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

INFORMATION COMMUNICATION TECHNOLOGY POLICY AND PROCEDURES 2015

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

MARCH, 2015

FOREWORD

The positive impact of the use of information and communication technologies on education and economic development is now well established. MoCU ICT policy has always been reviewed and updated several times to take into account new important issues such as various user policies, security issues, service level agreements, and policies for the use of ICT in education and administrative services.

This ICT policy assures the availability of all anticipated ICT services/systems at any workplace in the university, and, for selected services; availability of user-level Data Communication Services such as Email, Access-to-Internet, Internet/Intranet Services; promote office computing in all offices; improve both the efficiency and effectiveness of library operations and services through the implementation of an integrated online Library Information System; enhance and streamline student education related administrative and managerial processes and to improve academic reporting facilities at both central and faculty level through the implementation of an integrated Moshi University Academic Records Information System (MUSARIS).

The University therefore is committed to provide for the growth and financial sustainability of the ICT resources through appropriate funding and operational mechanisms to ensure availability of internet bandwidth within the institution ICT infrastructure and train students, academic, administrative, and managerial staff so that they fully exploit the ICT environment in their different functions.

However, it is the responsibility of every MoCU member to adhere to the ICT policy technical and organizational preconditions

Prof. F.K Bee (PhD)
Ag. Vice Chancellor

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

ATM	Automatic Teller Machine
BYOD	Bring Your Own Device
DVC	Deputy Vice Chancellor
FTP	File Transfer Protocol
GFS	Grandfather-Father-Son
ICT	Information and Communication Technology
IEEE	Institute of Electrical and Electronics Engineers
IS	Information System
ISO	International Standardization for Organization
IP	Internet Protocol
IPR	Intellectual Property Right
IPSec	Internet Protocol Security
LAN	Local Area Network
LPO	Local Purchase Order
MoCU	Moshi Co-operative University
MUCCoBS	Moshi University College of Co-operative and Business Studies
NFS	Network File System
POC	Point of Contact
SSH	Secure Shell
Telnet	A terminal emulation program for TCP/IP networks such as the Internet
TCP	Transmission Control Protocol
TCU	Tanzania Commission for Universities
UPS	Uninterrupted Power Supply
VPN	Virtual Private Networks
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
WWW	World Wide Web

DEFINITIONS OF TERMS

In this policy unless directed otherwise, the below mentioned terms shall mean the following;

Antivirus	Is computer software used to prevent, detect and remove malicious software.
Backbone	The University network will consist of several parts: "Backbone" systems, a collection of inter-building connections; "Campus LANs," a collection of "inter-campus" connections; wireless networks (Hotspots); Virtual Private Networks (VPN), data centers and campus Network Operation Centers (NOC)."The University Network Backbone will comprise an inter-building cabling system, together with one or more "Gateway" interfaces at each building or in the path to each building which will connect the Backbone to the network(s) within each building.
Bandwidth	Is 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).
Chain letters	Messages that purport to tell the addressee how, for a relatively small investment, the addressee can make huge amounts of money. There are several variations, but they are all based on a common fraudulent concept — that the addressee pays a relatively small amount of money to a few people above the addressee in a chain, with the expectation that later a very large numbers of people will be making similar payments to the addressee.
Denial of service	Procedures or actions that can prevent a system from servicing normal and legitimate requests as expected.
Electronic mail	Is a method of exchanging digital messages from an author to one or more recipients.
Firewall	Is a network security system that controls the incoming and outgoing network traffic based on an applied rule set.
Gateway	A network node equipped for interfacing with another network that uses different communication protocols.
Network sniffing	Attaching a device or a program to a network to monitor and record data traveling between computers on the network.
Ping attack	A form of a denial of service attack, where a system on a network gets "pinged," that is, receives a echo-request, by another system

	at a fast repeating rate thus tying up the computer so no one else can contact it.
Port scanning	Attempting to learn about the weaknesses of a computer or a network device by repeatedly probing it with a series of requests for information.
Software	Is any set of machine-readable instructions that directs a computer's processor to perform specific operations.
Spam	Unauthorized and/or unsolicited electronic mass mailings
Spoofing	The deliberate inducement of a user or a computer device to take an incorrect action by Impersonating, mimicking, or masquerading as a legitimate source.
Wi-Fi	Local area wireless technology that allows an electronic device to participate in computer networking using radio waves.
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 and Communication Technology (ICT) is the acquisition, processing, storage and dissemination of vocal, pictorial, textual and numeric information by a micro-electronics based combination of computing and telecommunications. ICT change, with time resulting into significant shift of emphasis. Computers are being predominantly used for text manipulation and electronic mail. The merging of computing, information, communication and technology have made ICT an essential part of our social infrastructure development. Several organisations including academic institutions are increasingly using ICT for conducting their activities including teaching, research and consultancy services.

The use of ICT at the University is increasing in response to the demand of students and staff. It is therefore imperative for the University to have in place the necessary infrastructure, which can sustain the growing demand. The ICT policy of the University shall therefore, focus on addressing the basic needs of staff and students in the quest for knowledge in their various disciplines.

1.2 Establishment

The Moshi Co-operative University (MoCU) is one of the higher learning institutions in Tanzania. MoCU came into being as a result of transforming Moshi University College of Co-operative and Business Studies (MUCCoBS) to full-fledged University in September, 2014. The former University College was a result of upgrading the status of the then Co operative College Moshi into Moshi University College of Co-operative and Business Studies into a Constituent College of Sokoine University of Agriculture (SUA) as declared through Declaration Order No. 22 of 2004.

1.3 Vision and Mission Statements

1.3.1 Vision

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

1.3.2 Mission

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

1.4 Core Values

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

1.5 Motto

The motto of the University is "Ushirika ni Biashara"

2.0 THE POLICY

2.1 Policy Statement

The ICT policy is intended to support teaching, learning, research, consultancy, outreach as well as administrative activities of the university. Data shared in the performance of such activities shall form part of the university critical assets and are subject to security breaches that may compromise confidential information and expose the university to losses and other legal risks.

2.2 Policy Goals

In its endeavour to realise the vision, the following ICT goals are set to:

(a) Make the computer centre a facilitator and an enabler in providing maximum opportunities to the development of ICT in the University;
(b) Develop a pool of trained ICT manpower at all levels to meet the requirements of the University and interested stakeholders;
(c) Provide opportunities for teaching, professional, and technical growth to ensure capacity building of the University ICT sector;
(d) Develop an enabling regulatory framework for ICT management;
(e) Establish an efficient and cost-effective ICT infrastructure that provides equitable access to local and wide area networks;
(f) Set up the University database that is reliable, secure, up-to-date and easily accessible; and
(g) Promote widespread use of ICT applications in faculties and departments for efficient teaching, researching and learning.

2.3 Policy Objectives

The objectives of this policy are to:

(a) ensure smooth and effective management of ICT resources;
(b) ensure that MoCU computer users have access to ICT facilities;
(c) ensure proper and regular maintenance of computer facilities and infrastructure;
(d) ensure proper utilization of ICT facilities by MoCU community members;
(e) ensure proper interaction between MoCU and the outside world through ICT facilities; and
(f) ensure that students benefit from ICT training and research facilities.

2.4 Policy Principles

The ICT unit will be accountable to the Deputy Vice Chancellor Academics and governed by the following basic principle:

(a) Subject to the provisions of the Public Procurement Act No. 7 of 2011 and Regulations GN 466 of 2013 of the United Republic of Tanzania, all acquisitions, including maintenance services, will be subject to the approval of Deputy Vice Chancellor Academics upon recommendations from the ICT unit;

(b) All purchases/acquisitions will 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) All users have a duty of reporting to the relevant authority any mishandling, damage, theft, tempering or any other act which is detrimental to the well being of the ICT unit.

2.5 Scope of the University ICT Policy

This policy applies to any person accessing/developing/implementing and/or using ICT-based information and ICT 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 that is owned or leased by the University.

Adherence to this policy applies to all these and other relevant parties.

2.6 Rationale for ICT Policy

The overall strategy for ICT is to provide staff and students with the appropriate facilities necessary for teaching, research and outreach activities. These facilities shall be easily accessible from the personal computer or computer laboratory through a common user-friendly interface. In order to access a wide variety of local and international networks, a high-speed communication network shall be made available. It is anticipated that this will be achieved on phases as indicated in the University Corporate Strategic Plan 2014/15 to 2018/19.

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 2003, which among others encourages public, private and community sector 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 2003. The policy is also intended to meet the demands of the Tanzania Development Vision 2025, and Millennium Development Goals (MDG's).

2.7 Policy Issues

This policy will capture the following issues:

(a) ICT infrastructure development;
(b) Connection to and Usage of ICT Facilities;
(c) Software development;
(d) Procurement of ICT tools, facilities and services;
(e) ICT Training;
(f) Website contents; and
(g) ICT security and internet.

3.0 POLICY ISSUES, STATEMENTS AND STRATEGIES

3.1 ICT Infrastructure Development

3.1.1 Policy Statement

University shall venture to:

(a) develop and maintain efficient and effective LAN to meet increasing Internet requirements;
(b) acquire and maintain sufficient computers to meet the needs of the increasing staff and student population;
(c) provide an efficient and effective telecommunication system within the University;
(d) regularly update ICT hardware and software to keep up with the changing technology environment;
(e) improve and manage Internet services to meet ever-increasing requirements;
(f) build and maintain institutional capacity for managing ICTs effectively;

(g) ensure availability of power backup and stabilizer mechanisms to increase the availability Internet services and protect ICT equipment; and
(h) maintain a broadcast facility to support the University mission.

3.1.2 Implementation Strategies

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

3.1.2.1 Implementation strategies for new development

Towards implementing the ICT policy on new development, the following strategies will be employed:

(a) The ICT unit will prepare a rolling four (4) years network development plan, advising on appropriate developments aiming at ensuring the adequacy of the University's ICT infrastructure taking into account the usage and demand patterns; technological change; security; management and cost implications;
(b) Prior to installation of the "live" situation, major network developments shall be "soak-tested" in off-line simulation;
(c) For up to two months after the live installation of the new development, the network provision that it is to be replaced shall, wherever possible, remain in place as a "back-up" in the event of any subsequent failure of the new development when it is subject to actual user demand ; and
(d) All new buildings shall make provision for data and telephone points at the offices, meeting rooms and lecture halls, effective electrical grounding and lightening arrestors and interconnection to the optical fibre network backbone.

3.1.2.2 Implementation strategies for existing buildings

(a) All existing buildings shall make provision for data and telephone points, effective electrical grounding and lightening arrestors, lecture rooms be equipped with data and telephone points and interconnected to the MoCU optical fibre backbone network;
(b) The estate officer shall ensure that the grounding and lightening arrestors of buildings are regularly tested; and
(c) The University shall be turned into a managed access hot-spot area based on high capacity High Power wireless ports outdoor Wi-Fi Multi-band Base Station compliant with 802.11a/b/g/n standard.

3.1.2.3 Implementation strategies for backbone

(a) The University Network Backbone shall connect, singly or severally, to buildings, not to individual departments or units;
(b) The planning, installation, maintenance and support of the University

Network Backbone shall be under the control of the ICT unit;

(c) Connection to the University Network Backbone shall be approved by the Head, ICT Unit;

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

(e) The University Network Backbone at any particular point of time will be aimed at facilitating the traffic flow between connected buildings or networks.

3.1.2.4 Implementation strategies for campus LANs

(a) The respective network manager will take responsibility for the Campus LANs, namely, the necessary wiring and related equipment 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 University 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) Building networks connecting to the University network shall meet the overall University network security and management requirements; and

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

3.1.2.5 Implementation strategies for wireless networks

(a) Installation, configuration, maintenance, and operation of wireless networks serving on any property owned or rented by the University, are the sole responsibility of ICT unit. Any independently installed wireless communications equipment is prohibited;

(b) Any request for installation of wireless device must be approved by Head, ICT unit;

(c) Wireless access points shall terminate at a point of connection to the University Network Backbone. In cases where it is not feasible to establish a single connection, multiple wireless gateways may be installed limited to a maximum of three hops; and

(d) Wireless networks connecting to the University network shall meet the overall University network security and management requirements including approved network identifiers.

3.1.2.6 Strategies for access to ICT facilities

(a) All communication rooms and cabinets shall be locked at all times;

(b) Entry to communication rooms and cabinets, and interference with ICT network equipment is strictly prohibited;

(c) Other than in an emergency situations, access to communications rooms, cabinets and ICT network equipment shall be restricted to designated members of staff of the ICT unit. Any necessary access must have prior written consent of the Head, ICT unit;

(d) In the event of a fire or other emergency, security staff and/or staff of the Estates Department and/or the emergency services may enter these areas, without permission, to deal with the incident;

(e) Where ICT network equipment is housed in rooms used for other purposes, the arrangements for access by the other user of the room shall require prior written consent of the Head, ICT unit. This consent shall specifically exclude access by the other user to any communications cabinets or ICT network equipment located in the shared room;

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

(g) Contractors shall observe any specific access conditions which apply within the areas in which they will be working. These access conditions include, in all cases, that contractors working in main server rooms shall be accompanied by the appropriate University ICT personnel;

(h) All installations and changes of electrical power cabling in facilities housing ICT equipment shall be approved and managed by the Estates Department in consultation with the DVC Academic, in writing;

(i) The specification of any equipment to be installed in communications rooms and cabinets and the installation of such equipment, shall require the prior written consent of the Head, ICT Unit;

(j) Only designated members of the staff of ICT Unit are authorized to install and maintain active network equipment including hubs, switches and routers connected to the University's ICT networks; and

(k) Where the Head, ICT Unit agrees that academic staff or the ICT Unit's technical staff may install and maintain hubs and switches within local staff or student networks, such permission will in every case specifically exclude the point at which these hubs and switches connect to the University's network infrastructure.

3.2 Connection to and Usage of ICT Facilities

3.2.1 Policy statement

The University shall endeavour to have proper connection and usage of ICT facilities that conform to protocol and good conduct.

3.2.2 Implementation strategies

In implementing the policy in connection to and usage of ICT facilities, the following strategies will be used:

3.2.2.1 Implementation strategies for connection to the ICT network and Usage of ICT facilities

(a) All connections to the University's ICT networks must conform to the protocols defined by the ICT Unit and with the requirements that apply to Internet Protocol (IP) addresses;

(b) Only designated members of staff of the ICT Unit, or other staff authorized specifically by the Head, ICT, may make connections of desktop services equipment to the ICT network;

(c) Computer workstations connected to the ICT network will not be set up to offer services to other users, for example, to act as servers, unless the prior written consent of the Head, ICT Unit has been obtained. Such consent will normally exclude all external access;

(d) Where specific external access is required to servers on the backbone network, the Head, ICT Unit shall ensure that this access is strictly controlled and limited to specific external locations or persons;

(e) The Head, ICT will monitor compliance with access arrangements as stipulated in this ICT Policy and the relevant ICT Security Policy on Server Security issued by the University from time to time;

(f) Abuses of or failure to comply with these arrangements shall result in immediate restriction or disconnection from the network;

(g) All Domain Name Services (DNS) activities hosted within the University shall be managed and monitored centrally, for the whole University, by the ICT Unit; and

(h) Electronic mail or e-mail shall be received and stored on central servers managed by the ICT Unit from where it can be accessed or downloaded by individual account holders.

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

(a) A user's access to the University's ICT networks will be revoked automatically:

(i) at the end of studies, employment or research contract;

(ii) at the request of the Director/Dean of Faculty/Head of Resource

Centre/Head of Department or Head of Unit with specified reason(s);

(iii) where there is a breach of these regulations

(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) The Director of Human Resource Management and Administration/Director of Undergraduate Studies/Director of Postgraduate Studies will establish mechanisms to ensure that changes in student/employment status are communicated immediately to the Director of ICT so that their network access and e-mail accounts can be suspended or deleted as appropriate immediately;

(d) 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;

(e) Any breach of ICT policy shall be reported or communicated in writing to the DVC Academic;

(f) Upon receipt of any such complaint, the Head, ICT Unit shall classify the complaint as "serious" or "non-serious." A "non-serious" complaint shall be defined as a breach of policy which does not subject the University to a cost nor any high risk;

(g) When a complaint is classified as "non-serious," the Head, ICT Unit is authorized to suspend the account for a minimum period of four weeks or permanently disabling of the account;

(h) When a complaint is classified as "serious," the Head, ICT Unit shall refer the complaint to the DVC Academic for appropriate action. The possible penalties may be any or a combination of the following:

(i) Suspension of the account which will be communicated to the relevant Director/Dean and/or Head of Department or Section;

(ii) Suspension of the account shall be for a 28 days minimum, formal approval of the relevant Director/Dean and/or Head of Department or Head of Unit and a signed undertaking to abide by the rules of use shall be required before reinstatement of the account;

(iii) Permanent disabling of the account shall be taken, where the severity of the offence warrants such action;

(iv) Accounts may be reinstated before the end of the suspension period where either the student or staff presents information to the DVC Academic, which indicates that he or she was not involved in the transgression of the rules of use, or the Director/Dean and/or the Head of Department or Head of Unit requests the account be reinstated for employment/course related work only (e.g. completion of an assignment), such request shall be communicated to DVC Academic. In this case, the user is

required to sign an undertaking to abide by the rules of use;

(v) A system administrator can make a recommendation to disable an account to the Head, ICT Unit. The Head, ICT Unit shall review the request and if it is considered to be, on the balance of probability, a transgression of the ICT policy, the account shall be suspended;

(vi) An account may also be suspended, if a request has been made to the Head, ICT Unit from a systems administrator of another system, with a reasonable and accepted case for suspension; and

(vii) Users should note that suspension of access to ICT facilities also includes access to the terminal server password access, and as such dial-up modem access will be disabled where a user account is suspended.

3.2.2.3 Implementation strategies for additional or changed equipment

(a) The Head, ICT Unit shall be advised in advance and at the earliest opportunity, of any plan to add items of desktop services equipment, or to replace or to re-locate desktop equipment that are connected, or that may require connection to the University's ICT network;

(b) The Head, ICT Unit shall be informed in advance of any plan that involves a new use, a change of use or addition to the University's ICT networks that might impact on the performance or security of the network;

(c) The Head, ICT Unit shall assess the likely impact on the University's ICT networks of the proposed change. The Head, ICT Unit shall give approval for the proposed change only where appropriate adjustments can be made to accommodate any effects on network traffic that this change may cause; and

(d) The Head, ICT Unit shall assess the likely impact of the proposed use and will advise on the consequential impact upon the performance of the University's ICT network. Such changes shall be effected after approval by the Head, ICT Unit.

3.2.2.4 Implementation strategies for external data communication

(a) All external data communications shall be channelled through University approved links;

(b) No external network connections shall be made without the prior written consent of the DVC-Academic and ICT unit;

(c) The installation and use of private links on premises owned, managed or occupied by the University shall require the prior written consent of the Estates Officer;

(d) The ICT Unit shall be responsible for provision and management of the University web cache facilities for incoming web traffic;

(e) All web access shall be set up to ensure use of the University's web cache facility for incoming web traffic under the ICT Internet Usage Policy;

(f) The Head, ICT Unit shall be responsible for the implementation of appropriate filtering facilities for web-based and non-web internet traffic, including MP3 traffic and other high bandwidth intensive services that may not have direct educational or research value, where and when necessary in conformity with the ICT policy and relevant ICT guidelines that promote efficient and high availability of internet services to the majority of users; and

(g) The Network Manager, ICT Unit, shall monitor and document the University ICT network performance and usage and shall maintain regular monthly reports.

3.3 Software Development

3.3.1 Policy Statement

The ICT Unit is responsible for administering MoCU system development projects and maintaining implemented systems. All entities at the University, engaged in systems or software development activities, Standard Software Development Life-Cycle (SDLC) methodology shall be applied to planning, analysis, design, implementation and maintenance of custom-built software.

3.3.2 Implementation strategies

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

3.3.2.1 Implementation strategies for in-house developed software

(a) The ICT unit shall coordinate with other stakeholders where needed 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) Application Development Approach: Standard Software Development Life-Cycle (SDLC) methodology shall be applied to plan, analyse and design as well as management and implementation of custom-built software; and

(d) All stages of software development (requirement gathering, design, implementation and testing) shall be documented by the developers.

3.3.2.2 Implementation strategies for off-shelf software

(a) The ICT Unit shall coordinate the procurement and implementation of common software applications used by the University. Such software applications shall be run at the Directorate/Faculty/Department or Unit level where it is used;

(b) No pirated or unlicensed software shall be installed on individual workstations or on servers;
(c) Users shall not allow MoCU licensed software and/or associated documentation to be copied by outsiders and may not themselves make copies other than those provided for in the relevant licensing agreements; and
(d) Software configurations shall be documented for easier reference.

3.4 Procurement of ICT Tools, Facilities and Services

3.4.1 Policy Statement

The University shall acquire ICT tools, facilities and services according to the needs of users in accordance with the laws, regulations and policies governing the procurement process in the United Republic of Tanzania.

3.4.2 Implementation strategies

(a) Technical and performance specifications for procuring ICT goods and services shall be prepared by users in consultation with the ICT Unit;
(b) Identification of reputable companies or registered providers of ICT services shall be done by the Procurement Management Unit with assistance from ICT Unit;
(c) The procurement procedures shall conform to the University's rules and regulations while ensuring that ICT projects are pursued diligently and efficiently;
(d) ICT goods and services to be procured are of the right quality and quantity; delivered in the right time and purchased at reasonable price;
(e) Inventory of all ICT goods procured must be forwarded to the Head, ICT Unit for record keeping purposes;
(f) ICT Unit shall inspect the delivered of goods and services against the LPO to examine and test the compliance of the goods to technical and performance specifications;
(g) ICT hardware shall be replaced after every five years in accordance with user needs and change in technology. While for software the life cycle is dependent on the release of the new versions in accordance with the software maintenance agreement; and
(h) The disposal of obsolete equipment shall be governed by the Public Procurement Act of 2011 and Regulations GN 446 of 2013.

3.5 Website Contents

3.5.1 Policy Statement

The University shall maintain a comprehensive website that has web pages for all Directorates/Faculties/Departments and Units. Contents of the website shall

be accurate, consistent and up-to-date to uphold the integrity and image of the University.

3.5.2 Implementation Strategies

(a) Directorates/Faculties/Departments/Units shall ensure that the contents of their pages in the website are relevant, accurate, consistent and up-to-date;
(b) In order to ensure that the University website contains relevant, accurate, consistent and up-to-date contents there shall be a committee to oversee contents. The committee shall be constituted by the DVC Academic;
(c) The ICT Unit shall upload website contents from the Directorates/Faculties/Departments and Units after the approval by the DVC Academic; and
(d) The University shall equip the webmasters with relevant skills and tools for managing the University's website.

3.6 ICT Training

3.6.1 Policy Statement

The university shall endeavour to equip staff, students and stakeholders with appropriate ICT knowledge and skills in order to make them effective and efficient in exploiting ICT resources, products and services.

3.6.2 Implementation Strategies

(a) Internal ICT user training targeting the University community shall be scheduled on a continuous basis and be conducted in the teaching centres, campuses and at the computer laboratory;
(b) External ICT training shall be organised by the ICT Unit in response to need as may be assessed from time to time when training is not possible within the University;
(c) The ICT Unit shall jointly with user departments nominate trainees for internal and external ICT training when the need for such training arises;
(d) The ICT Unit in liaison with the user department shall identify the appropriate trainers for the training as demanded by the needs of the scheduled training;
(e) The ICT Unit jointly with the user departments shall provide necessary resources to facilitate the training;
(f) The ICT Unit shall develop curricula for all training including development of source material. To this end, the Unit shall where possible recommend curriculum for all external training and conduct on-line assessment tests and examinations; and
(g) ICT Unit in collaboration with other partners shall initiate and facilitate

ICT training to cooperative movement stakeholders.

3.7 ICT Security and Internet

3.7.1 Policy Statement

University shall endeavour to:

i. protect ICT systems and institutional data
ii. establish data backup and recovery mechanisms
iii. develop proper ICT security procedures and disaster recovery plans
iv. ensure that ICT facilities and services are used by authorized individuals depending on their work and study requirements
v. ensure that ICT facilities and services are used to carry out legitimate activities
vi. improve and manage internet services to meet ever-increasing requirements.

3.7.2 Implementation Strategies

The implementation strategies for ICT and internet security are divided into the following groups:

3.7.2.1 Implementation strategies for confidential and proprietary information

(a) The University data contained in ICT systems shall be classified as either confidential or non-confidential. Examples of confidential information include but are not limited to: payroll data, human resource data, and research data. Employees shall take all necessary steps to prevent unauthorized access to confidential information;

(b) Users shall keep passwords secure and shall not share accounts. Shared accounts are prohibited. Authorized users are responsible for the security of their passwords and accounts. System level passwords shall be changed on six months basis; user level passwords shall be changed at least once in every six (6) months;

(c) All PCs, laptops, and workstations shall be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host is unattended;

(d) Postings by users from the University e-mail address to newsgroups shall contain a disclaimer stating that the opinions expressed are strictly the user's and not necessarily those of the University, unless posting is in the course and within the scope of official duties; and

(e) The user shall exercise caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or trojan horse code.

3.7.2.2. Implementation strategies for unacceptable system and network activities

(a) Violating of the rights of any person or company protected by Tanzania's copyright, trade mark, patent, or other Intellectual Property Rights (IPR) law and the University's Intellectual Property Policy, other relevant policies, or the University's code of conduct;

(b) Introducing of malicious programs into the network or server, for instance viruses, worms, trojan horses or e-mail bombs;

(c) Sharing of the University user accounts and passwords– users shall take full responsibility for any abuse;

(d) Using the University computing resources to actively engage in procuring or transmitting material that could amount to sexual harassment or constitute creation of a hostile work environment;

(e) Making fraudulent offers of products, items, or services originating from any of the University account;

(f) Causing a security breach or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which one is not an intended recipient or logging onto a server that one is not expressly authorized to access, unless this is within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged attacks, packet spoofing, denial of service, and forged routing information for malicious purposes;

(g) Port scanning or security scanning unless prior notification to ICT Unit management is made;

(h) Executing any form of network monitoring which will intercept data not intended for the originator's host computer, unless this activity is a part of an employee's normal job or duty;

(i) Circumventing user authentication or security of any host, network or account;

(j) Interfering with or denying service to other network users, also known as denial of service attack;

(k) Using any program, script, command or sending messages of any kind, with the intent to interfere with, or disable, another user's terminal session, via any means, locally or via the Internet, intranet or extranet; and

(l) Using the University network or infrastructure services, including remote connection facilities, to offer services to others within or outside the University premises on free or commercial terms.

3.7.2.3 Implementation strategies for wireless network users responsibilities

(a) Any person attaching a wireless device to the University network shall be responsible for the security of the computer device and for any

intentional or unintentional activities arising through the network pathway allocated to the device;

(b) The University takes no responsibility for any loss or damage to the user computing device as a result of connection to the wireless network;

(c) Users shall ensure that they run up to date antivirus, host firewall and anti-mal ware software, and that their devices are installed with the latest operating system patches and hot fixes;

(d) Users shall authenticate on the wireless network for every session;

(e) Wireless network users shall ensure that their computer systems are properly configured and operated so that they do not cause inconveniences to the other University network users;

(f) Wireless network is provided to support teaching, research or related academic activities at the University. The use of the University wireless network services for other purposes is prohibited; and

(g) Wireless network users shall get their network addresses automatically; a valid network address shall be granted when connected. Use of other network addresses is prohibited.

3.7.2.4 Implementation strategies for appropriate use of electronic mail

(a) Electronic mail and communications facilities provided by the University are intended for teaching, learning, research, outreach and administrative purposes. Electronic mail may be used for personal communications within appropriate limits.

(b) Users shall explicitly recognize their responsibility for the content, dissemination and management of the messages they send. This responsibility means ensuring messages have the following features:

i) are courteous and polite;
ii) are consistent with the University policies;
iii) protect others' right to privacy and confidentiality;
iv) do not contain obscene, offensive or slanderous material;
v) are not used for purposes that do not conflict with the University's interests;
vi) do not unnecessarily or frivolously overload the email system (e.g. spam and junk mail);
vii) do not carry harmful content, such as viruses; and
viii) are not for commercial purposes.

3.7.2.5 Implementation strategies for confidentiality and security

(a) As the University networks and computers are the property of the University, the University retains the right to allow authorized ICT Unit staffs to monitor and examine the information stored within;

(b) It is recommended that personal confidential material are not stored on or sent through University ICT infrastructure;

(c) Users must ensure integrity of their password and abide by University guidelines on passwords;
(d) Sensitive confidential material shall NOT be sent through electronic mail unless it is encrypted;
(e) Confidential information shall be redirected only where there is a need and with the permission of the originator, where possible;
(f) Users shall be aware that a message is not deleted from the system until all recipients of the message and of any forwarded or attached copies have deleted their copies;
(g) Electronic mail messages can be forged in the same way as faxes and memoranda. If a message is suspect, users shall verify authenticity with the ICT Unit;
(h) Users agree to indemnify the University for any loss or damage arising from use of University's e-mail; and
(i) The University takes no responsibility and provides no warranty against the non-delivery or loss of any files, messages or data nor does it accept any liability for consequential loss in the event of improper use or any other circumstances.

3.7.2.6 Implementation strategy for bring your own device (BYOD)

(a) Employees who prefer to use their personally-owned IT equipment for work purposes must secure corporate data to the same extent as on corporate ICT equipment, and must not introduce unacceptable risks (such as malware) onto the corporate networks by failing to secure their own equipment;
(b) BYOD users must use appropriate forms of user authentication approved by information security, such as user IDs, passwords and authentication devices;
(c) The following classes or types of corporate data are not suitable for BYOD and are not permitted on personal owned devices:
    (i) Anything classified SECRET or CONFIDENTIAL;
    (ii) Other currently unclassified but highly valuable or sensitive corporate information which is likely to be classified as SECRET or above;
    (iii) Large quantities of corporate data (i.e. greater than 1 Gb in aggregate on any one personal owned devices or storage device).
(d) The University has the right to control its information. This includes the right to backup, retrieve, modify, determine access and/or delete corporate data without reference to the owner or user of the device;
(e) The University has the right to seize and forensically examine any device within the University premises believed to contain, or to have contained, corporate data where necessary for investigatory or control purposes;
(f) Suitable antivirus software must be properly installed and running on all

devices;

(g) Device users must ensure that valuable corporate data created or modified on the devices are backed up regularly, preferably by connecting to the corporate network and synchronizing the data between the device and a network drive or on removable media stored securely;

(h) Any device used to access, store or process sensitive information must encrypt data transferred over the network (e.g. using SSL or a VPN);

(i) Since ICT User support does not have the resources or expertise to support all possible devices and software, devices used for BYOD will receive limited support on a 'best endeavours' basis for academic purposes only;

(j) While employees have a reasonable expectation of privacy over their personal information on their own equipment, the University's right to control its data and manage devices may occasionally result in support personnel unintentionally gaining access to their personal information. To reduce the possibility of such disclosure, device users are advised to keep their personal data separate from University data on the device in separate directories, clearly named (e.g. "Private" and "BYOD"); and

(k) Take care not to infringe other people's privacy rights; for example, do not use devices to make audio-visual recordings at work.

3.7.2.7 Implementation strategies for password

(a) All system-level passwords such as root, enable, server operating system, application software, shall be changed at least once every six (6) months;

(b) All user-level passwords such as e-mail, web, and desktop computer shall be changed at least once in every six (6) months;

(c) User accounts that have system-level privileges granted through group memberships or programs such as "sudo" shall have passwords distinct from all other accounts held by such users;

(d) Passwords shall not be inserted into e-mail messages or other forms of electronic communication;

(e) Passwords for the University accounts shall not be used for other non University access such as personal ISP account, Web Mail, and Bank ATM.

(f) All passwords shall be treated as sensitive, confidential University information. Users shall not share the University passwords with anyone, including administrative assistants or secretaries;

(g) Users shall not use the "Remember Password" feature of any browser such as, Internet Explorer, Mozilla Firefox, Opera, Google Chrome;

(h) Users shall not write passwords down and store them anywhere in their offices;

(i) Where an account or password is suspected to be compromised the affected passwords shall be changed immediately. The ICT Unit shall be alerted

immediately to investigate the incident, if it affects the critical University information systems or processes;

(j) As a proactive defence procedure, password cracking or guessing tools may be performed on a periodic or random basis by the relevant staff of the ICT Unit or its delegates. If a password is guessed or cracked during one of these scans, the affected user shall be required to change the password immediately; and

(k) All user-level and system-level passwords shall conform to the guidelines described below.

3.7.3 Strategies for construction of strong passwords

(a) Users are discouraged to use weak passwords which use English, Swahili or other dictionary words such as family names, place names, plate numbers, birth dates and any other easily accessible personal information; and

(b) Users are encouraged to use strong passwords which have the following characteristics:

(i) Contain both upper and lower case characters like a-z, A-Z.

(ii) Have digits and punctuation characters as well as letters such as 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?, or /.

(iii) Are at least eight alphanumeric characters long.

(iv) Are not words in any language, slang, dialect, or jargon, among others.

(v) Are not based on personal information, or names of family, among others.

3.7.2.8 Implementation strategies for server security

(a) Any server deployed on the University ICT network shall have an operational group that shall be responsible for its system administration. Operational groups shall monitor configuration compliance and shall implement an exception policy tailored to their environment. Each operational group shall establish a process for changing the configuration guides; if the server is executing critical University systems this shall involve a final review and approval by the DVC Academic;

(b) All servers shall be registered with the ICT Unit. At a minimum, the following information shall be forwarded:

(i) Contacts of the System administrator

(ii) Physical location of the server

(iii) Hardware and operating system version in use

(iv) Description of functions and applications of the server

(c) Configuration changes for servers shall follow the appropriate change management procedures;

(d) Server Operating Systems shall be configured in line with approved ICT guidelines;

(e) Services and applications that are not used shall be disabled at all times, for instance NFS, Telnet, and FTP;

(f) Access to services shall be logged and protected through access-control methods where possible;

(g) The most recent security patches shall be installed on the systems as soon as practical, the only exception being when immediate application would interfere with business requirements;

(h) Antivirus software shall be installed and configured to update regularly;

(i) User access privileges on a server shall be allocated on "least possible required privilege" terms, just sufficient privilege for one to access or perform the desired function;

(j) Super-user accounts such as "root" shall not be used when a non-privileged account can do;

(k) If a methodology for *secure channel connection* is available, that is technically feasible, privileged access shall be performed over secure channels, for instance, encrypted network connections using SSH or IPSec;

(l) Servers shall be physically located in an access-controlled environment;

(m) It shall be prohibited to operate servers from uncontrolled or easily accessible areas;

(n) All security-related events on critical or sensitive systems shall be logged and audit trails backed-up in all scheduled system backups; and

(o) Security-related events shall be reported to the ICT Information Security Officer/System Administrator, who shall review logs and report incidents to Head ICT. Corrective measures shall be prescribed as needed. Security-related events include, but are not limited to:

(i) port-scan attacks

(ii) evidence of unauthorized access to privileged accounts

(iii) anomalous occurrences that are not related to specific applications on the host.

3.7.2.9 Implementation strategies for audit

For the purpose of performing an audit, any access needed shall be provided to members of the University ICT audit team when requested. This access shall include:

(i) User level and/or system level access to any computing or communications device.

(ii) Access to information (such as electronic or hardcopy) that may be produced, transmitted or stored on the University ICT infrastructure.
(iii) Access to work areas such as computer laboratories, offices, cubicles, or storage areas.
(iv) Admission to interactively monitor and log traffic on the University ICT networks.

3.7.2.10 Implementation strategies for computer laboratory security

(a) All University computer laboratories shall be monitored by Computer laboratory administrators, who shall take charge of computer laboratories. A computer laboratory administrator shall be responsible for the day to day running of a computer laboratory, and shall be the Point of Contact (PoC) for the ICT Unit on all operational issues regarding the laboratory;
(b) Computer laboratory administrators shall be responsible for the security of their laboratories and their impact on the University network, or any other network. They shall be responsible for overseeing adherence to this policy and associated processes;
(c) Computer laboratory administrators shall be responsible for the laboratory's compliance with all the University ICT policies;
(d) Computer laboratory administrators shall be responsible for controlling access to their computer laboratories; they shall ensure that only legitimate users can gain access to laboratory resources; and
(e) The ICT Unit reserves the right to interrupt laboratory connections if such connections are viewed to impact negatively on the ICT infrastructure, or pose a security risk. For this purpose, computer laboratory administrators shall be available round-the-clock for emergencies, otherwise actions shall be taken without their involvement.

3.7.2.11 Implementation strategies for anti-virus

(a) All computers connected to the University ICT network shall run the standard supported anti-virus software, and be configured to perform full-system and on-access scans;
(b) Anti-virus software and the virus update files shall be kept up-to-date always through scheduled daily automatic updates;
(c) Computer laboratory administrators and owners of computers, in consultation with the relevant ICT Unit personnel, shall be responsible for executing required procedures that ensure virus protection on their computers. They shall ensure that their computers are virus-free before being allowed to connect to the University network;
(d) Once discovered, any virus-infected computer shall be removed from the University network until it is verified as virus-free; and

(e) The following precautions shall be observed by all users to reduce virus problems. Users shall:
    (i) never open any files or macros attached to e-mails from an unknown, suspicious or untrustworthy source. Such emails shall be deleted immediately and emptied from trash folders;
    (ii) delete spam, chain letter, and other junk e-mail without forwarding;
    (iii) never download files from unknown or suspicious sources;
    (iv) avoid direct disk sharing with read/write access unless this is absolutely necessary.
    (v) always scan removable media, including diskettes and memory sticks, from unknown sources for viruses before using.
    (vi) back-up critical data and system configurations on a regular basis and store the data in a safe place.
    (vii) not run any applications that could transfer a virus such as e-mail or file sharing in a computer where the anti-virus software is disabled. Such a computer shall be disconnected from the network.
    (viii) periodically check for anti-virus updates and virus alerts because new viruses are discovered almost every day.

3.7.2.12 Implementation strategies for computer server room(s)

(a) Computer servers shall be housed in a room built and secured for the purpose;
(b) The computer server rooms shall contain an adequate air conditioning system in order to provide a stable operating environment and to reduce the risk of system crashes due to component failure;
(c) No water, rainwater or drainage pipes shall run within or above computer server rooms to reduce the risk of flooding;
(d) Where possible the floor within the computer suite shall be a raised false floor to allow computer cables to run beneath the floor and reduce the risk of damage to computer equipment in the case of flooding;
(e) Power feeds to the servers shall be connected through Uninterrupted Power Supply (UPS) and surge protector equipment to allow the smooth shutdown and protection of computer systems in case of power failure;
(f) Where possible generator power shall be provided to the computer site to help protect the computer systems in the case of a main power failure;
(g) Access to the computer server rooms shall be restricted the authorized University staff only;
(h) The system administrator shall be responsible for maintaining the integrity of the system and data, and for determining end-user access rights;
(i) All supervisor passwords of vital network equipment and of those critical ICT Unit servers shall be recorded in confidence with the Head, ICT Unit

and the record safely stored under lock and key for emergencies; and

(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.

3.7.2.13 Implementation strategies for physical LAN/WAN security

(a) LAN and WAN equipment such as switches, hubs, routers, and firewall shall be kept in secured rooms. In addition, the equipment shall be stored in lockable communication cabinets;

(b) Whenever legitimate access to communication cabinets is necessary, it shall be done with physical supervision of the responsible ICT personnel;

(c) Users shall log out of their workstations when they leave their workstation;

(d) All unused workstations shall be switched off outside working hours;

(e) All internal or external network wiring shall be fully documented;

(f) All unused network points shall be de-activated when not in use;

(g) Users shall not place or store any item on top of network cabling;

(h) Where ducting is involved, inspection shall be carried out regularly to curb damage to the cables;

(i) Redundant cabling schemes shall be used where possible;

(j) All servers and work stations shall be fitted with UPS to condition power supply;

(k) All switches, routers, firewalls, and critical network equipment shall be fitted with UPS;

(l) Critical servers shall be configured to implement orderly shutdown in the event of a total power failure depending on the operating system used; and

(m) All UPS equipment shall be tested periodically.

(n) ICT Unit shall keep a full inventory of all computer equipment and software in use throughout the University.

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

3.7.2.14 Implementation strategies for systems backup and restoration

(a) The University ICT Unit is responsible to back-up the entire critical corporate database for the entire University which is located at the servers. Individual users and staff will be responsible to back-up their own data which is on their own desktop and notebook computers. The University will provide the necessary storage and back-up media to staff who request for it in order for them to perform the back-up process. All the backup disks will be kept in an offsite locked place;

(b) Step-by-step procedures are needed in order to achieve complete data

reconstruction and resumption of system operations from back-ups the. A hard copy of this document shall be filed in the back-up inventory file; and

(c) The retention period for back-up media shall be set in such a manner as to minimize the risk of catastrophic loss of data at reasonable media cost. The following guide, commonly known as the Grandfather-Father-Son (GFS) method, shall be adopted:
    (i) Daily back-ups, known as the Son, shall be carried out on all, or selected days of the week;
    (ii) The last full daily back-ups in a week, known as the Father, shall be the weekly back-up;
    (iii) Daily back-ups age only for the length of the week, hence the media shall be reused in the coming week;
    (iv) The weekly back-ups shall be retained for a month and shall be reused during the next month;
    (v) The last full back-up of the month is known as the monthly backup, or the Grandfather;
    (vi) The Grandfather back-ups become the oldest, and shall be retained for a year before the media can be reused.

(d) Back-up media must first be tested to guarantee their integrity before re-use. Media re-use must always begin with the oldest set.

(e) Back-up plans, with the schedule of the general regular back-up pattern for the key University systems, shall be documented. The ICT security officer/system administrator shall prepare this plan in conjunction with the persons responsible for back-ups. The ratified plan shall be authorized by the Head, ICT Unit and filed in the *back-up inventory file*. Persons responsible for back-ups shall carryout all back-ups as scheduled on the back-up plan, but may also stipulate additional event-dependent intervals where necessary.

3.7.2.15 Implementation strategies for internet usage

(a) All software used to access the Internet shall be part of the standard software suite or approved under the ISO standard;

(b) All users shall ensure that Internet access software shall incorporate the latest security updates provided by the vendors;

(c) All Internet access software shall be configured to use stipulated gateways, firewalls, or proxy servers. Bypassing any of these servers shall be strictly prohibited;

(d) Internet access traffic through the University ICT infrastructure shall be subject to logging and review;

(e) The University Internet access infrastructure shall not be used for personal solicitations, or personal commercial ventures; and

(f) Official electronic files shall be subject to the same rules regarding the

retention of records that apply to other documents and information or records shall be retained in accordance with the University records retention schedules.

3.7.2.16 Implementation strategies for business continuity management

(a) All critical information systems should have a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) to ensure the ability to recovery from failure or unexpected interruption; and

(b) The information owner is responsible for the implementation of a routine of risk assessment in order to refine the recovery requirements. The Business Continuity and Disaster Recovery Plans must be updated to reflect these refinements.

4.0 POLICY ENFORCEMENT

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

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

(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 Unit shall be responsible for coordinating and implementing this ICT policy and procedures. The ICT unit will also advice and assist all units/department/faculty/directorate /bureau and other stakeholders across the University on ICT matters.

The ICT Unit 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.

An overall policy review will be undertaken after every five years or earlier, as need arises.

6.0 COMMENCEMENT DATE

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

7.0 AUTHENTIFICATION