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

INFORMATION AND COMMUNICATION TECHNOLOGY POLICY AND PROCEDURES

(Made under section 54 of the Universities Act, 2005)

2nd Edition

2019

FOREWORD

The Moshi Co-operative University (MoCU) became a full-fledged University in 2014 and launched its first ICT Policy in 2015. Since then, the ICT Policy has been used as a guide for identification, promotion and usage of ICT in planning and implementation of academic, research, consultancy and administrative functions. 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.

Nevertheless, since the development of this policy, there have been significant changes 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 arised to review and update the ICT Policy to accommodate new and important developments and help the University to implement its mandated functions.

The revised Policy has captured various issues namely ICT Infrastructure Development, Access and Usage of ICT Facilities, Software Development and Acquisition, ICT Procurement, ICT Skills Capacity Building, Content Development and Communication, Data Communication Networks, Electronic Services and Management, Telecommunications and Unified Communications, Special Needs ICT Usage, ICT Infrastructure Maintenance and Management, ICT Security and Safety; and Disposal of ICTs waste.

It is anticipated that this Policy will help the University to move toward its Vision which urge the University to become a Centre of Excellence in Co-operative Education and Practice. Therefore, it is the responsibility of every MoCU member to adhere to the ICT Policy to meet the envisioned dream.

Professor Alfred S. Sife
Ag. Vice Chancellor

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

DVC-A	Deputy Vice Chancellor (Academics)
E-learning	Electronic Learning
E-mail	Electronic Mail
ICT	Information and Communication Technology
IEEE	Institute of Electrical and Electronics Engineers
LAN	Local Area Network
LPO	Local Purchase Order
MoCU	Moshi Co-operative University
MUCCoBS	Moshi University College of Co-operative and Business Studies
MUSARIS	Moshi University Students Academic Records Information System
SDGs	Sustainable Development Goals
SDLC	Software Development Life Cycle
UPS	Uninterrupted Power Supply
VOIP	Voice Over Internet Protocol
VPN	Virtual Private Network

DEFINITIONS OF TERMS

Antivirus A computer software used to prevent, detect and remove malicious software.

Bandwidth The amount of data that can be transferred over a network in a given time period (usually a second). Bandwidth is usually expressed in bits per second (bps), or as some larger denomination of bits, such as Kilobits/second (Kbps), Megabits/second (Mbps), or Gigabits/second (Gbps).

Electronic mail A method of exchanging digital messages from an author to one or more recipients.

Firewall A network security system that controls the incoming and outgoing network traffic based on an applied set rule.

Gateway A network node equipped for interfacing with another network that uses different communication protocols.

Internet A massive Network of Networks that connects millions of computers globally.

LAN A computer Network that covers a small geographical area likes single building, office or school.

Network A set of computers connected together so as to share the available resources such as printer and software.

Network Backbone A central conduit part of Computer Network Infrastructure which interconnects different Networks and provides a path for exchange of the data between different Networks. It is designed to carry Network traffic at higher speed so as to maximize the reliability and performance of large scale data communications.

Off-the-Shelf Software A Software products which are ready-made and available for sale to the general public.

Software Any set of machine-readable instructions that direct a computer's processor to perform specific operations.

Spam Unauthorized and/or unsolicited electronic mass mailings.

Virus A malicious software designed to affect the host software.

Wireless networks Wireless LAN also known as Hotspot or Wi-Fi are networks rolled out using radio waves to provide mobile network access as defined under IEEE 802.11 protocol.

1.0 INTRODUCTION

1.1 Background Information

The history of the Moshi Co-operative University (MoCU) dates back to 5th January 1963 when the Co-operative College Moshi started to provide training to the co- operative sector in the country under the then Ministry of Co-operatives and Community Development. The Co-operative College Moshi was legally established through the Co-operative College Act No. 32 (Repealed) of 1964 as an autonomous institution with its own Governing Body.

In 2004, the Co-operative College Moshi was transformed into the Moshi University College of Co-operative and Business Studies (MUCCoBS) as the Constituent College of the Sokoine University of Agriculture through Declaration Order No. 22 of 2004. MoCU came into being as a result of transforming MUCCoBS to a full-fledged University on 4th September, 2014. The University is governed by its own Charter, made under the Universities Act No. 7 of 2005 (Cap 346) of Tanzania laws.

The existing MoCU ICT Policy of 2015 with eight different issues was formulated with the aim of guiding the identification, promotion and appropriate utilization of ICT at the University. The Policy aimed at ensuring that ICT applications are integrated into planning and implementation of the University mission to improve the quality of activities. However, since then several technological, institutional and structural changes have occurred globally, nationally and within the University that have influence on ICT development at MoCU. Globally, there have been phenomenal ICT developments in terms of availability, emergence and obsolescence of technologies. There are also technological convergences that increasingly blur distinctions between different types of ICT. The revised Policy having twelve different issues and strategies for implementation will guide the development and appropriate utilization of ICT at MoCU. This Policy will also enable MoCU to harness the potential of ICT to provide high standard services to students, staff and the wider community.

1.2 Vision and Mission Statements

1.2.1 Vision

The vision of the University is "to become a Centre of Excellence in Co-operative Education and Practice".

1.2.2 Mission

The mission of the University is "to provide quality education, training, research and advisory services to enhance co-operative development”.

1.3 Core Values

In fulfilling the vision and mission, the University is guided by the following core values: cooperation, objectivity, pursuit of excellence in service delivery, integrity and accountability, courtesy to all, and social responsibility.

1.4 Motto

The motto of the University is "Ushirika ni Biashara"

2.0 THE POLICY FRAMEWORK

2.1 Overview

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 and regularly review the ICT policy to guide the design, development, implementation, and effective utilization of ICT infrastructure and services. The ICT Policy of the University shall therefore, focus on addressing the quest for knowledge in the various disciplines.

2.2 Policy Statement

The ICT policy is intended to support teaching, learning, research, consultancy, outreach as well as administrative activities of the University. ICT infrastructure and services shall form part of the University critical assets which will be subject to security and safety for protection of confidential information and other related risks.

2.3 Policy Goals

This policy is intended to achieve the following goals:

(a) Develop a pool of trained ICT manpower at all levels to meet the requirements of the University and interested stakeholders;

(b) Provide opportunities for teaching, professional, and technical growth to ensure capacity building of the University ICT services;

(c) Develop an enabling regulatory framework for ICT management;

(d) Establish an efficient and cost-effective ICT infrastructure that provides equitable access to local and wide area networks;

(e) Set up the University database for various operations that is reliable, secure, up-to-date and easily accessible; and

(f) Promote widespread use of ICT applications in the University operations.

2.4 Policy Objectives

The objectives of this policy are to ensure:

(a) Smooth and effective management of ICT resources;
(b) Computer users have access to ICT facilities;
(c) Proper and regular maintenance of ICT facilities and infrastructure;
(d) Appropriate utilization of ICT facilities;
(e) Suitable interaction between the University and the outside world through ICT facilities;
(f) Students benefit from ICT facilities;
(g) Adequate security requirements across the University's ICT infrastructure; and
(h) Contents of the University's information are accurate, consistent and up-to-date.

2.5 Policy Principles

for administrative matters, the ICT department will be accountable to the Deputy Vice Chancellor (Academic) and governed by the following basic principles:

(a) Acquisitions including maintenance services shall be subject to the approval of Deputy Vice Chancellor (Academics) upon recommendations from the ICT department;
(b) Purchases or acquisitions shall be done on the basis of budgetary allocations;
(c) ICT users have a responsibility of ensuring safety and care of the ICT facilities; and
(d) 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 ICT department.

2.6 Scope of the Policy

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. This includes all University staff and students; any other organizations accessing services over the University ICT resources; persons contracted to develop, repair or maintain the University's ICT resources; and suppliers of outsourced ICT services. This policy applies to all ICT equipment, software or other facilities owned or leased by the University. Adherence to this policy applies to all these and other relevant parties.

2.7 Rationale and Justification

This policy expounds various courses of action that the University will take when dealing with all matters relating to ICT within and outside the University. The policy is intended to guide the entire process regarding the provision and use of ICT services. The policy has been prompted by the fact that, more members of the University are increasingly having access to the ICT services. Besides, ICT services have expanded to cater for a growing student and staff population which call for orderly acquisition, maintenance and use of ICT resources. These facts also meet the National ICT Development Policy of 2016, which among others encourages public, private and community sectors to invest in ICT infrastructure for national development. Likewise, it encourages development of ICT networking, human capital, legal framework, leadership and universal access. In view to these developments and inter-linkages for national development, there is a need to have a common guiding policy for such undertakings, which will facilitate the implementation of the University Corporate Strategic Plan and the National ICT Development Policy of 2016. The policy is also intended to meet the demands of the Tanzania Development Vision 2025, and Sustainable Development Goals (SDGs).

2.8 Policy Issues

The Policy captures the following issues:

(a) ICT Infrastructure Development;
(b) Access and Usage of ICT Facilities;
(c) Software Development and Acquisition;
(d) ICT Procurement;
(e) ICT Skills Capacity Building;
(f) Content Development and Communication;
(g) Data Communication Networks;
(h) Electronic Services and Management;
(i) Telecommunications and Unified Communications;

(j) Special Needs ICT Usage;
(k) ICT Infrastructure Maintenance and Management; and
(l) ICT Security and Safety.

3.0 POLICY ISSUES, STATEMENTS AND STRATEGIES

3.1 ICT Infrastructure Development

ICT infrastructure embraces availability of computer rooms, networks connectivity and broadcasting, equipment and supplies. This raises the issues of technology standardization of equipment, procurement, services, maintenance and disposal. The availability of appropriate network infrastructure, equipment and network access services such as e-mail, common data service, Internet and intranet, website, e-learning and office computing systems is of paramount importance.

3.1.1 Policy statements

University shall venture to:

(a) develop and maintain efficient and effective LAN to meet increasing requirements;
(b) acquire and maintain sufficient computers to meet the increasing needs of staff and student; and
(c) regularly update ICT hardware and software to keep up with the changing technology.

3.1.2 Policy objective

The objective is to guide the development and rollout of ICT infrastructure to ensure easy accessibility, resiliency, reliability, affordability, stability, modern and high quality levels of ICT facilities and services.

3.1.3 Implementation strategies

The implementation strategies for ICT infrastructure development are in four groups namely; new developments, existing infrastructure, backbone and LAN.

3.1.3.1 Implementation strategies for New developments

The following strategies shall be implemented on the new developments:

(a) The ICT department shall prepare an action plan on appropriate developments of ICT infrastructure taking into account the usage and demand patterns, technological change, security, management and cost implications;

(b) All new systems/infrastructure must be tested before installation;

(c) Upon installation of the new systems, existing system will remain in place as a back-up; and

(d) All new buildings shall have a provision for data and telephone points, effective electrical grounding, lightening arrestors and interconnection to the optical fibre backbone.

3.1.3.2 Implementation strategies for existing infrastructure

(a) All existing buildings shall have a provision for data and telephone points, effective electrical grounding, lightening arrestors and interconnection to the optical fibre backbone;

(b) Electrical grounding and lightening arrestors of buildings shall regularly be checked; and

(c) Wireless access points shall be installed to all buildings.

3.1.3.3 Implementation strategies for backbone

(a) The University Network Backbone shall connect to buildings, not to individual departments or units;

(b) Connection to the University Network Backbone shall be approved and controlled by the Head of ICT Department;

(c) The ICT Department shall adhere to and maintain copies of all relevant networking standards, and keep abreast of national and international developments in these standards; and

3.1.3.4 Implementation strategies for Local Area Networks (LANs)

(a) The ICT Department will take responsibility for the LANs within existing buildings to allow connection to the LAN gateways;

(b) Wherever feasible, the network(s) within each building shall be arranged so that there is a point of connection to the Network Backbone. In cases where it is not possible to establish a single connection, multiple building gateways may be installed;

(c) Network protocols used on building networks and communicating through the gateway must use approved configuration parameters including approved network identifiers;

(d) Installing LANs connecting to the University network shall meet the overall network security and management requirements of the University; and

(e) In cases where there are constraints to connecting any building to the University Network Backbone, consultations and subsequent approvals by the ICT department shall be made to allow for alternative configurations.

3.2 Access and Usage of ICT Facilities

Access and usage of ICT facilities and services shall be open to all students, staff, participants attending short courses, members of partner institutions visiting for official assignments and others under certain restrictions to be prescribed by the University.

3.2.1 Policy statements

The University shall endeavour to:

(a) ensure that ICT facilities and services are used by authorized individuals depending on their work and study requirements; and

(b) ensure that ICT facilities and services are accessed and used to carry out legitimate activities.

3.2.2 Policy Objective

The objective is to define and implement an effective ICT facilities access and usage management.

3.2.3 Implementation strategies

The implementation strategies for access and usage of ICT facilities are in two groups namely access and usage.

3.2.3.1 Implementation strategies for access to ICT facilities

(a) The ICT department shall centrally manage the provision of ICT resources to all user groups;

(b) Duly authorized officers of the University shall access or monitor electronic data held on or transiting University ICT facilities in accordance to the law;

(c) The provision of secured e-mail services shall be centrally defined, managed and periodically reviewed by the ICT Department;

(d) The University portals and media shall be centrally hosted;

(e) The University shall establish and maintain an effective dedicated web cache management service to optimize bandwidth provision;

(f) The University shall ensure the provision of secure and efficient intranet and web portal and its universal access;

(g) The University reserves the right to audit, without prior notice, any ICT equipment connected to its networks for the purposes of protection against exploitable security vulnerabilities;

(h) Other than in an emergency situations, access to communications rooms, cabinets and ICT network equipment shall be restricted to designated members of staff; and

(i) Contractors providing ICT services must obtain prior approval of the DVC (Academic) and shall obtain the appropriate authorization in compliance with procedures and regulations of the University security system.

3.2.3.2 Implementation strategies for usage to ICT facilities

(a) Users shall not access, interfere or remove any ICT facility or data or information unless they have been authorized;

(b) Users shall use ICT facilities in a manner that is consistent with their role;

(c) All use of ICT facilities shall be lawful, honest and decent and shall have regard to the rights and sensitivities of other people;

(d) Users shall not deliberately create, use or distribute materials that could bring the University into dispute;

(e) Users shall not install, transmit or otherwise make available any confidential information or material that contains viruses;

(f) Users shall refrain from any activities that intentionally compromise the computer operating system's security;

(g) Users shall refrain from transmitting, posting or otherwise displaying threatening materials, obscene, discriminatory, or defamatory;

(h) No equipment shall be attached to the network without explicit permission of the Head of ICT department;

(i) The University shall not guarantee protection of personal data residing on ICT infrastructure; and

(j) Users shall exercise good judgment regarding the reasonableness of personal use of ICT services.

3.2.3.3 Implementation strategies for suspension and/or termination to access and usage of ICT facilities

(a) Users' access and usage to the University's ICT facilities will be revoked automatically at the end of studies, employment or research contract or in violation of this policy;

(b) The University reserves the right to revoke a user's access to the University's ICT network where the user is suspended pursuant to a disciplinary investigation;

(c) Appropriate procedures shall apply in restricting usage after a formal complaint has been lodged or a breach of policy or rule has been reported or detected.

3.3 Software Development and Acquisition

The University recognizes the need to achieve a common methodology for both development and off-the-shelf software acquisition. In regard to this, software in use could be developed by staff, local vendors or purchased off–the-shelf.

3.3.1 Policy statements

The University shall strive to:

(a) Set direction for standardizing software development, resulting in better resource utilization and higher-quality software products delivered to end users; and

(b) Periodically define the Systems Development Life Cycle.

3.3.2 Policy objective

The objective is to set procedures and guidelines for proper software development and acquisition in order to increase efficiency, information assurance, value for money and enhance rationalization of ICT.

3.3.3 Implementation strategies

The implementation strategies for software development are grouped into in-house developed and off- the -shelf purchased software as follows:

3.3.3.1 Implementation strategies for in-house developed software

(a) The ICT Department shall collaborate with other stakeholders where needed in the development of in-house software;

(b) All developed software shall be patented according to intellectual property laws and regulations of the United Republic of Tanzania;

(c) Standard Software Development Life-Cycle (SDLC) methodology shall be applied to plan, analyse, design, manage and implement custom-built software;

(d) All stages of software development shall be documented by the developers; and

(e) The head of ICT Department shall ensure safe custody and authorized usage of all software licenses, copyright and usage keys.

3.3.3.2 Implementation strategies for off-the-shelf software

(a) The ICT department shall coordinate the procurement and implementation of common software applications used by the University;

(b) All software acquisitions shall have an appropriate level of maintenance or support agreement as part of the purchase or development approval process.

(c) No pirated or unlicensed software shall be installed on individual workstations or on servers;

(d) All University licensed software and/or associated documentation shall not be copied by outsiders and may not themselves make copies other than those provided for in the relevant licensing agreements;

(e) Software configurations shall be documented for easier reference;

(f) All acquired software shall contain provision for technical support and upgrades; and

(g) The University shall promote the use of open source software based on a risk based assessment;

3.4 ICT Procurement

All ICTs and services purchased by the University shall meet the user specifications. In addition, all purchases shall be in conformity with the overall standards of University procurement of goods and services as aligned to the Public Procurement Act.

3.4.1 Policy statements

The University shall endeavour to:

(a) Acquire ICTs and services in accordance to the needs of users; laws, regulations and policies governing the procurement process in the University and the United Republic of Tanzania; and

(b) Guide the procurement of all ICT goods and services towards ensuring standardization, transparency, timely delivery, quality assurance, and value for money as well as compatibility with existing infrastructure and services.

3.4.2 Policy objective

The objective is to inform and guide procurement of all ICT related goods and services in the University.

3.4.3 Implementation strategies

(a) Technical and performance specifications for procuring ICT goods and services shall be prepared by users in consultation with the ICT department;

(b) Identification of reputable companies or registered providers of ICT services shall be done by the Procurement Management Unit with assistance from the ICT department;

(c) The procurement procedures shall conform to the University's rules and regulations while ensuring that ICT projects are pursued diligently and efficiently;

(d) Inventory of all ICT goods procured must be forwarded to the Head, ICT department for record keeping purposes;

(e) ICT hardware shall be replaced in accordance with user needs and change in technology;

(f) Installation and configuration of any procured ICT equipment, software or service must comply with the approved ICT specifications, standards and guidelines;

(g) Disposal of obsolete ICT equipment shall be governed by the Public Procurement Act of 2011 and its Regulations.

3.5 ICT Skills Capacity Building

The University recognizes that ICT is a dynamic field and benefits to be derived from its usage are significant. As such, the University shall plan for ICT capacity building programmes and implement them as per and when the need arises.

3.5.1 Policy statements

The university shall endeavour to:

(a) Plan and implement capacity building for ICT skills; and

(b) Develop sufficient skills and expertise amongst staff and students to maximize appropriate usage of ICTs.

3.5.2 Policy objectives

The objective is to provide guidelines applicable for planning, organizing and conducting ICT capacity building at the University.

3.5.3 Implementation strategies

(a) The University in consultation with the ICT Department shall plan, coordinate and implement capacity building programmes for ICT skills to achieve coherency and efficient utilization of resources;

(b) Internal ICT user training targeting the University community shall be scheduled and conducted on a continuous basis;

(c) External ICT training shall be organised by the ICT department in response to need as may be assessed from time to time when training is not possible within the University; and

(d) The ICT department shall coordinate the periodic assessment of existing ICT skills capacity amongst all user groups to be able to identify gaps in partnership with other departments.

3.6 Content Development and Communication

The University develops a number of digital contents which are disseminated to various local and global stakeholders through different communication media including website, e-mail, e-learning, radio, television and social media networks.

3.6.1 Policy statements

The University shall strive to:

(a) Develop relevant, accurate, consistent and up-to-date contents related to University activities; and

(a) Use relevant platform for communicating and showcasing its activities to the World.

3.6.2 Policy objective

The objective is to guide the development of digital contents and usage of appropriate communication media to disseminate information related to University activities.

3.6.3 Implementation strategies

Implementation strategies for this policy are divided into two parts namely content development and communication.

3.6.3.1 Implementation strategies for contents development

(a) The relevant authorities shall ensure appropriateness, relevance, accuracy, consistency and timeliness of all developed and contents; and

(b) The University shall equip all designated personnel with relevant skills and tools.

3.6.3.2 Implementation strategies for communication

(a) The University relevant authorities shall ensure that the contents to be communicated/shared are relevant, accurate, consistent, up-to-date and with adherence to privacy and confidentiality;

(b) All developed digital contents shall be uploaded by authorised personnel after the approval by the DVC (Academic);

(c) The University shall equip all designated personnel with relevant up to date communication media skills and knowledge;

(d) Only the University official media shall be allowed to make use of university logo and symbols;

(e) All the University websites and portals shall be centrally hosted and suitable social media accounts being opened to enhance communication with the general public;

(f) The University shall establish the appropriate common e-learning platform to support the teaching and learning process; and

(g) Any information shared across the University media shall comply with University and national policies and should not make reference to any biased statements on matters such as politics, religion, race, gender, sexual orientation and statements that contain obscenities or vulgarities.

3.7 Data Communication Networks

Data Communication Networks and Services have evolved into the backbone for the provision and usage of daily ICT services at the University. In that case, the University reorganizes that there is a need for fast rate of innovation and more effective technological developments.

3.7.1 Policy statements

The University shall endeavour to:

(a) provide a resilient, secured and stable fast data communications network and services;

(b) facilitate processing, storage, dissemination and accessing of information relating to various needs of the teaching, learning, administration and research domains.

3.7.2 Policy objective

The objective is to guide the usage and management of the University Backbone to ensure resiliency, stability and higher uptime rates of data communication network services.

3.7.3 Implementation strategies

(a) The University shall take into consideration the ever changing computing needs, growth in usage demand of the backbone as well as technological advances that introduce smarter and innovative practices;

(b) The University shall establish and maintain one central data repository for all databases and web hosting;

(c) The University shall provide connectivity to the Internet to prioritized areas;

(d) The University shall support the provision of secure remote access to authorized users for approved University resources;

(e) To establish and maintain an effective methods to optimize bandwidth provision with prioritization to university applications such as e-mail;

(f) All internal and external data communications shall be channelled through University approved links;

(g) The ICT department shall monitor and document network performance and usage and shall maintain regular reports;

(h) Official electronic records shall be retained in accordance with the University records retention schedules;

(i) The ICT department shall periodically define the methodology for access to external data destinations and data routes.

3.8 Electronic Services and Management

The University recognizes the need for digitization of its functions to reduce paper usage and manual work. In that case, the University commits itself to the provision of appropriate electronic services and ensure efficient management. This will be achieved through empowering the ICT department, relevant authorities and end users.

3.8.1 Policy statements

The University shall strive to:

(a) Define appropriate electronic services for different functions and promote their usage;

(b) Define and implement an electronic service management process and procedures; and

(c) Support the ICT department define and implement a business model for the provision of electronic services to external clients.

3.8.2 Policy objective

The objective is to define and implement an effective electronic service and management and support approach to ensure efficiency, stability and continuity on University operations.

3.8.3 Implementation strategies

(a) Raise awareness about electronic services among various categories of users;

(b) Equip staff and students with knowledge and skills on access and usage of electronic services;

(c) Ensure proportional allocation of financial resources for electronic services and management;

(d) Encourage the utilization of open access e-resources;

(e) Define how service support operations are to be carried out by authorized personnel;

(f) The ICT department shall ensure protection mechanisms for all the electronic services; and

(g) Provide technical support in line with approved ICT procedures for any system, service, device downtime or breach.

3.9 Telecommunications and Unified Communications

The University envisions the use of Telecommunications and Unified Communications Services towards implementation of an ICT enabled communications service. These services include telephone, teleconference, videoconference, facsimile, and VOIP services. These services will be provided to support the communication needs required for the smooth operations across the University.

3.9.1 Policy statements

The University intends to:

(a) Establish a secure and stable unified communication systems to support the University functions; and

(b) Support and promote the usage of Unified Communications service.

3.9.2 Policy objective

The objective is to implement Unified Communications service, on digital network to provide secure, convenient and highly available communication.

3.9.3 Implementation strategies

(a) Design and implement the University wide telephony service and numbering plan to support both intercom services and external calls;

(b) Design and implement a unified communication systems that support new integrated communications channels;

(c) Ensure proper license usage for all unified communications components;

(d) Provide technical assistance for any expansion of the communications services within the university;

(e) Periodically review communications services to ensure uniformity for the service provision and compatibility with existing infrastructure; and

(f) Undertake routine maintenance, upgrade and daily monitoring of the communications service usage.

3.10 ICT for People with Special Needs

Universally, the development in ICT supports the extension of access to all users. The University recognizes that, the provision of ICT services should take into account the needs of special user groups such as the visually, motor and auditory impaired.

3.10.1 Policy statements

The University envisions to:

(a) Define and implement provisions for ICT usage for special user groups towards enabling equal access to information and knowledge; and

(b) Support and promote inclusion of people with special needs in all ICTs.

3.10.2 Policy objective

The objective is to provide ICTs working environment that supports people with special needs.

3.10.3 Implementation strategies

(a) Define the appropriate technology aligned to needs of special user groups from time to time;

(b) Ensure the provision of the appropriate access for special user groups for all ICTs; and

(c) Ensure the provision of appropriate mechanisms within all Electronic Services for special user groups.

3.11 ICT Infrastructure Maintenance and Management

The University recognizes the importance of maintenance and repair of ICT facilities in due time. To ensure safe and proper usage, the University requires a well-planned maintenance plan. To that end, all ICT infrastructure and facilities shall be appropriately maintained and properly managed.

3.11.1 Policy statements

The University envisages to:

(a) Put in place an elaborate programme of renovation and replacement of obsolete and out-dated ICT equipment; and

(b) Make available adequate resources for regular maintenance of ICT facilities.

3.11.2 Policy objective

The objective is to ensure that all ICT facilities are regularly maintained to ensure all systems operates smoothly with less downtime.

3.11.3 Implementation Strategies

(a) The ICT department shall define and disseminate updated ICT facilities maintenance guidelines from time to time;

(b) The University shall make provision for adequate resources to ensure regular maintenance of ICT facilities;

(c) The ICT Department shall undertake a periodic assessment of all the ICT facilities to ensure compliance with the set maintenance guidelines; and

3.12 ICT Security and Safety

Security and safety is about protection of ICT infrastructure, data and the user community against attacks from internal or external sources. ICT facilities like computer rooms, workstations, servers, switches, hubs, routers, firewalls, network wiring systems and other small or large ICT equipment shall be secured.

3.12.1 Policy statements

The University shall venture to:

(a) Ensure protection, resiliency and stability of all ICT facilities, information and services against any threats; and

(b) Develop proper ICT security and safety procedures and disaster recovery plans.

3.12.2 Policy objective

The objective is to give high priority for preventing threats thereby ensuring safety and security of ICT facilities.

3.12.3 Implementation Strategies

(a) The ICT department shall set out procedures and operation manual with the consideration of preventing anticipated threats that may damage ICT facilities;

(b) All user authentication methods such as passwords and biometric finger prints shall be seriously treated as private and confidential and must not be exposed, shown or given to any party other than the user;

(c) Passwords protecting critical University systems must be strong (at least 8 characters in length), automatic lockout user accounts on five (5) unsuccessful login attempts, and automatic session timeout after 10 minutes of inactive or idle;

(d) Authorized users are responsible for the security of their passwords and accounts. System level passwords shall be changed on three months (90 days) basis, and user level passwords shall be changed at least once in every three months (90 days);

(e) The ICT Department shall plan and ensure backup and recovery of University operational data;

(f) Servers and other critical systems shall be housed in a server room containing adequate air conditioning. No water, rainwater or drainage pipes shall run within or above computer server rooms to reduce the risk of flooding. And, access to the server rooms shall be restricted the authorized University staff only;

(g) All areas with sensitive equipment and systems shall be labelled as secured and shall be entered only by authorized personnel;

(h) All ICT facilities shall be adequately protected against fire, water and physical damage;

(i) Network infrastructure shall be secured against e-mail spam, intruders or hackers, break-ins, viruses, and other disruptive software;

(j) System audit facilities shall be enabled on all systems to record all log-in attempts and failures, and to track changes made to systems;

(k) All network cables shall be periodically scanned and whenever needed corrective measures be taken;

(l) All servers, workstations, switches, routers, firewalls and other critical network equipment shall be fitted with UPS to condition power supply;

(m) Computer hardware and software audits shall be carried out periodically to track unauthorized copies of software and changes to hardware and software configurations;

(n) Procedures consistent with security best practices shall be followed for reliable removal of licensed software and confidential data before equipment transfer or disposal takes place; and

(o) All computer laboratories shall be monitored by administrators who will be responsible for the security of laboratories and impact on the network.

4.0 POLICY ENFORCEMENT

Violators of this ICT Policy shall be subjected to any of following actions:

(a) Withdrawal or suspension of facilities access and usage: The system and network privileges of the user will be withdrawn, suspended, or restricted following consultations with the Head, ICT department;

(b) Disciplinary action: Disciplinary action against the user shall be escalated to the Deputy Vice Chancellor (Academic) to be dealt with under the University's disciplinary procedures;

(c) Breaches of the law: Where appropriate, breaches of the law will be reported to the police. Where the breach has occurred in a jurisdiction outside Tanzania, the breach will be reported to the relevant authorities within that jurisdiction;

(d) A student who abuse of ICT privileges is subject to disciplinary action, which may include the loss of these privileges and other disciplinary sanctions up to and including dismissal;

(e) A student who abuses the University's computing, information, and communications resources may also be subject to civil action and/or criminal prosecution; and

(f) The University will pursue criminal and civil prosecution of violators when appropriate. Individuals will also be responsible for any financial loss to the University that results from inappropriate use of ICT resources.

5.0 IMPLEMENTATION, MONITORING AND REVIEW

The ICT department shall be responsible for coordinating and implementing this ICT Policy and procedures. It will also advice and assist all units/department/faculty/directorate/bureau and other stakeholders across the University on ICT matters. The department shall work with other stakeholders in monitoring and evaluating policy activities. Relevant indicators shall be developed and be made available to enable stakeholders at all levels monitor and assess ICT development activities on a regular basis.

5.1 Role of ICT Department

In relation to this policy, the ICT department shall be responsible for the:

(a) implementation of ICT policies, strategies and standards;
(b) formulation and preparation of relevant guidelines and procedures towards the implementation of this policy;
(c) management of the network and internet facilities;
(d) management of the University e-mail system;
(e) provision of Internet access or connection;
(f) development, implementation and support of network systems and technologies; and
(g) provision of ICT support to academic, research, and administrative units of the University.

An overall policy review will be undertaken after every five years or earlier, as need arises. However, the ICT department may, from time to time, propose amendments that are necessary to enhance the objectives of this policy. Before the enactment of such amendments, the department shall provide opportunities to major stakeholders to comment on the proposal. Members of the University community who wish to propose amendments may submit their proposed amendments to the ICT department.

6.0 COMMENCEMENT DATE

This ICT policy shall commence after the approval by the University Council.

7.0 AUTHENTICATION

……………………………….. ……………………………………

Council Chairperson Council Secretary

…………………………… …………………………………..

Date Date