding institutional network, which includes the main campus in Moshi, KICoB in Shinyanga, and thirteen regional offices serving all regions of Tanzania Mainland. This expansion is supported by a range of ICT systems and services, including institutional networks, internet and intranet connectivity, electronic communication platforms, academic information systems, cloud and mobile-based applications, CCTV and physical access control systems, and other computer-based applications. Significant investment in this infrastructure has enhanced communication, research, online learning, data management, and collaboration with local and international partners.

Despite these achievements, the University faces growing challenges associated with managing an increasingly decentralised ICT environment. User awareness of responsible ICT practices remains inconsistent in some areas, exposing institutional systems to cybersecurity threats such as malware, phishing attacks, weak password practices, and mishandling of institutional data. The use of unapproved or unlicensed software, together with increased reliance on personally owned and mobile devices to access institutional systems, has heightened the risk of data leakage, unauthorised access, and other security breaches.

At present, the acceptable use of ICT resources is guided largely by general institutional expectations rather than by a single, comprehensive and formally documented framework. New staff and students are not consistently required to acknowledge ICT acceptable use obligations upon joining the University, while cybersecurity awareness and responsible digital conduct are promoted mainly through occasional rather than structured and mandatory training programmes. In addition, although some systems are monitored, there is no consistent University-wide mechanism for audit trails, usage logging, or coordinated incident reporting across departments, regional offices, and teaching centres. This has contributed to inconsistent ICT practices and weakened accountability and enforcement mechanisms.

Nevertheless, the University is well-positioned to strengthen ICT governance through existing MoCU ICT policies and strategies, applicable national ICT standards and data protection legislation, increasing institutional awareness of cybersecurity risks, and the availability of qualified ICT personnel within the ICT Services Department. This Policy has therefore been developed to provide a comprehensive framework for the responsible and secure use of ICT resources, including guidance on internet and email usage, password management, software licensing, mobile device and equipment security, CCTV and access control, and incident reporting. The Policy aims to safeguard institutional information resources while supporting a secure, efficient, and accountable ICT environment aligned with MoCU's academic and institutional goals.

2.3. Policy Objectives

Main Objective

The main objective of this policy is to ensure responsible, secure, ethical, and future-ready use of the University's ICT resources to support teaching, learning, research, administration, and community engagement, while protecting institutional information assets and preparing the University community for an evolving digital future.

Specific Objectives

The following are the specific objectives of the Policy:

i. To provide clear guidelines on acceptable and responsible use of the University's ICT resources by staff, students, and other authorized users;
ii. To safeguard the confidentiality, integrity, and availability of the University's information systems, networks, and data;
iii. To promote awareness and understanding of ICT security practices and responsible digital behaviour among all users;
iv. To prevent misuse, unauthorized access, and activities that may compromise the performance, reliability, or security of ICT systems.
v. To ensure compliance with relevant laws, regulations, and institutional policies governing the use of ICT resources;
vi. To protect the University's ICT infrastructure from cyber threats, malicious activities, and other security risks;
vii. To establish accountability mechanisms for monitoring ICT usage and addressing violations of acceptable use standards.

2.4. Guiding Principles

All use of the University's ICT resources shall be governed by the following principles:

i. **Legality:** All ICT use shall comply with applicable laws, regulations, and institutional policies.
ii. **Accountability**: Users shall be responsible for their actions on University ICT systems, and appropriate mechanisms shall be maintained to trace and attribute ICT usage.
iii. **Purposefulness:** ICT resources shall be used primarily for authorized academic, research, administrative, and other legitimate institutional purposes.
iv. **Integrity:** Users shall act with honesty and ethical responsibility in all digital interactions, including the use of AI tools, online communications, and research activities.

v. **Privacy and Data Protection:** Personal data of staff, students, and third parties shall be handled in accordance with applicable data protection legislation and institutional guidelines.

vi. **Security:** Users and the University shall take proactive measures to protect ICT systems, data, and infrastructure from unauthorized access and cyber threats.

vii. **Inclusivity and Accessibility**: ICT resources and digital services shall be made accessible to all users, including those with special needs.

viii. **Transparency:** The University shall be transparent about how ICT systems are monitored and how user data is managed.

ix. **Sustainability:** The University shall promote environmentally responsible use of ICT resources, including energy efficiency and responsible disposal of ICT equipment.

x. **Continuous Improvement:** The University shall regularly review and update ICT policies to reflect technological developments and emerging risks.

2.5. Scope

This Acceptable ICT Use Policy applies to all MoCU staff (permanent, temporary, part-time, and contract), students, contractors, consultants, visiting researchers, and any third parties who use ICT resources owned, leased, or rented by MoCU. It applies regardless of location, including the main campus, KICoB, all regional offices, and off-campus and remote working environments. It also applies to any person who connects personally owned devices to the MoCU network or remotely accesses MoCU systems and data, including through cloud platforms and virtual private networks (VPNs).

3. POLICY STATEMENTS

3.1. Acceptable Behaviour in Use of ICT Resources

3.1.1 The University shall provide mandatory ICT usage awareness and cybersecurity training to all staff and students to enhance their knowledge of responsible ICT use, data protection, and emerging cyber threats.

3.1.2 The University shall enforce user access controls based on roles and responsibilities, ensuring that individuals can only access systems and information necessary for their assigned duties.

3.1.3 The University shall establish and maintain ICT usage monitoring mechanisms, including system logs and audit trails, to detect, prevent, and respond to misuse or unauthorized activities.

3.1.4 The University shall require all users to formally sign ICT Acceptable Use declarations, confirming their understanding of and commitment to comply with institutional ICT policies.

3.1.5 The University shall conduct periodic ICT compliance audits and assessments to evaluate adherence to policies and identify potential security risks or gaps.

3.1.6 Users shall use ICT resources strictly for authorized academic, research, and administrative purposes, ensuring alignment with the University's mission and avoiding any misuse.

3.1.7 Users shall safeguard their access credentials, including usernames and passwords, and shall not share them or allow unauthorized access to ICT systems.

3.1.8 Users shall comply with all applicable ICT policies, legal requirements, and institutional guidelines, ensuring that their actions do not expose the University to legal or security risks.

3.1.9 Users shall respect data privacy, confidentiality, and intellectual property rights when accessing, processing, or sharing information through ICT systems.

3.1.10 Users shall promptly report any ICT security incidents, suspected breaches, or misuse to the appropriate University authority to enable timely response and mitigation.

3.2 Unacceptable Behaviour and Misuse of ICT Resources

3.2.1 The University shall implement network monitoring systems and intrusion detection mechanisms to identify, prevent, and respond to unauthorized access and cyber threats.

3.2.2 The University shall establish and enforce clear disciplinary procedures and incident response frameworks to address ICT misuse and violations.

3.2.3 The University shall deploy endpoint security solutions, including antivirus and anti-malware tools, to protect institutional systems.

3.2.4 The University shall conduct regular cybersecurity awareness programs to educate users on risks and responsible ICT use.

3.2.5 Users shall refrain from attempting unauthorised access to ICT systems, networks, or data.

3.2.6 Users shall not introduce malware, viruses, or harmful software into university systems.

3.2.7 Users shall avoid engaging in illegal or unethical activities, including hacking, piracy, and cyber harassment.

3.2.8 Users shall use ICT resources in a manner that does not disrupt services or other users.

3.2.9 Users shall report any misuse or suspicious ICT activities promptly.

3.3 Acceptable Use of ICT Assets and Information

3.3.1 The University shall implement data classification and secure information handling frameworks to protect institutional data.

3.3.2 The University shall enforce role-based access control (RBAC) to restrict access to authorized users only.

3.3.3 The University shall provide secure data storage, backup, and recovery mechanisms to ensure data availability and integrity.

3.3.4 The University shall establish secure data disposal procedures to prevent unauthorized access to obsolete data.

3.3.5 The University shall conduct information security awareness training for all users.

3.3.6 Users shall handle institutional data in accordance with data protection and classification guidelines.

3.3.7 Users shall access ICT assets and information only within their authorized privileges.

3.3.8 Users shall protect institutional data from unauthorized disclosure, alteration, or loss.

3.3.9 Users shall use ICT assets responsibly and avoid damage, loss, or misuse.

3.3.10 Users shall ensure secure disposal or transfer of information in compliance with university procedures.

3.4 Acceptable Use of Institutional Email Systems

3.4.1 The University shall implement email filtering, anti-phishing, and secure email gateway solutions to protect communication systems.

3.4.2 The University shall enforce official email usage standards and monitor compliance to ensure proper use.

3.4.3 The University shall provide training on phishing and social engineering attacks to enhance user awareness.

3.4.4 The University shall monitor institutional email systems to detect misuse and ensure compliance.

3.4.5 The University shall implement spam filtering and email security technologies to reduce threats.

3.4.6 Users shall use institutional email strictly for official communication purposes.

3.4.7 Users shall avoid sending or forwarding inappropriate, offensive, or illegal content.

3.4.8 Users shall remain vigilant against phishing and suspicious emails.

3.4.9 Users shall protect email accounts from unauthorized access.

3.4.10 Users shall ensure professionalism, accuracy, and accountability in email.

3.5 Internet and Intranet Usage

3.5.1 The University shall implement web filtering and content control mechanisms to restrict harmful or inappropriate content.

3.5.2 The University shall monitor internet usage to ensure compliance with institutional policies.

3.5.3 The University shall restrict access to high-risk or malicious websites and domains.

3.5.4 The University shall enforce secure browsing practices and deploy antivirus scanning systems.

3.5.5 The University shall promote responsible internet use through awareness programs.

3.5.6 Users shall use internet and intranet services strictly for academic, research, and administrative purposes.

3.5.7 Users shall avoid accessing illegal, harmful, or inappropriate online content.

3.5.8 Users shall not engage in excessive bandwidth usage that affects system performance.

3.5.9 Users shall comply with secure browsing guidelines and institutional policies.

3.5.10 Users shall report suspicious websites or cybersecurity threats encountered online.

3.6 Password Management and Authentication

3.6.1 The University shall enforce strong password policies, including complexity and minimum requirements.

3.6.2 The University shall implement multi-factor authentication (MFA) for critical systems.

3.6.3 The University shall require password updates every three months to enhance security.

3.6.4 The University shall deploy identity and access management systems to manage authentication securely.

3.6.5 The University shall monitor login attempts and enforce account lockout mechanisms.

3.6.6 Users shall create strong passwords in accordance with institutional standards.

3.6.7 Users shall keep authentication credentials confidential and not share them.

3.6.8 Users shall update passwords regularly as required.

3.6.9 Users shall use multi-factor authentication where applicable.

3.6.10 Users shall report any suspected credential compromise immediately.

3.7 Security of ICT Equipment

3.7.1 The University shall maintain an ICT asset inventory and management system for all equipment.

3.7.2 The University shall enforce physical security measures to protect ICT equipment.

3.7.3 The University shall require prompt reporting of lost or stolen devices.

3.7.4 The University shall implement device encryption and endpoint protection technologies.

3.7.5 The University shall conduct periodic ICT asset audits.

3.7.6 Users shall safeguard ICT equipment assigned to them against theft, loss, or damage.

3.7.7 Users shall use ICT equipment strictly for authorized purposes.

3.7.8 Users shall report lost, stolen, or damaged equipment immediately.

3.7.9 Users shall ensure devices are secured when not in use.

3.7.10 Users shall comply with institutional guidelines on handling ICT equipment.

3.8 Mobile Device Usage

3.8.1 The University shall implement Mobile Device Management (MDM) solutions to secure mobile devices.

3.8.2 The University shall enforce encryption and secure authentication on mobile devices.

3.8.3 The University shall deploy antivirus and endpoint protection for mobile environments.

3.8.4 The University shall restrict network access for non-compliant devices.

3.8.5 The University shall provide guidelines for secure use of mobile devices off-campus.

3.8.6 Users shall ensure mobile devices comply with institutional security requirements.

3.8.7 Users shall protect mobile devices using passwords, encryption, or biometrics.

3.8.8 Users shall avoid using unsecured networks when accessing institutional systems.

3.8.9 Users shall install only authorized and secure applications.

3.8.10 Users shall report loss or compromise of mobile devices immediately.

3.9 CCTV and Physical Surveillance Systems

3.9.1 The University shall restrict access to CCTV systems to authorized personnel only.

3.9.2 The University shall ensure secure storage and management of surveillance recordings.

3.9.3 The University shall ensure release of CCTV footage is subject to formal authorization by designated authorities.

3.9.4 The University shall conduct periodic audits of CCTV systems.

3.9.5 The University shall provide training for personnel responsible for CCTV management.

3.9.6 Users shall respect privacy and confidentiality in areas under surveillance.

3.9.7 Users shall not tamper with CCTV systems or equipment.

3.9.8 Users shall access CCTV systems or footage only when authorized.

3.9.9 Users shall use surveillance data strictly for legitimate purposes.

3.9.10 Users shall report any misuse or malfunction of CCTV systems.

3.10Access Cards and Physical Access Control

3.10.1 The University shall implement electronic access control systems to regulate entry into restricted areas.

3.10.2 The University shall maintain records of access card issuance and usage.

3.10.3 The University shall require immediate reporting of lost access cards.

3.10.4 The University shall conduct periodic reviews of access permissions.

3.10.5 The University shall integrate access control systems with institutional security monitoring.

3.10.6 Users shall use access cards strictly for authorized entry purposes.

3.10.7 Users shall not share or lend access cards.

3.10.8 Users shall report lost or stolen access cards immediately.

3.10.9 Users shall comply with access control procedures for restricted areas.

3.10.10 Users shall not attempt to bypass physical security controls.

3.11 Software Use and Licensing

3.11.1 The University shall maintain a centralized software license management system to ensure compliance.

3.11.2 The University shall conduct periodic software audits to verify licensing compliance.

3.11.3 The University shall restrict software installation privileges to authorized personnel.

3.11.4 The University shall provide approved and secure software repositories for users.

3.11.5 The University shall remove unauthorized or unlicensed software from institutional devices.

3.11.6 Users shall use only licensed and University-approved software.

3.11.7 Users shall not install or use unauthorized or pirated software.

3.11.8 Users shall comply with software licensing agreements and terms of use.

3.11.9 Users shall report any unauthorized software installations.

3.11.10 Users shall ensure proper and secure use of software to avoid security and legal risks.

4. IMPLEMENTATION, REVIEWS, AND ENFORCEMENT

4.1. Implementation and Reviews

i. This document will become effective once approved by the university management and will then be mandatory for all MoCU business operations.

ii. Failure to observe this policy may subject individuals to loss of ICT resources access privileges or to disciplinary action, including termination of employment or contract.

iii. This document shall be reviewed within three years, or whenever the business environment of MoCU changes in a way that affects the current policy.

4.2. Exceptions

i. In case of any exceptions to this policy, it shall be thoroughly documented and reported to the head of ICT Services.

4.3. Roles and Responsibilities

i. It is the responsibility of any person using MoCU's ICT resources to read, understand, and follow these guidelines.

ii. In addition, users are expected to exercise reasonable judgment in interpreting these guidelines and in making decisions about the use of ICT resources.

iii. Any person with questions regarding the application or meaning of statements in this policy should seek clarification from the ICT Services Departments.

iv. The head of ICT Services shall enforce compliance by using audit trails and triggering access revocation/removal to MoCU systems and networks.

4.4. Monitoring and Evaluation

i. The ICT Steering Committee shall meet regularly to monitor and evaluate compliance with MoCU's acceptable ICT use policy.

5. GLOSSARY AND ACRONYMS

5.1. Glossary

Acceptable ICT Use Policy – A document that elaborate on the Public Institution's ICT Management Philosophy by outlining appropriate use of the Institution's Information, Communication and Technology resources and it applies to all users of ICT resources.

6. Acronyms

6.1 **CCTV** – Closed Circuit Television

6.2 **ICT** – Information & Communication Technology

6.3 **ID** – Identification

6.4 **MoCU**- Moshi Co-operative University

6.5 **ICT'S**- Information Communication Technology Services

7. RELATED DOCUMENTS

7.1 ICT Policy

7.2 ICT Strategy

7.3 Enterprise Architecture

7.4 ICT Security Policy

7.5 ICT Service Management Guidelines

7.6 Disaster Recovery Plan

7.7 ICT Project Management Guidelines

7.8 ICT Acquisition, Development and Maintenance Guidelines

DOCUMENT CONTROL

Version	Name	Comment	Date
Ver. 1.0	Responsible Section	The policy has been developed	March, 2026

8. APPENDIX

Declarations by staff/students/stakeholders

These declarations are designed to certify that users acknowledge awareness of MoCU's Acceptable Information and Communication Technology Use Policy and agree to abide by its terms.

I…… acknowledge that the Acceptable ICT Use Policy has been made available to me for adequate review and understanding. I certify that I have been given ample opportunity to read and understand it, and ask questions about my responsibilities on it. I am, therefore, aware that I am countable to all its terms and requirements; and that I shall abide by them. I also understand that failure to abide by them, shall result in appropriate disciplinary action or legal action, or both, as the case may be.

Signature:……

Department/Unit:……..
Job Title:……..

Date: ____ / __ / ____