UNITED REPUBLIC OF TANZANIA

MINISTRY OF EDUCATION, SCIENCE AND TECHNOLOGY

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

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) SECURITY POLICY

APRIL, 2022

FOREWORD

The Moshi Co-operative University (MoCU) became a full-fledged University in 2014 and launched its first ICT Policy in 2015 and revised it in 2019. Since then, the ICT Policy has been used as a guide for the identification, promotion, and usage of ICT in the planning and implementation of academic, research, consultancy, and administrative functions. The ICT Policy, however, is not a fit-all in ICT demands, especially in ICT security concerns of the institution. ICT security issues need to be addressed in finer details to ensure confidentiality, integrity, and availability of ICT services in the institution. The University, thus, found it necessary to come up with this ICT Security Policy.

The ICT Security Policy has captured various security issues namely, ICT Security Governance and Management, ICT security Operations, Security of ICT Assets, Identity and Access Management, ICT Security Incident Management, Information Systems Continuity Management, Security of ICT Acquisition, Development and Maintenance, Human Resource Security, Physical and Environmental Security and ICT Security Compliance and Audit. Furthermore, the guidance for implementation, reviews, and monitoring of this policy is also covered.

The ICT Security Policy aims at providing insight into securing ICT infrastructure, resources, and operations in the university. It is anticipated that this policy will help the University to move toward its Vision of becoming: “An eminent academic institution committed to supporting co-operative and business development”. The University wishes to extend its gratitude to various stakeholders who contributed to the formulation of this ICT security policy and argues every MoCU member to adhere to the policy to meet the envisioned dream.

Prof. Alfred. S. Sife
Vice Chancellor

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

ICT	Information & Communication Technology
KICoB	Kizumbi Institute of Co-operative and Business Education
MoCU	Moshi Co-operative University
MUCCoBS	Moshi University College of Co-operative and Business Studies
SUA	Sokoine University of Agriculture

DEFINITION OF TERMS

Contractors Professionals who provide skills or services to the university for a set period. They may be contracted for a set number of hours, a certain time frame, or the duration of a project or activity.

Event Logs A file that contains information about usage and operations of information systems or applications

ICT Security Relevant incidents as well as measures, controls and procedures applied by enterprise in order to ensure integrity, confidentiality and availability of their data and ICT systems

Information audits Systematic evaluation of information use, resources and flows, with a verification by reference to both people and existing documents in order to establish the extent to which they are contributing to an organization's objectives.

Security threats Condition or something that may damage or steal your data or allow someone else to access your computer, without your knowledge or consent

Staff Staff of the University as defined by the MoCU Charter, 2015

Student A registered student at MoCU in a particular semester or module

1. INTRODUCTION

1.1 Institutional 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 the training of human resource 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 of 1964 (Repealed) as an autonomous institution with its own Governing Board.

In 2004, the Co-operative College Moshi was transformed into MUCCoBS as the Constituent University College of Sokoine University of Agriculture (SUA) through the Government Notice No. 172 of 2004. MoCU came into being as a result of transforming 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. MoCU is located in Moshi Municipality, on the foot of Mount Kilimanjaro along Sokoine Road. The University has an Institute located in Shinyanga Region along Tabora Road, namely Kizumbi Institute of Co-operative and Business Education (KICoB).

1.1.1 Vision

The Vision of the University is *"To be an eminent academic institution committed to support co-operative and business development".*

1.1.2 Mission Statement

The University Mission is *"To promote sustainable co-operative and business development through quality training, research and advisory services."*

1.1.3 Motto

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

1.1.4 Objects and Functions

The general objectives and functions of the University shall be to advance knowledge, wisdom, understanding, and enhance creativity through training, research, and advisory services 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. The specific objects and functions of the University are spelled out in the MoCU Charter, 2015.

1.1.5 Core Values

The University’s core values include cooperation, professionalism, integrity, transparency, accountability, social responsibility, equality, courtesy to all, creativity, and innovation.

2. THE POLICY FRAMEWORK

2.1 Overview

The University's information and technology assets are highly valuable and must be closely safeguarded. MoCU operates within an increasingly electronic, interconnected, and regulated environment that necessitates a consistent and standardized approach to securing technology and information assets.

To ensure the continued protection of the institution's information and to maintain a secure environment, the management team of the university strongly believes that an ICT security approach aligned with industry standards is necessary. The ICT Security Policy of the University shall therefore, focus on addressing the Confidentiality, Integrity and Availability of information and ICT facilities.

2.2 Policy Statement

This policy seeks to protect the confidently, integrity, and availability of information and ICT facilities through the use of established ICT security processes and practices. The university is committed to ensuring that information security is given the highest possible degree of importance. Information is central to the University's core function and it is the aim of the University to ensure that the confidentiality, integrity and availability of information are protected at all times.

2.3 Policy Goal

This ICT Security Policy is the cornerstone of the university's ICT security strategy, aimed at securing the information assets of the institution. It also outlines the roles and responsibilities of relevant actors who are responsible for implementing the security controls.

2.4 Policy Objectives

The objectives of this ICT Security Policy are to ensure:

(i) ICT used in the university is properly assessed for risks and threats to security;

(ii) Appropriate levels of security are applied to maintain the confidentiality, integrity and availability of Information and ICT;

(iii) All staff are aware of their roles, responsibilities and accountability for information security;

(iv) Awareness of information security issues, their impact is communicated to the university for management, staff and students;

(v) Procedures to detect, investigate and resolve security breaches are in place and are dealt with consistently throughout the university;

(vi) Relevant legislation and regulatory requirements are complied with;

(vii) Plans to ensure continuity for all business-critical systems are in place; and

(viii) Monitoring arrangements exist to audit the ongoing effectiveness of the information security arrangements in the university.

2.5 Scope

This Policy applies to all employees, students, contractors, consultants; temporary and permanent workers at the University including all personnel affiliated with external parties. This Policy applies regardless of the location from which a user gains access to the facilities.

2.6 Rationale

It is the mandate of the University that the information assets are protected from all types of threats, whether internal or external, deliberate or accidental, such that:

(i) Confidentiality of information is maintained;

(ii) Integrity of information can be relied upon;

(iii) Information is available when the business needs it; and

(iv) Relevant statutory, regulatory, and contractual obligations are met.

2.7 Policy Issues

This Policy covers the following issues:

(i) ICT Security Governance and Management;

(ii) ICT security Operations;

(iii) Security of ICT Assets;

(iv) Identity and Access Management;

(v) ICT Security Incident Management;

(vi) Information Systems Continuity Management;

(vii) Security of ICT Acquisition, Development and Maintenance;

(viii) Human Resource Security;

(ix) Physical and Environmental Security; and

(x) ICT Security Compliance and Audit.

3. POLICY ISSUES, STATEMENTS AND STRATEGIES

3.1 ICT Security Governance and Management

3.1.1 Policy Issue

ICT security governance is what will ensure all security strategies are aligned with core objectives of the University and are consistent with regulations. Proper security governance and management will facilitate detection, prevention and response to ICT security incidents.

3.1.2 Policy Statement

The University shall ensure effective ICT security governance and management of all applications and equipment used for information processing.

3.1.3 Implementation Strategies

(i) There shall be an ICT Security Governance Committee which may have members not necessarily limited to MoCU staff;

(ii) The Department of ICT shall prepare ICT security risk management framework that includes risk assessment, risk mitigation, risk acceptance, risk communication and risk monitoring and evaluation; and

(iii) The University shall implement a policy and support ICT security measures to protect information accessed, processed, or stored at teleworking sites.

3.2 ICT Security Operations

3.2.1 Policy Issue

The University recognizes the need for users to get reliable information. This poses a requirement for the university to ensure availability of information which is not altered by any means.

3.2.2 Policy Statement

The university shall protect all processes performed by users of ICT services and equipment from vulnerability to security threats.

3.2.3 Implementation Strategies

(i) Changes to the institution, business processes, information processing facilities, and systems that affect ICT security shall be controlled and communicated to the appointed/authorized personnel whenever they occur;

(ii) The use of resources shall be monitored to ensure the required system performance;

(iii) Backup copies of information, software, and system images shall be taken and tested regularly;

(iv) Event logs recording user activities, exceptions, faults, and CT security events shall be produced, kept, and regularly reviewed; and

3.3 Security of ICT Assets

3.3.1 Policy Issue

ICT assets are increasing in numbers befitting usage of daily ICT services at the University. In that case, the University reorganizes that there is a need for a mechanism to monitor and secure these assets as they are used as processing facilities of the vital information.

3.3.2 Policy Statement

The University shall ensure protection and proper handling of ICT assets associated with information and information processing facilities.

3.3.3 Implementation Strategies

(i) ICT assets associated with information and information processing facilities at the university shall be identified and an inventory of these assets should be drawn up and maintained;

(ii) Acceptable use of information, assets associated with information, and information processing facilities shall be identified, documented, and implemented;

(iii) Procedures for handling ICT assets and removable media shall be instituted; and

(iv) The university shall develop and implement cryptographic controls mechanisms for the protection of information and information processing facilities.

3.4 Identity and Access Management

3.4.1 Policy Issue

Users of information systems can pose risks to security through getting access to confidential information, modifying and deleting contents. To avoid this, the University needs to have a mechanism of identifying all users of information processing facilities and give them different privileges according to their roles' access requirements.

3.4.2 Policy Statement

The University shall ensure that, the use of ICT services is controlled and information is protected from unauthorized access.

3.4.3 Implementation Strategies

(i) Access Control procedures shall be established, documented, and reviewed based on business and ICT security requirements of the University;

(ii) The use of utility programs that might be capable of overriding system and application controls must be restricted and closely controlled; and

(iii) The allocation of secret authentication information/password shall be controlled through a formal management process.

3.5 ICT Security Incident Management

3.5.1 Policy Issue

Mechanism that ensures security incidents are reported and resolved on time can help to avoid major consequences that may occur. In recognition of the importance of security incidents management, the University needs a proper mechanism to enable quick reporting of security incidents as well as resolving the security incidents and reducing the possible future incidents.

3.5.2 Policy Statement

The University shall ensure that ICT security breaches are detected, reported and resolved consistently.

3.5.3 Implementation Strategies

(i) Management and users' responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents; and

(ii) The university through the Department of ICT shall define and apply procedures for the identification, collection, acquisition, and preservation of information, regarding ICT security incidents for evidence;

3.6 Information Systems Continuity Management

3.6.1 Policy Issue

The University has some information processing facilities which if they become malfunction by any reason; services offered to different stakeholders may stop. The university recognizes the importance of having its services up and running even after being impacted by crisis or disaster. This is why the University needs to ensure continuity of its information systems.

3.6.2 Policy Statement

The University shall ensure continuity for all business-critical systems.

3.6.3 Implementation Strategies

(i) The university shall establish, document, implement and maintain processes, procedures, and controls to ensure the required level of continuity for ICT security during an adverse situation; and

(ii) The university shall verify the established and implemented ICT security continuity controls at regular intervals to ensure that they are valid and effective during adverse situations.

3.7 Security of ICT Acquisition, Development, and Maintenance

3.7.1 Policy Issue

The University recognizes the need to maintain security functionalities for both developed and purchased software. In regard to this, security functionalities for software developed by staff, local vendors or purchased must comply with the requirement of the University.

3.7.2 Policy Statement

The University shall ensure that the security functionalities for developed and acquired software are in place.

3.7.3 Implementation Strategies

(i) A procedure for secure development of software and systems shall be established and applied to developments within the organization;

(ii) The ICT security-related requirements shall be included in the requirements for new information systems or enhancements to existing information systems;

(iii) Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures; and

(iv) When operating platforms are changed, business-critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or ICT security.

3.8 Human Resource Security

3.8.1 Policy Issue

Security breaches may also be originated from authorized users of the information systems. It is with this regard that the University recognizes the need to ensure that all users of its information systems are equipped with necessary knowledge of ICT security responsibilities and consequences of breach that they may cause.

3.8.2 Policy Statement

The University shall ensure that all staff, students and contractors are aware of their roles, responsibilities and accountability for information security.

3.8.3 Implementation strategies

(i) The contractual agreements with employees and contractors shall state the employee's and university's responsibilities for information security;

(ii) Students, employees and contractors shall receive appropriate awareness education and training and regular updates in ICT security policy, as relevant to their function; and

(iii) There shall be a formal and communicated disciplinary process in place to take action against users who have committed an ICT security breach.

3.9 Physical and Environmental Security

3.9.1 Policy Issue

The university recognizes the need of creating environment for its ICT equipment which is safe from natural disasters and physical access to unauthorized users. This is due to the fact that availability of ICT services can be affected by natural disasters and accidents such as fire as well as theft and deliberate destruction of information processing equipment.

3.9.2 Policy Statement

The University shall ensure safety and security of ICT facilities against threats caused by environment and natural disasters or accidents.

3.9.3 Implementation Strategies

(i) Secured areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access;

(ii) Physical protection against natural disasters, malicious attack, or accidents shall be designed and applied for office, rooms and ICT facilities;

(iii) Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference, or damage; and

(iv) Security shall be applied to off-site ICT assets taking into account the different risks of working outside the University premises.

3.10 ICT Security Compliance and Audit

3.10.1 Policy Issue

Information systems operations are guided by number of legislative statutory, regulatory and contractual requirements. The University is aware of importance of complying with ICT security legal requirements and it is committed to create environment for compliance.

3.10.2 Policy Statement

The University shall ensure that relevant legislation and regulatory requirements for ICT security are complied with.

3.10.3 Implementation Strategies

(i) Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements related to intellectual property rights and the use of proprietary software products;

(ii) The University shall ensure that regular reviews are done, on the compliance of information processing and procedures with the appropriate ICT security policy, standards, and any other ICT security requirements;

(iii) Information systems shall be regularly reviewed for compliance with the University information security standards and guidelines;

(iv) Records shall be protected from loss, destruction, falsification, unauthorized access, and unauthorized release, by legislative, regulatory, contractual, and business requirements; and

(v) Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.

4. POLICY IMPLEMENTATION, REVIEW AND MONITORING

4.1 Implementation and Reviews

4.1.1 This Policy shall come into operation immediately after being approved by the University Council and shall remain valid and binding until it is revoked.

4.1.2 This Policy will be reviewed from time to time as and when need arises. The review exercise shall be participatory in order to generate realistic results and come up with relevant and practical recommendations.

4.2 Roles and Responsibilities

4.2.1 Vice Chancellor

4.2.1.1 Shall be the overall Authority for the ICT Security Management of the University

4.2.1.2 Shall be the chair of ICT Security Governance Committee, the task which may be delegated.

4.2.1.3 Shall find a suitable method for selecting the ICT Security Secretary, most likely the institution’s Single Point of Contact for ICT Security.

4.2.2 ICT Security Governance Committee

4.2.2.1 Shall comprise of permanent members from Executive Management Team or possibly the Management Team Sitting with a focus on ICT Security Matters.

4.2.2.2 Shall develop ICT Security Strategic Plan for the university.

4.2.2.3 Shall identify current and future ICT Security technology needs for the University.

4.2.2.4 Shall monitor and evaluate ICT Security Achievements against ICT Security Strategic Plan.

4.2.2.5 Shall provide advice and recommendations to the Vice-Chancellor on pressing ICT Security Matters affecting the University.

4.2.3 ICT Security Governance Committee Secretary

4.2.3.1 Shall be responsible for overseeing the implementation of ICT Security plans

4.2.3.2 Shall coordinate and advise Management about the implementations of ICT Security Strategic Plans.

4.2.3.3 Shall be a permanent member of ICT Security Governance Committee for his/her duration of the appointment.

4.2.4 Directors/ Deans/Head of Departments/Units

4.2.4.1 Shall be responsible for the implementation of ICT Security plans to fall under areas of their responsibilities through coordination and to liaise with ICT Security Governance Committee Secretary.

4.2.4.2 Shall supervise all ICT Security issues falling under their areas of responsibilities for execution.

4.2.5 Employees

4.2.5.1 All employees shall have basic ICT security awareness training, any suspicious issue related to ICT security to the relevant authorities.

4.3 Monitoring and Evaluation

4.3.1 ICT Security Governance Committee shall meet at least quarterly to monitor and evaluate the implementation of this ICT Security Policy.