MBEYA UNIVERSITY OF SCIENCE AND TECHNOLOGY

Information and Communication Technology Policy

NOVEMBER, 2019

Table of Contents

PART I

1. PRELIMINARIES

1.1. List of Acronyms

AFRINIC	-	African Network Information Centre
CD-ROM	-	Compact Disk Read Only Memory
CoICT	-	College of Information and Communication Technology
DICTSS	-	Directorate of Information and Communication Technology Services and Statistics
DNS	-	Domain Name Services
DVC-PFA	-	Deputy Vice Chancellor Planning, Finance and Administration
DVC-ARC	-	Deputy Vice Chancellor Academic, Research and Consultancy
ETSC	-	Estates and Technical Services Committee
ICANN	-	Internet Corporation of Assigned Names and Numbers
ICT	-	Information and Communication Technology
ICTSS		Information and Communication Technology Services and Statistics
IITT	-	Institute of Innovation and Technology Transfer
IP	-	Internet Protocol
LAN	-	Local Area Network
MUST	-	Mbeya University of Science and Technology
OPAC	-	Online Public Access Catalogue
WAN	-	Wide Area Network

1.2. Definitions of Key Terms

Capacity Building (**Capacity Development**) is the process by which individuals and organizations obtain, improve, and retain the skills and knowledge needed to do their jobs competently. Capacity building and capacity development are often used interchangeably. However, some people interpret capacity building as not recognizing people's existing capacity whereas capacity development recognizes existing capacities, which require improvement.

Community is a structural mechanism whereby content sharing similar characteristics are organized.

Copyright is a set of exclusive rights granted to the author or creator of an original work, including the right to copy, distribute and adapt the work. Copyright owners have the exclusive statutory rights to exercise control over copying and other exploitation of the works for specific period, after which the work is said to enter the public domain.

Cyber Security is defined as the protection of the university digital infrastructure and information assets against any compromise or attack that may affect its confidentiality, integrity and/ or availability.

Digital Networks are all equipment involved in the transmission and routing of all digital communications within the University at all campuses.

ICT Capacity Building refers to the process whereby individuals and organizations obtain, improve, and retain the ICT skills and knowledge needed to do their jobs competently.

Intellectual Property refers to creations of the mind: inventions, literary and artistic works, symbols, names, images and design used in commerce. Intellectual Property

has two categories: Industrial Property which includes inventions (patents), trademarks, industrial designs and geographic indication of source; and Copyright, which includes literary and artistic works such as novels, poems, plays, films, and musical works. Artistic works includes drawings, paintings, photographs, sculptures and architectural designs.

Social Media is any electronic platform and software that provides electronic social interaction amongst its subscribers and communities.

Software refers to all computer programs used to support university functions. This encompasses systems software such as operating systems, systems utilities such as anti-viruses and application. Such software shall be either developed internally (in house or outsourced) or off the shelf software.

University Wide Area Networks refers to all of the aggregated inter-connected campuses on the virtual one-network University domain.

1.3. Policy Objective

The main objective of this policy is to provide key ICT issues and the framework for governance of all ICT related matters that will support effective and efficient implementation of the University goals and objectives in teaching, research and administrative functions.

1.4. Policy Vision

Mbeya University of Science and Technology ICT vision is to become a centre of excellence in the application of ICT in teaching, learning, research and consultancy.

1.5. Policy Mission

To innovatively use ICT to enhance teaching, consultancy and research at the Mbeya University of Science and Technology as well as provide modern ICT tools to increase efficiency and effectiveness of the University operations.

1.6. Policy Scope

This policy applies to all MUST community and other stakeholders that deal with the University on matters pertaining to ICT.

1.7. Policy Review Process

The Mbeya University of Science of Technology ICT Policy review process began at the ICT Sub-Committee. The Director of Information and Communication Technology Services and Statistics (DICTSS) appointed members to prepare the first review draft of the Policy which was submitted to various stakeholders within the University including Colleges, and Workers associations. It was then presented to the ICT Sub-Committee before its presentation to the Estates and Technical Services Committee (ETSC).

PART II

2. SITUATIONAL ANALYSIS

2.1. Introduction

The Mbeya University of Science and Technology has continued to grow in myriad ways since its establishment in the 2012 by the President of United Republic of Tanzania signing the Mbeya University of Science and Technology Charter. The growth trend is particularly noticeable in the number of enrolled students which is currently more than 4,500; 545 staff, and 26 programmes offered, ranging from ordinary diploma, bachelor, master to PhD level. Critical to this spectacular growth witnessed over the years, and future of the University in fulfilling its core vision is provision of ICT for adequate support of teaching, research, consultancy and administrative functions.

The National Development Vision 2025 recognizes and promotes ICT as central to increase competence and competitiveness, noting that "*these technologies are a major driving force for the realization of the [National Development] Vision*". In the same vein, the University has set its objective in its Five-Year Strategic Plan as "*ICT infrastructures and e-learning enhanced*"; thus making emphasis in leveraging ICT for efficient and effective training, research and public service. Hence, the University has clearly shown its emphasis in using ICT as a key infrastructure for teaching and learning.

Following the crucial role of ICT in any higher learning institution in achieving its goals, the University formulated its first ICT policy in 2014. The document formed the basis for governing key aspects of ICT and was the basis for creating the Centre for Networking and Computing which was later changed to Directorate of Information and Communication Technology Services and Statistics (ICTSS) to oversee issues pertaining to implementation and management of ICT matters at the University. The current policy has been in operation for five years, calling for

reviewing to reflect the current needs, taking into consideration alignment with other existing MUST policies as well as national laws, policies and regulations relevant to ICT.

2.2 Rationale

The review of the ICT Policy has been necessitated by the changing environment in key areas which were either not covered in the first policy or because configuration of such issues has changed. For example, while the increasing use of ICT for teaching, research and operations improve convenience and efficiency in the University functioning, such dependency has come with possible threats particularly cybercrimes, but also there is a need to consider people with disability to ensure such developments do not leave them unattended. The review of the ICT Policy has enabled the University to fine-tune its priorities based on these new realities for safe and effective use of ICT at the University.

Also, as stated above, the University is growing in a number of aspects, and the use of ICT has been intensified over time. Such changes call for alignment of governance of ICT at the University, particularly proper management structure for ICT which matches its expanding role at the University. Thus, the review of this policy has considered improvement of the governance structure responsible for planning, development and management of University ICT infrastructure and services.

PART III

3. POLICY STATEMENTS

3.1. Policy Issue: University Data Communications Network and Services

In MUST, the teaching, learning and research, as well as consultancies and administrative functions are already in electronic formats and platforms to varied levels and degrees. The fast rate of innovation has led to newer and more effective technological developments that have greater value. The core of this infrastructure is the Data Communications Network and Services that has evolved into the backbone for the provision and usage of daily ICT services.

3.1.1 Policy statement

The University commits itself to provide a resilient, secured and stable fast data communications network and services as an enabler to the processing, storage, dissemination and accessing of information or ICT enabled services as relates to the various needs of the teaching, learning, administration, research and consultancy domains.

Strategies

a) The University shall prepare a five (5) year ICT infrastructure rollout plan aligned with the University Strategic Plan. The plan will take into consideration the ever changing University computing needs, growth in usage demand of the backbone as well as technological advances that introduce smarter and innovative practices. The core of this plan is the alignment to the existing resource provision to ensure value for money as well as achieve sustainability;

b) The University shall establish and maintain a Data Center to act as the only central repository for all university databases and web hosting;

c) The University shall develop and maintain updated structured cabling standards to ensure a uniform level of acceptable design across all units;

d) The University shall develop and maintain an updated University wide Enterprise Architecture as the blueprint for alignment of business requirements and ICT investments;

e) The University shall provide connectivity to the internet using wireless technology through authorized Access Points to prioritized areas;

f) The University shall provide connectivity to all buildings at the University using fiber or similar technology, and connect all Colleges with wireless connection as a redundant link;

g) The University shall support the provision of remote access for approved University resources. This supports access provision of network resources to authorized users across public internet infrastructure with consideration for information security;

h) The University shall strive to make sure that internet bandwidth and related resources are well managed;

i) The University shall ensure that internet bandwidth is properly managed using equipments and software for bandwidth management;

j) The University shall ensure all access obligations including payment of fees are effected on time to avoid inconveniences;

k) The University shall collaborate with government and private institutions to set-up and effectively utilize national Internet Exchange Points (IXPs).

3.1.2 Policy Statement: The University shall strive to ensure digitization of operational functions to reduce paper usage.

Strategies

a) The provision of secured University E-mail services and related storage quotas will be centrally defined, managed and periodically reviewed by MUST ICTS;

b) All MUST websites and portals will be centrally hosted;

c) Establish and maintain an effective dedicated web cache management service to optimize bandwidth provision;

d) The University shall manage the provision of computing resources to all user groups within the research, consultancy, teaching, learning and administration units of the University;

e) The University shall ensure the provision of a secure and efficient university intranet and web portal and its universal access;

f) Provision of ICT services will take into consideration the needs of:

    a. Special user groups ;

    b. Guest access;

g) The University shall strive to remove paper work and replace with digitization (paperless);

h) The University shall reserve the right to audit, without prior notice, any ICT equipment connected to its networks for the purposes of protection against exploitable security vulnerabilities.

3.2. Policy Issue: Cyber Security

The University acknowledges the transition towards a digital organization is not without risks, in particular cyber crimes. The University therefore envisages having secure information infrastructure for well functioning of the organization, which includes the use of best practices, standards, competent human resource and security technology.

3.2.1 Policy statement: The University strives to ensure the protection, resiliency and stability of all University ICT infrastructures, the information held there within and services against any cyber threats.

Strategies

a) The University through the DICTSS shall:

i. Undertake ownership of all cyber security and cyber risks;

ii. Provide leadership for the Governance of Cyber Security within the University;

iii. Articulate the University's information risk appetite.

b) The Directorate of ICTSS shall:

i. Ensure that the appropriate security controls and mechanisms have been put in place based on a formal periodic risk assessment;

ii. Maintain an updated ICT risk register in line the National Information Security Framework;

iii. Maintain an updated and tested Business Continuity and Disaster Recovery Plan for all critical University digital infrastructure and information assets;

iv. Implement periodic systems and infrastructure audit;

v. Maintain updated and documented secure configurations baselines for all hardware and software;

vi. Develop and implement a patch management plan;

vii. Implement network filtering to protect the network against malware related threats;

viii. Ensure the controlled and audited usage of ICT administrative privileges;

ix. Implement monitoring and real time analysis of all ICT network device event security logs with a centralized mechanism;

x. Ensure the limited and controlled use of network ports and controls;

xi. Ensure the implementation of appropriate Wireless Access Provision protection mechanisms;

xii. Coordinate and lead the rollout of periodic cross-cutting security awareness and training;

xiii. Ensure all ICT equipment is installed with the appropriate active malware protection that is continuously updated;

xiv. Develop and maintain a handover mechanism for ICT equipment and information during end of staff employment contracts aligned to the University Human Resource Policy;

xv. Secure access to all the university ICT resources and enforce acceptable usage of the same by the deployment of security standards, technologies and best practices;

xvi. Implement and maintain centralized authentication, authorization, and accounting service mechanism for all network core equipment to all ICT resources;

xvii. From time to time, define the password strength and lifecycle specification for all user categories;

xviii. Change all default system or hardware passwords;

xix. Ensure access termination to University ICT resources due to:

1. End of studentship or staff employment tenure.
2. Request from University Council, University Management, College management, Heads of Department.
3. Occurrence of any of the unacceptable usage restrictions.

c) Users shall:

i. Ensure compliance to the Cyber Security procedures as stipulated in the ICT Policy;

ii. Report any cyber security incident to Directorate of ICTSS;

iii. Ensure the privacy of their passwords;

iv. Agree to the terms of usage which strictly prohibited the following activities, with no exceptions:

1. Sharing of individual access passphrases;
2. Usage of any pirated software on University computing devices;
3. Usage of any unauthorized peer to peer software;
4. Any user action that contravenes the Cybercrime Act, 2015;

5. Any user action that violates the rights of any person or entity's legally registered copyright and/ or Intellectual Property;
6. Introduction of any malicious software onto any University computing device or network;
7. Any user action that disrupts the normal functioning of any university computing device or network;
8. Violations of the rights of any person or company protected by Tanzania's copyright, trade mark, patent, or other intellectual property (IP) law and the University's Intellectual Property Policy, other relevant policies, or the University's code of conduct;
9. Any password cracking, software spying, privilege escalation, unauthorized network port scanning and network reconnaissance, network and/or software penetration;
10. Usage of university ICT devices and/ or network to disrupt an external system or network;
11. Usage of university ICT devices and/ or network to send out any spam;
12. Usage of university ICT devices and/ or network for any gambling activity;
13. Usage of university ICT devices and/ or network for any personal commercial purposes.

3.2.2 Policy Statement: The University promotes the use of personal devices on the university network as long as such devices comply with the University policies and offer a similar level of protection as specified by the Directorate of ICTSS.

Strategies

Users of devices shall be subject to the following:

a) No sensitive or confidential University information shall be stored on such devices;

b) The University will provide an acceptable level of protection for such personal devices as defined by the Directorate responsible for ICT from time to time;
c) The University shall have the right to investigate/ audit such devices in case of any malicious activity, cybercrime or fraud that affects the University;
d) Registered with Directorate responsible for ICT.

3.2.3 Policy Statement: The University shall maintain appropriate and secure use of computer labs.

Strategies

College Principals, and Directors of Centers, or Directorates shall ensure the ICT infrastructure

a) Compliant to ICT approved baseline setup and configurations;
b) Routinely checked for unauthorized connections;
c) Accessed only by authorized students and/ or researchers;
d) Locked down to prevent physical theft of any component;
e) Protected against exposure to water leakages, fire and or dust;
f) Located in strongly burglar proofed rooms;
g) Labelled according to approved ICT nomenclature;
h) Professionally serviced and maintained.

3.2.4 Policy Statement: The University strives to maintain its Data Centers and Server Rooms as the primary storage of the University data in order to maintain maximum security at all times, minimizing the possibility of digital and physical vandalism.

Strategies

Data Centres and Server rooms shall be:

(a) Located in secure strong locations away from human or vehicle traffic;
(b) Fitted with both manual and electronic access control with CCTV monitoring;

(c) Protected against physical intrusion and exposure to water, dust and fire;

(d) Protected against power fluctuations;

(e) Supported by alternative power supply;

(f) Backups be located to the campus and remote sites.

3.2.5 Policy Statement: The University shall ensure access control to identified areas with sensitive ICT equipment as well as other assets of the University. The control shall include the use of digital technology to monitor and restrict access to those areas.

Strategies

The University through the ICT Technical Committee shall:

(a) Define and periodically review the technology for SMART Access control for different categories to take advantage of new ICT innovations;

(b) Maintain a smart access control to govern access to all University buildings by staff, students, visitors and contractors;

(c) Implement CCTV for access monitoring of all University buildings and entry points.

3.3. Policy Issue: Software Development and Acquisition

The University recognizes the need to achieve a defined common methodology for both development and off-the-shelf software acquisition for optimizing University resources.

3.3.1 Policy statement

This policy will strive to set direction for standardizing software development, resulting in better resource utilization and higher-quality software products delivered to end users.

Strategies

The University shall:

a) Ensure all software undergo testing and quality assurance before installation in any production environment within the University and ensure provision for:
    i. Information classification.
    ii. Usage of the least privilege principle.
    iii. Segregation of roles.
    iv. Audit trails.
b) Enforce all software used for the University to comply to Cyber Security guidelines
c) Ensure all acquired software shall, where necessary, contain provision for technical support and upgrades.
d) Ensure the University, Colleges, Departments, units and Centers shall, where necessary, make use of open source software based on a risk based assessment as contained in the cyber security guidelines.
e) Ensure development of application software to be used for the purpose of managing the University information resources by Colleges and Institutes or Centers, is done in collaboration with the Directorate of ICT.
f) Ensure that all software applications developed in-house undergo an overhaul redesign every three years unless otherwise decided.
g) Ensure all locally development applications shall support password encryption and user role segregation.

This policy does not apply to software development within Colleges for academic or educational purposes.

3.4. Policy Issue: ICT Services Management

The University commits itself to ensure the provision of the ICT Service within the University by defining and empowering governing bodies, along with the

Directorate of ICTSS as the central coordination point of contact for all ICT support. The ICT support shall cater for all areas under the University network, computing devices, hardware, software and implementation of ICT initiatives, projects and programs in all colleges, as well as schools and departments.

3.4.1 Policy Statement

The University shall provide for the centralized management, and be responsible for the support of all ICT related matters within University, aligned with MUST Strategic Plan where ICT is identified amongst the key components in the support of the MUST's mission and vision.

Strategies

The University shall:

a) Define and implement an appropriate ICT Service Management process and procedure aligned with the goals and objectives of the University

b) Define and implement a Business Model for the provision of ICT services to external clientele.

c) Define how service support operations are to be carried out by authorized personnel to ensure efficiency, stability and continuity of any ICT service or equipment to ensure it meets its intended user requirements. This will apply to all University owned ICT applications and devices.

d) Employ the ICT Services Personnel (system administrators/ICT Officers, ICT Lab attendants, ICT technicians, Software Developers/ICT Officer, Security Experts/ICT Officers and Web administrators/ICT Officer) to ensure smooth functioning services. Their functions shall include:

   i. Ensure protection mechanisms exist against ICT devices tampering, alteration or theft;

   ii. Ensure ICT protection controls exist to safeguard security of systems and information;

   iii. Provide assistance and guidance towards compliance of ICT policies;

iv. Provide technical support in line with approved ICT procedures for any system, service, device downtime or breach;

v. Ensure installation and configuration of all hardware and software is aligned to approved ICT standards;

vi. Ensure safe custody and authorized usage of all University software licenses, copyright and usage keys.

3.5. Policy Issue: ICT Skills Capacity Building

The University recognizes that the adoption of Information and Communications Technology (ICT) products and tools will require the attendant training to enable effective usage. This requires a dedicated approach within the University to be able to plan for such gaps and develop as well as implement the training as per and when the need arises. This will target all users within the University amongst the staff and student community to support the various functions of the University.

3.5.1 Policy statement

The University shall plan and implement capacity building for ICT skills to achieve coherency and efficient utilization of its resources, and technical capacities of its staff as need arises.

Strategies

The University shall be responsible for:

a) Coordinating the periodic assessment of existing ICT skills capacity amongst all user groups;

b) Undertaking a periodic capacity skills assessment to identify knowledge gaps within its technical staff to be able to seek appropriate capacity building programs;

c) Developing capacity building modules and courseware for identified ICT skills gaps and implement capacity building with either internal resource personnel or with subject matter experts according to the nature of the required ICT topic;
d) Coordinating the identification of any external expertise for specialized training needs;
e) Ensuring the presence of well-equipped ICT training computer laboratories.

3.6. Policy Issue: Telecommunications and Unified Communications

The University envisions the use of Unified Communications service alongside the traditional telephony services towards implementation of an ICT enabled communications service to support the University objectives. Telecommunications and Unified Communications Services will be provided to support the communication needs required for the smooth operations of the University amongst all Departments and Colleges.

3.6.1 Policy statement

The University shall implement digital communications, first on its digital network, to provide safe, convenient and highly available communication to all its Colleges and Departments.

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 University wide unified communications service to support new communications channels integrated with e-mail, online meetings, video conferencing, workplace collaboration and seamless file sharing;
c) Ensure proper license usage for all unified communications components;

d) Ensure management and take up responsibility for all infrastructure required to provide a smooth user experience as related to communications services;
e) Provide the required timely technical support through the IT services help desk for all communications related downtime;
f) Approve and provide technical assistance for any expansion of the communications services within the University;
g) Set and periodically review communications services technical specifications (hardware, consumable, software) as well as configuration and installation guidelines to ensure uniformity for the service provision and compatibility with existing infrastructure;
h) Undertake routine maintenance, upgrade and daily monitoring of the communications service usage;
i) Manage and maintain service level agreements with all suppliers of the required communications service, equipment and software;
j) Provide technical guidance and authorization in the design and provision of any radio communications service within the University.

3.7. Policy Issue: ICT Procurement

The University commits itself to ensure that procurement of all ICT equipment and services shall be in conformity with the overall University procurement of goods and services standard as aligned to the Public Procurement Act (2017) and the MUST ICT Devices Standards Guideline.

3.7.1 Policy Statement

The University shall guide the procurement of all University ICT equipment and services towards ensuring standardization of all ICT related assets, transparency, timely delivery, quality assurance, value for money as well as compatibility with existing infrastructure and services.

Strategies

The University Procurement Management Unit shall manage all procurement or disposal activities within the Universities in line with the Public Procurement Act (2017).User Departments shall;

a) Ensure conformity with the University Procurement Policy as implemented by the Procurement Unit;
b) Ensure conformity with approved technical guidelines and standards by ICTS in the procurement of any ICT equipment, software or service;
c) Initiate the process of ICT devices disposal for retired ICT equipment held in each User Department according to the University Disposal Policy.
d) The ICTS shall provide technical support to all user departments as itemized hereunder:
    i. Technical assistance in the development of specifications for any ICT equipment, software or service;
    ii. Technical assistance in the identification of user department ICT needs;
    iii. Ensure and verify that supplied ICT equipment, software or services comply with the approved ICT specifications, standards and guidelines;
    iv. Ensure that installation and configuration of any procured ICT equipment, software or service complies with the approved ICT specifications, standards and guidelines;
    v. Maintain an updated inventory of all ICT hardware and software indicating the life cycle;
    vi. Encourage acquisition of Open Source Software (OSS) related products and services to avoid incurring high costs on purchasing and maintaining licensed software;
    vii. Encourage and promote outsourcing of ICT services where necessary as a way of ensuring quality, cost effectiveness and sustainability of the services at the University;

viii. Provide support for bulk procurement of commonly used ICT equipment and Software as per business need;

ix. Define the life cycle for each category of procured ICT equipment to determine the replacement cycle and disposal in accordance with the University Disposal Policy or guideline;

x. Initiate the process of ICT devices disposal for retired ICT equipment held centrally.

3.8. Policy Issue: Social Media

The University envisages using Social Media as a platform for communicating and showcasing to the world its activities, particularly those which relates to academic output such as research findings; and public services such as outreaches.

3.8.1 Policy Statement

The University shall strives to safeguard privacy and personal liberties while at the same time upholding professional and institutional reputations of the University and its community through the use of selected social media in accordance to the Government policies, laws, regulations, guidelines and circulars.

Strategies

(a) Content, roles and responsibility of communication in Social Media shall be as stated in the University Communications Guideline;

(b) The Directorate of ICT shall be responsible for technical support in set up and design of the University Social Media pages. Such activities will be achieved through collaboration with the entity managing the page;

(c) The Directorate of ICT shall provide technical assistance to ensure design based content such as posters or video are professionally prepared to uphold the reputation of the University;

3.9. Policy Issue: Software Licensing and Ownership

All software used for teaching, learning, research and administration in all units of the University; and its related licenses, copyright, intellectual property or source code used by the University shall be owned as assets of the University.

3.9.1 Policy Statement

The University shall ensure that all software in use throughout the University are correctly licensed and/or owned by the University. The University reserves the right to audit, without prior notice, any ICT equipment connected to its networks for the purposes of software license validation.

Strategies

The University shall ensure:

a) An inventory of all software is maintained;
b) All software packages are licensed to the responsible University unit as aligned to purchase agreements;
c) All software in usage are properly managed, administered and maintained;
d) All software in usage are approved and aligned to the University information security policies;
e) Any computing equipment that is written off, sold or given to a third party shall have all non-transferable licensed software permanently removed;
f) Staff and students shall not be given the ability to download and install software on University equipment;
g) Software shall only be used in accordance with its license and duration;
h) Software shall only be distributed in accordance with its license agreement;
i) Software licensed for official purposes must not be used on personal computing devices;
j) All software source code developed with either internal or external resources for University purposes shall be owned by the University and shall

be handed over to the Directorate of ICT for good custody, backup and patenting;

k) All University units outsourcing software development that has source code restrictions shall ensure usage of appropriate third party source code escrow agents to ensure continuity.

3.10. Policy Issue: Information Systems and Data Warehousing

Data Warehousing in MUST and interoperable information systems is envisioned to support the harmonization of resources, increase ICT investment value, allow for accurate reporting and enable information/data consistency. Similarly, it is expected to promote the use of central data repository and interoperability between MUST information systems.

3.10.1 Policy Statement

The University shall strive to achieve centralized management of information systems within a central data repository and interoperability between MUST information systems.

Strategies

a) The University shall define the appropriate data warehousing framework aligned to the Cyber Security framework, data management standards and interoperability framework for the secure and reliable communication between all MUST Information Systems;

b) All MUST Colleges, Departments and Units undertaking the development of any information system shall ensure compliance to this policy;

c) MUST shall ensure the provision of the appropriate ICT infrastructure.

3.11. Policy Issue: Special Needs ICT Usage

The provision of ICT services should take into consideration the needs of special user groups to enhance teaching and learning. This takes into consideration the visually, motor, auditory impaired user groups and others. Globally, the development in ICT supports the extension of equitable access and quality services to all users.

3.11.1 Policy Statement

The University shall define and implement provisions for ICT usage for special user groups within the teaching, learning and research units of the University towards enabling equal access to information and knowledge.

Strategies

The Directorate of ICT shall:

a) Define the appropriate technology aligned to users with Special Needs;

b) Provide the provision of staff & end user training;

c) Ensure the provision of the appropriate access for special user groups for all University web based systems;

d) Ensure the provision of appropriate digital mechanisms within the Library for special user groups;

e) Ensure that all University Colleges, Departments, Units and Centres comply to this policy;

f) Ensure that the University provides the appropriate access for special user groups for all University web based systems.

3.12. Policy Issue: ICT Infrastructure and Services Maintenance

The usage of ICT devices within the University will require a well-planned maintenance plan so as to ensure its safe and proper usage. This relies on the cooperation of all units to ensure proper asset and inventory management on which such maintenance can be achieved through a central coordination role.

3.12.1 Policy Statement

The University shall ensure that, all ICT equipment is regularly maintained to ensure all systems run smoothly with less downtime. This policy applies to all ICT equipments owned by the University within the various units and colleges.

Strategies

a) The Directorate of ICTSS through ETSC shall:

   i. From time to time define and disseminate updated ICT equipment maintenance guidelines to all units and colleges;

   ii. Act as the central point of contact for all University ICT equipment maintenance;

   iii. Provide technical support in the development and implementation of service and maintenance schedules for all University ICT equipment;

   iv. Undertake periodic assessment in all Units and Colleges to ensure compliance with the set of maintenance guidelines.

b) All MUST Units, Departments, Centres, Directorates and Colleges shall:

   i. Maintain records of all ICT equipment they acquire including records of manufacturer equipment warranty;

   ii. Liaise with the unit responsible for ICT in developing service and maintenance schedules on an annual basis for all ICT equipment;

   iii. Maintain good documentation describing the service and maintenance history for all ICT equipment;

   iv. Ensure all ICT equipment is placed within adequate operating environment;

   v. Ensure all replacements or upgrades of any ICT equipment is undertaken with clearance from the unit responsible for ICT.

PART IV

4. IMPLEMENTATION PROCEDURES/GUIDELINES

4.1. Administrative Structure

The ownership of this policy will be under the University Council. The Directorate ICT Services and Statistics shall be responsible for its implementation, management and monitoring. This Policy will therefore assist in provision of the centralized effective governance of all ICT related matters within the University in a rationalized and harmonized manner.

Effective ICT governance provides a conducive environment for the alignment of all ICT investments in a rationalized manner that is geared towards enabling an organization to meet its goals and objectives. This will also contribute to the attainment of value for money, management of risks and effective ICT utilization.

ICT services and management at MUST shall be given a central support at the highest level of the University management. The policy provides guidance in ICT management and sustainability, itemizing the roles of various governing and functional directorates, colleges, centres, departments and units at MUST. For this purpose, issues related to provision of ICT services shall be under the oversight of the Council, and those related to infrastructure investment shall be under the oversight of the ETSC. This arrangement is aimed at providing effective and efficient oversight of the ICT infrastructure and services, given the cross-cutting nature of ICT.

4.1.2 The Estates and Technical Services Committee

There shall be the Estate and Technical Services Committee to oversee and advise the Council on ICT strategy and tactics developments and its use in the University. The Estate and Technical Services Committee will, inter alia, assist in the definition of University-wide ICT policies and all ICT matters pertaining to the ICT infrastructure, services and development. In executing its function ETSC shall do so in collaboration with the Directorate of ICT Services and Statistics, College of ICT, Centre for Innovation and Technology Transfer, University Library, and the ICT Sub-Committee. This in turn will advise the Chief Information Officer (DVC-PFA) on such matters.

4.1.3 The ICT Sub Committee

There shall be the ICT Sub Committee which shall oversee all activities under the Directorate of Information and Communication Technology Services and Statistics. The composition of this Subcommittee shall be

i. Depute Vice Chancellor – Planning, Finance and Administration – Chairperson;
ii. Depute Vice Chancellor – Academic, Research and Consultancy
iii. Director of ICTSS – Secretary
iv. Director of Estates and Technical Services;
v. One Staff representative from each College/School/Institute
vi. Two Students representatives (at least one should be female)
vii. One co-opted member who is an ICT expert from outside MUST

4.1.4 The Directorate of Information and Communication Technology Service and Statistics (DICTSS)

There shall be the Directorate of ICTSS which will be responsible for planning, managing and executing all ICT functions of MUST. The ICTSS Directorate shall be responsible for:-

a) The implementation of ICT policies, strategies and standards;
b) Being the focal point of contact for the ICT Service;
c) Specifying, verify and vet ICT standards, procedures and best practices for all University ICT deployments and operations;
d) Having the overall ownership of the professional and technical mandate of all ICT design and developments, management and maintenance;
e) Providing effective ICT support that is responsible to the academic, research, consultancy and administrative functions of the University; and
f) Cooperate with the Centre for Innovation on the ICT innovative solutions necessary for, the functioning of the University.

4.1.5 Departments under the Directorate of ICTSS

The Directorate of ICTSS shall be composed of three (3) departments to manage ICT specialized areas as follows:

a) Computer Maintenance, Networking and Troubleshooting department
b) Software Systems Department
c) Statistics Department

The department of Computer Maintenance, Networking and Troubleshooting shall consist of two units namely

a) Server infrastructure and services Section
b) Networking Section

4.1.6 The Director of Information and Communication Technology Services and Statistics

There shall be the Director of ICT who shall be a holder of a minimum of Masters Degree in Computer Science, Information Technology or equivalent qualifications from recognized institutions. PhD in relevant field is an added advantage. The Director should have working experience of at least twelve (12) years, of which 3 years must be in managerial position in a reputable organization, appointed by the

Council. The Director shall be in-charge of all operational activities of ICT at the University, and will head the Directorate of ICTSS in fulfilling its activities. The Director of ICTSS will report to the Deputy Vice Chancellor – Planning, Finance and Administration.

The Director of ICTS shall perform the following functions:-

a) Promote effective and appropriate utilization of ICT resources;
b) Contribute towards the sustainability of the Directorate in order to enable effective execution of its mandate;
c) Promote an environmentally friendly approach to the acquisition, use and disposal of ICT resources;
d) Coordinate and lead resource mobilization from other sources of funding for the implementation of the ICT strategy;
e) Operationalize and guide the ICT policy implementation.

4.1.6 College of Information and Communication Technologies

MUST is knowledge-driven and driving entity. ICT, as opposed to other resources and tools, is entirely knowledge driven. This congruency is seriously taken into account in this policy in order to maximize the potentials that are naturally at MUST disposal concerning ICT as a resource. It is noted that since ICT deployment will mainly require brain power, of which the University can freely unleash, this Policy strives to establish a strategy that will ensure that the free of charge brain power within MUST is maximally exploited for the good of the University community. In view of this, the College of Information and Communication Technologies, and its constituents, will form part of the ICT governance and deployment.

The College of Information and Communication Technologies shall be responsible for:

a) Collaboration with the Directorate of ICTS on developing new ICT solutions for consumption within and out of the University.
b) Promoting training of the ICT staff, as well as capacity building for ICT users both staff and students on emerging technologies relevant to enhance ICT services in the University.
c) Providing technical support to the Directorate on development and deployment of ICT infrastructure and services.
d) Collaborating with the Directorate of ICTS to conduct ICT research on the University infrastructure provided it does not jeopardize the University systems and use the findings to enhance a provision of the University ICT services.

4.1.7 The Directorate of Library Services

The Directorate of Library Services shall be responsible for:

a) Selecting, acquisition, processing and making available appropriate information resources to support teaching, learning and research.
b) Collaborating with DICTS to ensure that all ICT requirements for up-to-date library are in place.
c) Ensuring facilities are available for creation, maintenance, and accessibility of library systems, resources, and services. These systems include, but not limited, to Online Public Access Catalogue (OPAC), digital repositories and archives, e-books, e-journals, and other relevant information resources and services.

4.1.8 Boards of Colleges, Schools or Centres

This policy acknowledges existence of Colleges, Institutes, Schools and Centers and their respective Boards. As part of their activities, such Boards shall consider application of ICT policy in their respective areas, units of weakness and

shortcomings, targeted areas for intervention and improvement. They will also advise on ICT strategy and tactics for development and use in their entities.

Boards of Colleges, Institutes, Schools or Centers will be responsible for the following within their entities:

a) Establish development of new services.
b) Consider policy and technical issues regarding ICT in instructional and academic management, including electronic classrooms, course management systems and ICT support.
c) Identify the need for ICT at their areas and advise the ICT Technical Committee for implementation.
d) Advise the ICT Technical Committee on matters related to the use of ICT in the improvement of Mbeya University of Science and Technology functions related to their areas.
e) Evaluate the use of ICT at their area and recommend aspects for improvements.

4.1.9 The Centre of Innovation and Technology Transfer

Innovation is essential condition for business success, economic growth, competitiveness and live hood sustainability. Likewise Technology Transfer helps to develop early stage intellectual property asset by innovators or researchers into products for public use. In view of this, the College of Information and Communication Technologies, and its constituents, will form part of the ICT governance and deployment. Therefore the linkage between CITT and ICTSS will enhance successful implementation of Innovation and Technology Transfer and the products delivered to help in solving University challenges.

The Centre of **Innovation and Technology Transfer** shall be responsible for:

a) Collaboration with the Directorate of ICTSS on developing new ICT solutions for consumption within and out of the University;

b) Providing technical support to the Directorate on development and deployment of ICT Infrastructure and services;
c) Collaborating with the Directorate of ICTSS to conduct ICT research on the University infrastructure provided it does not jeopardize the University systems and use the findings to enhance provision of the University ICT services.

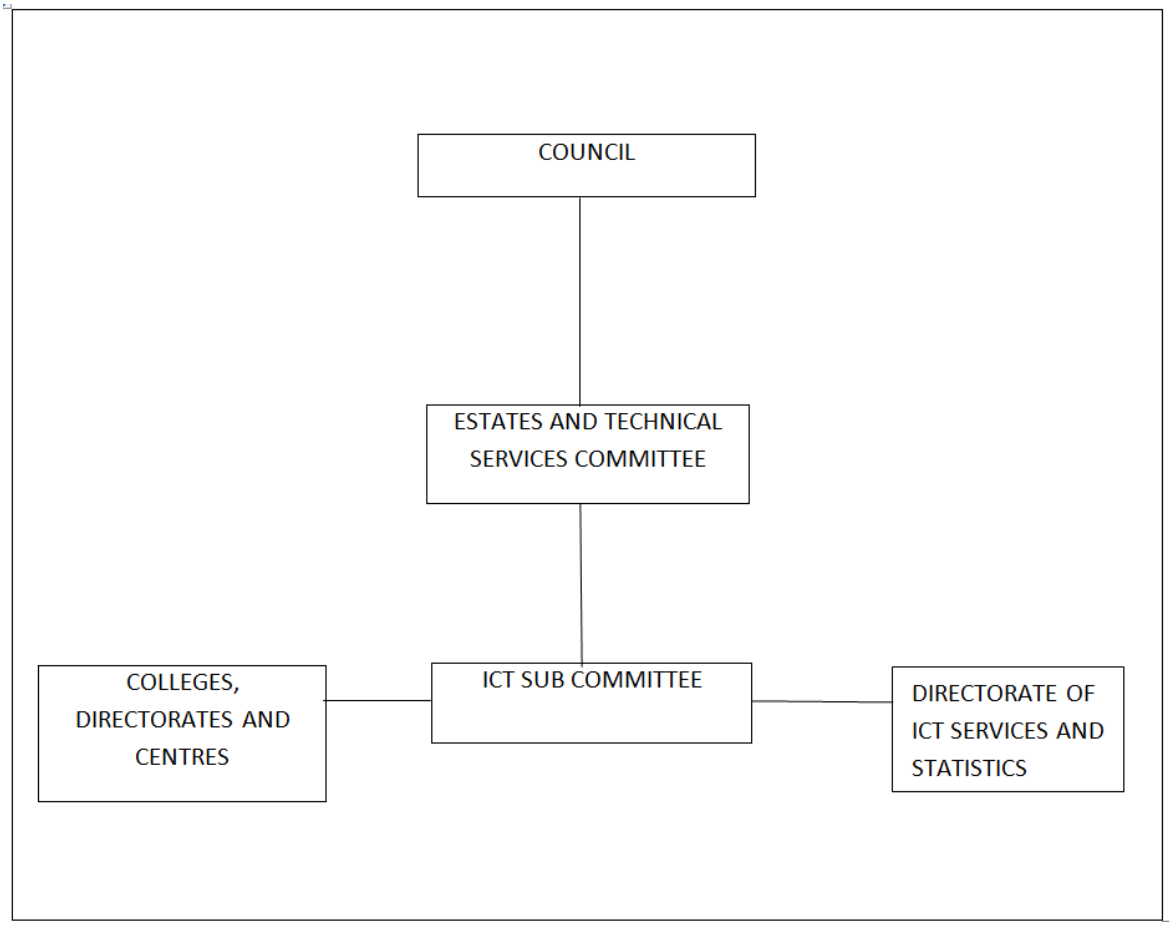
4.1.10 The Centre for Virtual and Continuing Education

MUST is knowledge -driven and -driving entity. ICT, as opposed to other resources and tools, is entirely knowledge driven. This congruency is seriously taken into account in this policy in order to maximize the potentials that are naturally at MUST disposal concerning ICT as a resource. It is noted that since ICT deployment will mainly require brain power, of which the University can freely unleash, this Policy strives to establish a strategy that will ensure that the free of charge brain power within MUST is maximally exploited for the good of the University community.

The Centre of Virtual and Continuing Education shall be responsible for:

a) Collaboration with the Directorate of ICTSS on developing new ICT solutions for consumption within and out of the University.
b) Promoting training of the ICT staff, as well as capacity building for ICT users both staff and students on emerging technologies relevant to enhance ICT services in the University.
c) Providing technical support to the Directorate of ICTSS on development and deployment of ICT infrastructure and services.
d) Collaborating with the Directorate of ICTSS to conduct ICT research on the University infrastructure provided it does not jeopardize the University systems, and use of the findings will enhance provision of the University ICT services.

The Organization Structure



4.2. Implementation Guidelines

This policy provides the framework guiding governance of ICT at the Mbeya University of Science and Technology. However, the policy is not exhaustive of all required regulations and guidelines for governance of ICTs. There shall be ICT regulations and guidelines which will accompany the policy and equally binding to provide guidance in planning, use and management of ICT at the Mbeya University of Science and Technology.

4.3. Monitoring and Evaluation

The implementation of the ICT policy is hinged against the policy statements stipulated in this document, the University Strategic Plan, as well as yearly work plan drawn by the Directorate of ICTSS. The ETSC shall work with all MUST stakeholders in

monitoring and evaluation of the policy. Feedback mechanism for implementation of this policy will begin at College, Directorates and Centres, followed by ICT Sub-committee then Estate and Technical Services Committee in their quarterly meetings. In a situation where the policy needs to be changed as the result of feedback from the said organs, such request shall be channeled to the Council, the overall overseer of the Policy.

4.4. Effective for the Policy

This policy shall be effective from the date it is approved by the Council.

4.5. Policy Review

The policy shall be reviewed after every five years or as it may be decided by the Council.

Bibliography

The United Republic of Tanzania (2016). National Information and Communications Technology Policy.

The Mbeya University of Science and Technology (2017/18 – 2021/22). Corporate Strategic Plan.

The Mbeya University of Science and Technology (2014). Information and Communication Technologies Policy.

The Mbeya University of Science and Technology (2017). Resource Mobilization Policy

Makerere University (2016), Information and Communication Technology Policy (2016-2020).URT (2010) National Development Vision 2025