MUHIMBILI UNIVERSITY OF HEALTH AND ALLIED SCIENCES

INFORMATION & COMMUNICATION TECHNOLOGY (ICT) POLICY AND PROCEDURES

November 2017

ACRONYMS

CCTV	Closed Circuit Television
CEPD	Continuing Education and Professional Development
DCEPD	Directorate of Continuing Education and Professional Development
DICT	Directorate of Information and Communication Technology
DLS	Directorate of Library Services
E-Learning	Electronic Learning
HEIs	Higher Education Institutions
ICT	Information and Communication Technology
IMS	Information Management System
ISP	Internet Service Provider
MAMC	MUHAS Academic Medical Centre
MUHAS	Muhimbili University of Health and Allied Sciences
NSGRP	National Strategy for Growth and Reduction of Poverty
R&D	Research and Development
SDGs	Sustainable Development Goals
SOP	Standard Operating Procedures
VPN	Virtual Private Network

TABLE OF CONTENTS

1. INTRODUCTION

1.1. Background

Information and Communication Technology (ICT) is central in facilitating research, curricular development and implementation, administration and management at universities. Accelerated developments in ICT have created new opportunities for higher education institutions (HEIs) to make optimal use of these developments. The Muhimbili University of Health and Allied Sciences (MUHAS) like other HEIs is challenged to appropriately deploy ICT infrastructute, systems and services to achieve its core functions. For MUHAS to attain its vision of becoming, *"A University excelling in quality training of health professionals, research and public services with conducive learning and working environment"*, it will have to adopt and implement extensive use of ICT to perform the University's core functions which include teaching, research and consultancy.

MUHAS foresees the need to continue expanding student enrolment and academic programs to meet the national health human resource needs. This is markedly demonstrated by the effort to expand into a more spacious area at Mloganzila campus. However, this expansion in enrolment and academic programs needs to be matched with the expansion of existing facilities and resources at MUHAS. Use of ICT provides opportunities for the University to cope with the challenges of training increased numbers of competent health professionals in this era of knowledge society. It is thus imperative for MUHAS to acquire the appropriate and adequate human resource and infrastructure to facilitate optimal deployment of ICT services to enable national economic growth through improved outputs of MUHAS core objectives. Furthermore, the University has to ensure that its ICT resources and facilities are used solely for the purposes for which they were intended. Thus, formulation of this policy and procedures is to guide proper planning, development, deployment and use of ICT services at the University. The context of this policy and procedures originates from other existing policies and strategies at MUHAS including MUHAS Five Years Rolling Strategic Plan 2015/16 to 2019/20, MUHAS Ten Years Corporate Strategic Plan 2014/2015 to 2023/24, Intellectual Property Policy & Procedures (2011), Library Policy and Procedures (2013), Research Policy and Procedures (2011) and the Institutional Repository Policy (2012), Report of a Technical Assessment of ICT Infrastructure, Systems and IT Services at MUHAS (2017).

1.2. Rationale

MUHAS needs to meet its objective of improving its services and increasing productivity by leveraging on new technologies. The University has been investing in ICT to facilitate its core functions of teaching, reseach and public services so as to attain its strategic goals. The university operations are increasingly depending on ICT, making the Institution vulnerable to ICT related risks. In this regard, it is evident that, MUHAS needs to develop and operationalize comprehensive ICT Policy to direct ICT adoption and usage within the Institution. Thus, MUHAS developed its first ICT Policy in 2004. Due to changes in ICTs and other institutional develepments occurred there is a need to revise the policy document to cater for the changes.

1.3. Purpose and Context

This document provides the highest level ICT directives for the Muhimbili University of Health and Allied Sciences (MUHAS) for the main purpose to ensure that MUHAS's ICT related investment, operations and maintenance processes and usage are well directed while discarging its core functions. The policy is based on standard policy framework issued by MUHAS and had taken into consideration other existing university level policies and other National policies for the purpose of ensuring institutional-wise and national policy linkages.

1.4. Scope of the ICT Policy and Procedures

This policy and procedures is applicable to all MUHAS's staff and students, visitors as well as providers offering services to MUHAS, all users of ICT equipment owned or leased by the Institution as well as all equipment connected to MUHAS's ICT related infrastructure. In addition, the policy applies to all MUHAS's ICT related resources and services. This is a University wide ICT policy and procedures applicable to all campuses and centres as well as student hostels.

1.5. Relevant Government Policies and Legislations

The ICT policy and procedures is in-line with the following National Framerorks and key policy documents:

i. The Tanzania's National ICT Policy of 2016, which emphasizes the use of ICT to enhance and improve the quality of delivery of education in all areas.

ii. The Education and Training Policy (2014) that emphasizes the importance of the application of ICT in the Universities to improve teaching and learning and other related functions.
iii. The Universities Act (2005) which advocates on the need for the availability of adequate ICT facilities and services in terms of quality and quantity to support the core functions of the University.
iv. Tanzania National Health Policy (2007), Tanzania Development Vision 2025, the National Strategy for Growth and Reduction of Poverty (NSGRP), Five Year Development Plan and the Sustainable Development Goals (SDGs).
v. Tanzania Cybercrimes Act, 2015
vi. Circular No. 3 of 2013 guidelines on the implementation of various ICT systems
vii. Circular No. 5 of 2009 on proper use and ICT security
viii. Circular No. 6 of 2009 on Storage and disposal of information on ICT devices

1.6. Policy Objectives and Outcomes

This document provides the highest level ICT directives on management, deployment and use ICT to ensure that MUHAS's ICT related investment, operations and maintenance processes are cost-effective and efficient for the enhancement of quality research, teaching and learning, administration and management related activities. The specific objectives of this policy are;

i. To provide equitable access to ICT services to all members of the MUHAS community.
ii. To strengthen and promote the use of ICT in MUHAS core functions
iii. To ensure the members of the universty use ICT facilities and services in an appropriate and responsible manner and to ensure that other persons do not misuse those ICT facilities and services.
iv. To facilitate strengthening of ICT infrastructure to support and enhance teaching and learning and public service.
v. To strengthen capacity to handle ICT security issues related to privacy, cyber-crime, ethical and moral conducts.
vi. To establish partnership on ICT with other institutions within and outside the nation.
vii. To enhance the existing teaching and learning partnership between MUHAS and other Institutions.

It is expected that the following outcomes will be attained upon fully implementation of the policy.

i. Establishment of appropriately-equipped and functional MUHAS ICT facilities
ii. Empowered MUHAS community in the optimal and ethical use of ICT facilities and services for enhanced output of the University core functions
iii. Expanded student enrolment and academic programs through distance education and e-learning programs
iv. Improved efficiency and effectiveness of administration and management related activities at MUHAS
v. Enhanced student learning through appropriate use of ICT for active, social and participatory learning, extended discussions and learning communities
vi. Increased capacity for research in e-learning technologies and their applications
vii. Enhanced capacity for income generation for the University
viii. Improved quality and accessibility of research outputs, delivery of educational materials and community services
ix. Improved visibility and ranking of the University profile globally

2. DEFINITION OF TERMS

i. **Antivirus** is a “protective software designed to defend your computer against malicious software. Malicious software, or "malware" includes: viruses, Trojans, key loggers, hijackers, dialers, and any other code that vandalizes or steals your computer contents”

ii. **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 Megabits per second (Mbps), or Gigabits/second (Gbps).

iii. **Distance learning** is defined as “Provision of learning opportunities to learners situated away from a University campus”.

iv. **E-learning** is use of information and communication technologies to enhance and support teaching and learning. This definition encompasses e-learning which supports teaching and learning through the provision of online resources to support classroom-based learning, distance learning, and distributed learning models.

v. **Electronic mail** is a system of world-wide electronic communication in which a computer user can compose a message at one terminal that can be regenerated at the recipient's terminal when the recipient logs in.

vi. **Firewall** is a set of related programs, located at a network gateway server that protects the resources of a private network from users from other networks. The integrity of this protective barrier depends on the effective deployment, configuration and capabilities of individual firewall programs.

vii. **Free and open source software (F/OSS, FOSS)** is software that is, liberally licensed to grant the right of users to use, study, change, and improve its design through the availability of its source code.

viii. **Hardware** is a comprehensive term for all of the physical parts of a computer, as distinguished from the data it contains or operates on, and the software that provides instructions for the hardware to accomplish tasks.

ix. ICT Assets/Resources cover all ICT facilities including the University and hospital network, all computers, computing laboratories, all associated networks in classrooms, lecture theatres, and video conferencing rooms across the University. It is also cover internet access both wired and wireless, email, hardware, data storage, computer accounts, software (both proprietary and those developed by the University), audio visual system including telephone services and voicemail.

x. **Information and Communication Technology (ICT)** refers to all those instruments, modes, and means through which information or data is captured, processed, stored and transmitted or communicated from one person to another or from place to place.

xi. **Information management systems** is a computer program (consisting of data storage systems, software and services, providing automated networked storage solutions) that lets one or more computer users create and access data in a database, having extensive transaction processing capabilities.

xii. **Institutional repository** is an online locus for collecting, preserving, and dissemination in digital form of the intellectual output of an institution, particularly a research institution.

xiii. **Internet** is a computer network consisting of worldwide interconnected networks of computers that use the standard Internet Protocol (TCP/IP) to facilitate data transmission and exchange,

xiv. **Intranet** is a private computer network that uses Internet Protocol technologies to securely share any part of an organization's information or operational systems within that organization, often protected from Internet traffic.

xv. **Online learning** means that the whole course is conducted online and students can follow their courses from any geographical location.

xvi. **Proprietary software** is a, "computer software licensed under exclusive legal rights of its owner"

xvii. **Software** is a collection of various kinds of programs that are used to operate computers and related devices.

3. POLICY STATEMENTS AND PROCEDURES

The policy statements are presented in Thirteen thematic policy issues followed by the operational procedures under each policy statement.

3.1. ICT Governance and Management

ICT Governance is an integral part of University governance and consists of the leadership, organisational structures and processes that ensure that the organisation's ICT sustains and extends the organisation's strategies and objectives.

Effective ICT Governance provides a conducive environment for the alignment of all ICT investments in a rationalized manner that is aligned towards enabling the University meet its goals and objectives. This also contributes to the attainment of value for money, management of risks and effective ICT utilization. In addition, to accelerate achievement of University mission, ICT services need to be given support at the highest level by the University management through resource allocation and the ICT directorate needs to engage in resource mobilization activities to supplement the limited resources received from the government.

3.1.1. Policy Statement 1

The University shall give the highest priority to ICT, and enforce its application cohesively in all its core functions.

Operational Procedures

The University shall:

i. Impose the use of ICT in all its administrative and management functions as well as in implementing MUHAS curricular
ii. Ensure availability of adequate and skilled ICT human resources in terms of technical, academic and administrative staff
iii. Ensure that MUHAS becomes a centre for creativity and generation of ICT related knowledge, and software to drive it's academic, administrative and management functions.
iv. Ensure that staff and students have access to ICT facilities to facilitate their day to day activities
v. Institute measures to ensure that schools, institutes, directorates and research projects consults DICT before undertaking any ICT initiative for the sake of harmonizing efforts

and optimizing resources

vi. Ensure availability of appropriate software and hardware to meet the needs of the University community

The DICT shall:

i. Monitor development and innovations in ICT sector, in order to advise on implementation of innovative and sustainable ICT solutions aligned to the University's strategic goals
ii. Undertake advocacy for the adoption and utilization of ICT within the University
iii. Promote effective and appropriate utilization of ICT facilities and services by staff, students and other authorized users.
iv. Ensure that ICT Risk Management periodically done, where ICT risk assessment is conducted and reviewed, likelihood and occurrence identified, mitigation strategy established and risks treated, accepted, transferred or avoided.
v. Establish mechanism for evaluating and monitoring ICT services (e.g. Service availability, staff satisfaction / feedback system) and its compliance.
vi. Develop guidelines on disciplinary actions for violation of this ICT policy

Heads of Departments, Administration and Research Units shall:

i. Integrate ICTs into their activities;
ii. Implement and ensure compliance to the Unit specific components of the ICT Policy and other related strategies; and
iii. Act as active participants during the periodic stakeholder consultations towards supporting and facilitating the effective implementation of the ICT Policy and other related strategies.

3.1.2. Policy statement 2

The University shall ensure availability of adequate financial resources to acquire and manage ICT facilities and services.

Operational Procedures

The University shall:

i. Include in its annual budget adequate funds to sustain ICT human and physical and software resources

The DICT shall:

i. Assess actual ICT resources needed at the University
ii. Prepare a predictable annual ICT budget for regular acquisition of appropriate ICT resources and services.
iii. Pursue innovative ways to mobilize resources for maintaining ICT services
iv. Seek partnerships and collaborations as a way to access resources for financing ICT services and facilities.
v. Develop short and long term ICT courses and execute other activities for purposes of mobilizing additional resources to sustain ICT services.
vi. Solicit funds by writing competitive fundable proposals
vii. Prepare and report its income generating activities on quarterly basis or when deemed necessary.

3.1.3. Policy Statement 3

The University shall utilize the existing partnerships and seek new partners to regularly improve MUHAS ICT infrastructure and services.

Operational Procedures

The University shall

i. Promote the use of innovative approaches to seek resources for maintaining ICT infrastructure and facilities
ii. Promote collaboration with both local and international partners in investments to improve ICT infrastructure.

3.1.4. Policy Statement 4

The University shall monitor and evaluate all usage of ICT facilities, services and contents to ensure applicability, safety and security.

Operational Procedures

The DICT shall:

i. Continuously monitor ICT resources and e-content to support MUHAS core functions, operational maintenance, auditing, security and investigative activities.
ii. Together with the University as part of its legal requirements and business processes, shall

conduct internal and external audits of all ICT facilities and services.

3.1.5. Policy Statement 5

The University shall ensure all users are aware of the provisions set forth in the policy document for compliance

Operational Procedures

The DICT shall:

i. Prepare leaflets summarizing key policy provisions targeting end users
ii. Publicize this policy to all MUHAS Community through MUHAS website, brochures and other communication media.

3.2. ICT Infrastructure and Internet Services

ICT infrastructure is the backbone for supporting the University business operations by enabling information exchange and providing secure access to different applications. This consists of all hardware devices such as network devices, servers, security devices, workstations, laptop computers, storage, back-up, operating facilities and supporting platforms like operating systems and databases.

The objective of managing ICT Infrastructure is to ensure that the University's ICT infrastructure operations are optimized in order to deliver higher level service quality and support business-relevant operations based on ICT planning and management best practices.

3.2.1. Policy statement 6

The University shall continue to improve its institution-wide data communication network and availability of appropriate hardware and software in order to meet the needs of the University Community.

Operational Procedures

The DICT shall:

i. Facilitate the development of a data communication infrastructure to linkup with its constituent campuses

ii. Ensure availability of appropriate software and hardware to meet the needs of staff and students
iii. Ensure availability of alternative sources of power for smooth running of ICT services
iv. Establish common set of standards for hardware, system architecture, and software (proprietary as well as free and open source) for use at the University
v. Encourage the development and deployment of localized software and applications developed to meet Tanzanian contexts.
vi. Collaborate with relevant institutions to examine and implement optimal configuration and utilization of ICT to perform MUHAS core functions, with focus on equitable access and quality.
vii. Ensure that the University libraries have adequate ICT to effectively act as points of dissemination of ICT-based information resources
viii. Safeguard the appropriate use of software by the various departments
ix. Establish a remote server system for real time storage of MUHAS data and documents
x. Establish an active directory server (ADs) for MUHAS staff and students to enhance real time storage of data
xi. Establish modalities for sharing of ICT resources at the University, in order to reduce costs and avoid duplication of efforts
xii. Ensure availability of wireless access to internet for enabling staff and students to access digital resources and services.

3.2.2. Policy statement 7

The University shall ensure that there is sufficient bandwidth to meet the requirements of the entire University and its campuses.

Operational Procedures

The DICT shall:

i. Ensure that all ISPs engaged by the University guarantee availability of adequate backup so that internet connectivity is available at all times and on the agreed bandwidth
ii. Bandwidth usage is restricted to ensure that access to critical information, research and online educational resources are always optimal
iii. Explore viable strategies to reduce bandwidth costs for the institution

iv. Ensure that the bandwidth is restricted from unauthorized persons and services
v. Monitor the bandwidth usage through management of network devices to ensure optimal functioning and security.
vi. Perform periodic Assessment of bandwidth requirements to meet needs of the university and campuses.

3.2.3. Policy statement 8

The University shall ensure availability of a secure and reliable email system and provide each student and staff an email address under the University domain name structure.

Operational Procedures

DICT shall

i. Develop email communications standard operating procedures for University staff and students
ii. Ensure that the e-mail system is protected from physical and non-physical threats
iii. Provide mechanisms to control the amount of unsolicited emails that users receive
iv. Provide mechanisms to intercept emails that contains viruses
v. Ensure postings by users from the University email 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.

3.2.4. Policy statement 9

The University shall ensure that its website is regularly update and have contents that conforms to its mission objectives and functions.

Operational Procedures

The DICT shall:

i. Ensure the University website is updated regularly.
ii. Ensure accessibility of the website within and outside the University network infrastructure.
iii. Provide a mechanism to ensure that intranet services are accessible only to the University

community.

iv. Prepare monthly, quarterly and annual reports summarizing website updates done per specific unit.

Heads of Schools, Directors, Departments, Administration and Research Units/Projects shall:

i. Prepare and submit to DICT web contents and information of their respective units for uploading onto the University website
ii. Regularly review and update contents of onto the University website
iii. Report in writing to DICT any anomalies/problems encountered in accessing the University website and their respective websites
iv. Units shall designate focal point (content developers) responsible with updating website content by providing content to website designated officer from ICT Unit.

3.2.5. Policy statement 10

The University shall ensure system are deployed and hosted in secured a Data Centre to enhance availability and accessibility

Operational Procedures

The University shall ensure that no entity within University are to be allowed to host its website or web-pages outside the university's web server.

The DICT shall:

i. Assess the requirement for Hosting Critical ICT Systems
ii. Advice the management on where ICT systems are to be hosted taking into consideration of Government issued guideline.

3.2.6. Policy statement 11

The university shall ensure that all buildings used for academic and administrative purposes are provided with access to the university's interconnected ICT facilities through the provision of data and telephone points.

Operational Procedures

Director of Estates shall ensure

1. The directorate of ICT is actively involved in the review and approval of specifications of ICT infrastructure and systems for new buildings and renovations
2. The directorate of ICT is consulted in writing before embarking on renovation of a building so that ICT facilities and systems are securely remove or relocated without affecting other systems/users

3.3. ICT Services and Access Management

The University shall ensure the provision of the ICT Services within the University as well as define a Unit responsible for ICT 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 at all campuses and their related technical support.

The objective is to define and implement an effective ICT Service Management and Support approach that is aligned to the Vision of the University Strategic Plan where ICT is identified amongst the key components in the support of the University's goals and objectives. This will eventually ensure that the use of University's ICT facilities and services is appropriate to avoid misuse of the facilities and services by authorized users as well as enable the monitoring and improvement of service quality through the effective application of processes.

3.3.1. Policy statement 12

The University shall provide access to ICT resources and services to MUHAS community at different levels.

Operational Procedures

DICT shall:

i. Ensure standard operating procedures for access and use of ICT services are in place and are monitored.

ii. Ensure ICT services for personal use are monitored to minimize disruption of University core business.

3.3.2. Policy statement 13

The University shall ensure proper use of ICT resources and services by MUHAS community at all levels in a cost-effective manner.

Operational Procedures

The University shall to promote shared use rather than duplication of ICT facilities. The Shared ICT facilities include:

i. Internet and email services Campus area network and wide area connectivity
ii. Corporate Antivirus
iii. Video conferencing system
iv. Management Information Systems
v. Integrated Library System
vi. Learning Management System
vii. Student Management System

DICT shall:

i. Ensure ICT use is in accordance with Government issued Guidelines and Circulars
ii. Ensure all software installed on MUHAS systems (including all commercial and shareware products) are used in compliance with all applicable licenses, notices, contracts, and agreements.
iii. Ensure that all authorized users have appropriate access privilege level that is protected.
iv. Monitor users to ensure that ICT resources are used primarily to perform University core functions
v. Users shall not be authorized to engage in any activity that is illegal under Tanzanian or international law while utilizing the University ICT resources. The following activities shall be strictly prohibited, with no exceptions, failure of which legal or disciplinary enforcement may be invoked:
    (a) To view, access, or transmit offensive material. This applies to any screen display or printing of images, sounds or messages that could reasonably be considered obscene, pornographic, profane or otherwise objectionable.
    (b) To threaten, harass, defame, libel or slander any other person
    (c) To introduce malicious programs into the network or server, for instance viruses,

worms, Trojan horses, e-mail bombs, creating or forwarding "chain letters," "Ponzi", junk mails or other "pyramid" schemes of any type.

(d) Extensive recreational game playing, video streaming, especially during normal working hours.

(e) Use University ICT infrastructure and services for unauthorized commercial purposes, such as advertisement, provision of services, and/or selling of commercial products or services.

(f) 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.

(g) Making fraudulent offers of products, items, or services.

(h) Disruptions of network communication as a result of accessing unauthorized data or logging onto the server via fraudulent means.

(i) Port scanning or security scanning unless authorized in writing by the Director of ICT.

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

(k) Circumventing user authentication or security of any host, network or account.

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

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

(n) Using the University network or infrastructure services to offer services to others within or outside the University premises on free or commercial terms.

(o) Unauthorized use, or forging, of email header information.

(p) Solicitation of email from any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

Director of Human Resource Management and Administration (DHMRA) shall

i. Inform DICT on any changes to staff engagement including hiring, change of duty status/location, suspension or termination, retirement.
ii. Ensure staff have their clearance forms of signed by DICT indicating that access to facilities/resources are revoked.

Users shall

i. Ensure lawful use of computer data and equipment while accessing MUHAS services
ii. Ensure all access rights granted to the user and not transferred to any person without authorisation from DICT
iii. Ensure that credential given to access MUHAS services are not used after the expiration of time or privileges which granted to access the computer system.
iv. Return organisation Equipment after the completion or termination of contract agreement.

3.3.3. Policy statement 14

The University shall provide all authorized ICT users with timely and appropriate technical support services.

Operational Procedures

The DICT shall

i. Establish a single point of contact (i.e. service desk for end users) where requests will be recorded, escalated to the technical staff, resolved and closed to ensure restoration of normal service operations as quickly as possible.
ii. Ensure the technical staff are responsible for ICT user support in the management, control, use, maintenance and repair of ICT facilities.
iii. Provide online support on basic ICT issues, advice and assistance on technical problems faced by users
iv. Establish an online support system using “issue tracker” for handling technical problems on ICT
v. Provide technical support in line with approved ICT procedures for any system, service, device downtime or breach
vi. Provide assistance and guidance towards compliance of ICT policies;
vii. Ensure that reports on service quality are reviewed periodically with customers along in

order to determine things that could be added or changed to improve service delivery and support.

3.4. ICT Security and Business Continuity Management

ICT Security covers all the processes by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction throughout an organization. The general objective of managing ICT Security is to provide MUHAS with information security mechanism to support the Institution to achieve its strategic goals based on best practices.

In addition, the University's business activities need not be interrupted by foreseen and unforeseen events (natural disasters, technological failures or human error) due to sensitivity of information and services provided to the general public and other institutions. For this to happen, Business continuity management need to be well planned and implemented to minimize the impact on business operation to an acceptable level and facilitate quick recovery of information systems. In this direction, policy commitments are needed to ensure all Strategic Business entities are identified and secured to ensure continued provision of business services.

3.4.1. Policy Statement 15

The University shall ensure that all ICT resources (software, hardware, data, system users) and services are maintained, controlled, protected and secured to enable the University functions run smoothly.

Operational Procedures

The University shall develop ICT Security Policy to ensure that

i. Each user respects the privacy and integrity of other users. No user shall be able to view, copy, alter or destroy another person's electronic files
ii. All University computing devices (desktop and laptop computers, servers, etc.) are protected against malicious software through the installation of antivirus and firewall software.
iii. System and network administrators will respect the privacy of personal communications in all forms including telephone, electronic mail and file transfers.
iv. Information systems are designed, acquired and implemented with effective ICT security

controls to safeguard the integrity, confidentiality and continual availability throughout the entire life cycle

v. ICT security risks are mitigated and controlled

Operational Procedures

The DICT shall monitor use of ICT Resources and ensure that

i. Each user respects the privacy and integrity of other users. No user shall be able to view, copy, alter or destroy another person's electronic files

ii. Users' accounts will be monitored in order to maintain and protect the integrity, security and functionality of University ICT resources.

iii. System and network administrators will respect the privacy of personal communications in all forms including telephone, electronic mail and file transfers.

3.4.2. Policy Statement 16

The University shall implement processes to ensure that services are available and accessible all the time.

Operational Procedures

The University shall develop Business Continuity and Service Recovery Plan to ensure that

i. Framework for building resilience and the capability for an effective response which safeguards the interests of the Authority and of its key stake holders is established

ii. Systematic approach processes to manage risks on continuous basis are implemented.

The DICT shall

i. Conduct a Business Impact Analysis to identify critical business functions to be supported by ICT.

ii. Ensure that a robust business continuity and service recovery plans are implemented and regularly reviewed and tested.

3.5. ICT Asset and Service Management

ICT Asset and Service Management involves activities for asset acquisition, storage, usage, maintenance and disposal as well as on how services are delivered. The assets include ICT

hardware, software, data, system documentation, and storage media, supporting assets such as computer rooms, air conditioners and power back up systems.

Poor management of ICT systems and individual components can pose grave risks to the MUHAS staff and students. It can also lead to waste of both physical and financial resources. Thus, there is a need to ensure that user departments' ICT assets and services and properly acquired, maintained to guarantee quality, value for money and avoid other associated risks.

3.5.1. Policy statement 17

The University shall acquire all ICT facilities and resources according to the needs of the University community.

Operational Procedures

The DICT shall

i. Assist user departments to derive and review their ICT acquisitions and purchases to ensure that the equipment required is of the required standard and have value for money.
ii. Establish standard procedures for the identification, evaluation and selection of appropriate hardware and software (proprietary and free and open source software)
iii. Update the minimum specifications of all ICT facilities to meet the demands of the latest technologies to fulfil the needs of the University community
iv. Acquire volume licenses for appropriate software in accordance to the needs of the University community

The Head of User Departments shall

i. Make sure all purchase requests for hardware, software, or computer-related components meets the department/unit needs
ii. Make sure all specifications of hardware, software, or computer-related components are reviewed and approved by the Directorate of ICT.

3.5.2. Policy statement 18

The University shall ensure that all acquired ICT Assets through projects or research collaborations are owned by the institutions.

Operational Procedures

The DICT shall

i. Keep inventory of all ICT Assets acquired through projects and research collaboration
ii. Provide periodic status of the facilities to management

The Head of Schools/Colleges/Departments and Units shall ensure that

i. ICT Assets acquired through projects are owned by units by which the project is implemented.

3.5.3. Policy statement 19

The University shall ensure that all ICT facilities and resources are continuously maintained to facilitate University Business Operations.

Operational Procedures

The DICT shall

i. Establish a database for all ICT assets within the university and promote the proper storage, management and easy retrieval of ICT assets and facilities.
ii. Keep up to date hardware documentation and the same shall be made available to staff who are authorised to support or maintain systems.
iii. Ensure prevention and periodic maintenance is performed on all ICT assets.

The Head of Schools/Colleges/Departments and Units shall ensure that

i. ICT Assets with faults that need to be fixed or upgraded are reported to ICT Directorate timely.
ii. The location of ICT Assets in their respective units are maintained and any re-location of ICT asset should be reported to ICT Directorate.
iii. Ensure the database of assets for their respective units is updated in collaboration with ICT Department.
iv. Acquisition report for ICT system submitted to DICT for record keeping.

Head of PMU shall

i. Notify ICT Department on all new acquired ICT equipment for inspection and record keeping.
ii. Ensure all ICT Equipment are codded per existing Government guidelines.

3.5.4. Policy statement 20

The University shall ensure that all obsolete ICT facilities and resources are disposed of and replaced to meet the needs of the University community.

Operational Procedures

The DICT shall

i. Put in place standard procedures to assess the viability of ICT facilities, resources and services.
ii. Establish a centralized backup and archive system to store important data from obsolete or decommissioned ICT equipment
iii. Ensure that there is a secure mechanism for erasing sensitive information before disposing ICT equipment.
iv. Collaborate with Procurement Management Unit (PMU) to ensure ICT equipment are disposed based on prevailing Government Guidelines for disposal of ICT Assets.

The Head of PMU shall

i. Notify DICT before disposing ICT Assets to ensure data contained in the equipment is removed and stored if needed.
ii. Ensure all ICT disposed Items are done per existing policies and guidelines

3.5.5. Policy statement 21

The University shall ensure that ICT Services are effectively and efficiently delivered to University community and other stakeholders.

Operational Procedures

The DICT shall

i. Define meaningful metrics to measure service results and using the metrics to drive

continuous service improvement

ii. Ensure that monitoring and improvement of service quality through the effective application of processes

iii. ensure compliance with all eGovernment Standards and Guidelines relating to the ICT Service Management.

iv. Ensure that for every ICT services provided, Service Level Agreements between the providers and the recipients are established

v. Ensure that reports on service quality are reviewed periodically with customers along in order to determine things that could be added or changed to improve service delivery and support

3.6. Information Systems and ICT Project Management

Information management systems (IMS) are important for the University to perform its management and administrative functions. To this end automation of the management and administrative functions and processes through the establishment of information systems need to ensure that all the various categories of functions and processes are considered in an integrated manner to avoid redundancy and enhance data and resource sharing among them.

Thus, the acquisition and management of these information systems needs to be well planned and coordinated to ensure optimal use of resources, systems interoperability and valued services. In this way, policy provisions are needed to ensure system acquisition; development, use, maintenance and upgrades are managed properly. In addition, any ICT project initiated within MUHAS need to be well managed for the authority to realize intended objectives. In this respect, policy provisions are required as well to ensure ICT projects are managed in a controlled process which aligns with the appropriate governance structures to control the project. This will identify and manage risks associated with ICT projects and ensure roles and responsibilities are clearly identified.

3.6.1. Policy statement 22

The University shall systematically develop, procure, adopt and adapt information management systems for all its management and administrative functions.

Operational Procedures

The University shall encourage and promote use of information management systems to manage:

i. Administrative transactions and functions
ii. Financial and procurement functions
iii. Estates and transport functions
iv. Laboratory functions including sample archives, diagnostic activities, and maintenance schedules
v. Students' management functions.
vi. Library management functions
vii. Human resources functions
viii. Hospital Management functions

The DICT shall:

i. Ensure that appropriate software and platforms are in place for managing different functions
ii. Acquire, develop or customize software which will be used for local purposes and for income generation
iii. Adopt and adapt open source software to ensure that the IMS used by the University are cost effective and guarantee survival in cases of poor funding.
iv. Train staff and students on the use of various University Information management systems (IMS)
v. Ensure quality management and maintenance of the University Information management systems (IMS)
vi. Make sure all acquired software bare legitimate licenses and accompanied by technician documentation and user manuals.
vii. Make sure all software developments and customisations comply with user department requirements and other relevant standards and guidelines.

The Head of Colleges/Schools/ /Departments/Units shall ensure that

i. All functions of their respective units are automated by providing requirements to the university.

3.6.2. Policy statement 23

The University shall implement ICT Projects or initiatives those are addressing university core mission, aligned to other university initiatives and sustainable in nature.

Operational Procedures

The University shall:

i. Develop a prioritised list of key ICT Projects or subcomponent of the Project / initiatives that they require to be implemented over the course of the financial year.
ii. Ensure that any ICT project or subcomponent of the Project /Initiative is aligned to University objectives regardless of sources of financing.
iii. Make sure DICT is involved in all stages of any ICT project namely initiation, preparation, negotiation, execution, monitoring and evaluation and closure.
iv. Shall ensure projects are reviewed by other authorities based on existing national policies and guidelines

The DICT shall:

i. Be involved in all stages of any ICT project or subcomponent of the Project namely initiation, preparation, negotiation, execution, evaluation and closure.
v. Make sure ICT projects are evaluated periodically to ensure the project is implemented within required standards.

The Head of Schools/Colleges/Departments shall ensure that

i. ICT projects or subcomponent of the Project need to be initiated by respective user department in collaboration with DICT through project Concept Note or similar project write-up.
ii. Initiated ICT projects take into consideration available ICT systems as well as other inter – departmental collaborative needs.

3.7. Application of ICT in Teaching, Research and Consultancy

Teaching, Research and Consultancy are among the three MUHAS core functions. The increasing pressure for the need to continue to expand student enrolment in a bid to meet the national health human resource needs, MUHAS need to improve the delivery of its educational programmes and

cope with the increasing number of students and programmes through integration of ICT in teaching and learning activities. In addition, Use of modern ICT to enhance research and consultancy services is vital to ensure effective and efficient knowledge creation, management and sharing. However, among the challenges that MUHAS is facing like many other modern universities is to responsibly align ICT as a positive force for encouraging creative pedagogical methods for academic staff and expanding instructional options for students and the expanding need to enhancing research and consultancy services though application of ICT.

3.7.1. Policy statement 24

The University shall use ICT to enhance teaching and learning.

Operational Procedures

The University shall:

i. Establish e-learning Policy to govern teaching and learning activities
ii. establish and maintain appropriate e-learning infrastructure and services to support teaching and learning
iii. Employ qualified technical ICT staff to manage and support e-learning infrastructure and services
iv. Make available alternative sustainable energy to ensure smooth running of e-learning systems.

The DICT shall:

i. Deploy and maintain one type of e-learning platform for the whole University to avoid duplication of efforts and to enhance sharing and exchange of contents, and tools
ii. Ensure open source e-learning platform is adopted to avoid unnecessary recurrent costs on software procurement.
iii. Ensure that the intranet and the internet infrastructure facilitate learning and teaching on campus and off-campus
iv. Acquire and maintain appropriate hardware (such as, computers, cameras, servers, hard disks, tele-presence and others) to support e-learning and teaching activities in all possible learning environments.
v. Improve network systems including Local Area Network (LAN), Wide Area Network (WAN) and other data communication systems in all possible learning environments
vi. Enhance and optimize internet bandwidth to meet requirements for e-learning.

vii. Acquire appropriate software for preventing plagiarism, authoring and editing of audio-visual e-learning content, and other related software for e-learning purposes

viii. Provide personalized accounts for users in the e-learning platform, to meet their diverse learning, teaching and research needs.

ix. In collaboration with DCEPD and DLS promote use of collaboration, communication, and feedback tools through discussion forums, chat rooms and other related features in the e-learning platform

x. In collaboration with DCEPD and DLS facilitate the dissemination of best practices, case studies and other relevant information for e-learning purposes

xi. In collaboration with DCEPD and DLS promote and support peer review tools and student assessment of academic staff (such as, mass voting system) to enhance teaching, learning and research

xii. Integrate the electronic materials stored by the University library systems (representing massive resources for research, teaching and learning) with the e-learning platforms to ensure re-usability of e-learning resources

xiii. Develop and maintain e-learning platform that supports a repository of reusable learning objects (RLO) at MUHAS to ensure future re-use of e-learning contents, templates and tools

xiv. In collaboration with the Directorate of Library Services (DLS) integrate the institutional repository, electronic reference services, and other emerging technologies at the library services with the e-learning platform.

xv. Link e-learning system with the library information system, student management information and financial information system and other relevant information systems at MUHAS.

3.7.2. Policy Statement 25

The University shall ensure that the e-learning system is secured and access given to authorized users only.

Operational Procedures

The DICT shall:

i. Ensure physical protection of the e-learning facilities at MUHAS

ii. Acquire the necessary hardware and software for the purpose of monitoring and protecting

e-learning systems against damage, misuse and unauthorised access.

iii. Put in place standard procedures for backup to ensure regular backups of e-learning contents and technologies.

iv. Ensure that access authentication mechanisms are implemented on the e-learning platform through the use of username and password.

v. Train faculty and other content developers on how to impose access restrictions on their materials for reading, editing or copying on the platform.

3.7.3. Policy Statement 26

The University shall ensure development and protection of appropriate local content for teaching and learning.

Operational Procedures

The University Shall

i. Ensure intellectual property policy and guidelines have provisions to govern copyright issues regarding e-resources and e-learning contents.

The DICT shall:

i. Ensure content developers adhere to intellectual property policy and guidelines

ii. E-resources copyright notices from online public systems are adhered to.

3.7.4. Policy Statement 27

The University shall facilitate use of ICT for research and consultancy management.

Operational Procedures

The DICT shall:

i. Provide the ICT expertise necessary to improve access and visibility of research findings produced at the University.

ii. Ensure accessibility of internally available electronic research resources outside the MUHAS network through establishment of a virtual private network (VPN)

iii. Establish and maintain research data management system where all the data from the field should be archived.

iv. Ensure use of software packages (preferably open source software tools) for research data analysis and management is a priority.

The DLS shall

i. Manage and maintain contents in the institutional repository based on existing university policies

3.8. ICT Training and Capacity Building

In order for the University to ensure good and efficient usage of ICT services all academic and administrative staff need to be equipped with adequate knowledge and skills on the proper use of ICT services. In this regards, policy guidance is necessary undergo continuing education and professional development programmes in order to keep up with the changing and emerging technologies.

3.8.1. Policy Statement 28

The University shall ensure that staff and students are equipped with adequate knowledge and skills in the use of ICT.

Operational Procedures

The DICT in collaboration with the Deans, Directors and Heads of Departments/Units shall create conducive environment for use of ICT among students and faculty. They shall

i. Constantly identify ICT training needs for MUHAS staff
ii. Develop and run courses on ICT to all undergraduate and postgraduate students
iii. Promote peer to peer learning through use of ICT
iv. Enhance students ability to make optimal use of ICT facilities and resources at MUHAS
v. Provide students with flexibility with regards to the learning environment
vi. Create a continuing education programme for academic and administrative staff on ICT
vii. Provide training on proper use of ICT to the surrounding community
viii. Ensure that all ICT staff undergo continuing education on ICT especially on the emerging technologies
ix. Ensure that ICT staff attends local and international ICT workshops and conferences to enhance their knowledge and skills

x. Continue to maintain MUHAS Education and Research Network membership(s) in order to exploit capacity building programmes meant to enhance optimal use of ICT among the members

xi. Ensure that all technical staff engage in self-learning and from time to time provides evidence for the same.

3.8.2. Policy Statement 29

The University shall utilize the existing partnerships and seek new partners to support life-long learning in ICT and to build the capacity of staff and students.

Operational Procedures

The University shall establish collaborations with other Government and non-Government institutions both nationally and internationally to:

i. Foster industrial linkages that will enhance skills and knowledge to both staff and students

ii. Enable sharing of e-resources available in these institutions

iii. Enhancing teaching and learning capacity through exchange programmes

3.9. ICT Research and Development

ICT research and development is a continuous process of innovation that can be applied to improve use of ICT to enhance MUHAS core functions. Research activities in ICT can also bring in funds, motivate staff and develop new knowledge, and thereby bring about credibility and recognition of the directorate of ICT as an academic unit of the University.

3.9.1. Policy Statement 30

The University shall facilitate ICT research and development activities among its stakeholders.

Operational Procedures

The DICT shall:

i. Establish an academic department for purposes of promoting research and development activities geared to enhance MUHAS core functions

ii. Encourage ICT staff to undertake research

iii. Identify areas of collaboration and develop fundable proposals with other academic staff from schools and other academic units at the University

iv. Promote research linkages with other research institutions.
v. Promote ICT research activities
vi. Promote commercialization of ICT research products and innovations

3.9.2. Policy Statement 31

The University shall promote ICT Research, Development and Innovation culture and practices for various units and programmes

Operational Procedures

The DICT shall:

i. Establish ICT Incubation programmes for enhancing development of innovative solutions for various university functions
ii. Liaise with head of schools and departments to undertake multidisciplinary research that includes application of ICT in their respective disciplines

3.10. Special need and Gender

ICT and assistive technology provide new opportunities for everyone including people with physical challenges, who make use of assistive technology for their daily activities to a higher extent than others. The national ICT policy asserts the need for individuals with physical challenges to be able to benefit on an equal basis from the rapid development of ICT, and to enable them to participate in an inclusive and barrier free information society.

On the other hand, over the years MUHAS has been implementing the national policies on gender mainstreaming which among other things advocate increased female students enrolment and observance of gender issues when recruiting staff. Furthermore, the emphasis of gender issues at MUHAS is evident through the existence and implementation of an institutional gender policy which seeks to ensure that MUHAS becomes a gender responsive area for both staff and students. It is imperative to provide direction on how ICT will foster inclusion in access of services for people with special needs and how ICT provided gender responsive services.

3.10.1. Policy statement 32

The University shall strive to ensure that ICT facilities and services are accessible to individuals

with special needs and that specialized technological resources are made available to meet and support their needs.

Operational Procedures

The DICT shall

i. strive to provide specialized ICT technologies and support needed for individual with physical challenges
ii. develop modalities to receive feedback from users of ICT that are physically challenged in order to improve their services

3.10.2. Policy statement 33

The DICT shall provide gender responsive services to both staff and students.

Operational Procedures

DICT shall continue to implement the MUHAS gender policy and anti-sexual harassment policy by ensuring:

i. Adherence to the institutional gender policy when recruiting ICT staff
ii. ICT services are provided to all staff and students of the University without any form of gender discrimination

3.11. Third Party Management

All external organisations or individuals who wish to supply products and services or to be provided with access to the MUHAS systems shall agree to follow this ICT Policy and associated procedures as part of their contractual terms. Management of third parties include issues on third party verification, Service level agreements, outsourcing, cloud computing services, equipment leasing, maintenance and support services, and lastly issues pertaining to Internet Service Providers (ISPs).

3.11.1. Policy Statement 34

The University shall establish procedures for vetting, verifying, granting of restrictive access and registering all third parties before being allowed access to any of the University's ICT resources.

Operational Procedures

The DICT shall ensure that:

i. All third-party access to the computer rooms are scheduled to occur during regular working hours. If this is not possible, a focal point person from the DICT will be scheduled after hours to accompany the third party.

ii. Third party and its agents comply with all applicable MUHAS standards, agreements, practices and policies

iii. Each third party onsite employee acquire an MUHAS ID badge that must be displayed at all times while on the premises. The badge must be returned to MUHAS upon termination or completion of a contract.

iv. Third-party agreements and contracts must specify:

   a. The work that is to be accomplished and work hours. Also, any configuration information of any installed software as well as virus checking of that software.
   b. The MUHAS information that the third party should have access to.
   c. The minimum security requirements that the third party must meet (i.e. method for remote access).
   d. How MUHAS information is to be safeguarded by the third party. Signing of a non-disclosure agreement (NDA) is typically required.
   e. Strict use of MUHAS information and information resources for the purpose of the business agreement by the third party. Any other MUHAS information acquired by the third party in the course of the contract cannot be used for the third-party's own purposes or divulged to others.
   f. Feasible methods for the destruction, disposal, or return of MUHAS information at the end of the contract.

3.11.2. Policy Statement 35

The University shall ensure that all Service contracts with service providers including third-party vendors shall include security clause concerning availability, integrity, confidentiality and integrity of data accessed on the course of serving the university.

Operational Procedures

The DICT shall:

i. Each third-party employee that has access to MUHAS sensitive information shall be cleared by signing confidentiality and non-disclosure forms for handling that information.
ii. All third-party employees are required to comply with all applicable auditing regulations and MUHAS auditing requirements, including the auditing of the third-party's work

4. POLICY STATUS

This is a revised policy. The 1st policy document was developed in 2004.

5. KEY STAKEHOLDERS

5.1. The stakeholders who were consulted during revision of this policy include the following:

i. Vice Chancellor, Deputy Vice Chancellors
ii. Deans and Directors
iii. Senate ICT Committee Members and the ICT staff
iv. Staff and Students

5.2. The main stakeholders of this policy are:

i. All MUHAS staff and students
ii. Vice Chancellor, Deputy Vice Chancellors
iii. Deans and Directors
iv. Heads of Departments and Administrative units
v. Staff and Students
vi. Visitors, and service providers/contractors

6. APPROVAL DETAILS

The policy was approved by the University Council at its 46th meeting held on 1st November, 2017.

7. RELATED LEGISLATION

i. MUHAS Institutional Repository Policy (2016)
ii. MUHAS Information and Communication Technology Policy (2004)
iii. MUHAS Research Policy (2011)
iv. MUHAS Gender Policy (2013)
v. MUHAS Human Resources Training and Development Policy (2012)
vi. MUHAS HIV/AIDS Policy (2008)
vii. MUHAS Intellectual Property Policy (2011)

viii. MUHAS Library Policy and Procedures (2013)

8. RELATED DOCUMENTS

i. MUHAS University Charter (2007)
ii. MUHAS Student bylaws (2013)
iii. MUHAS Staff Performance and Appraisal Guidelines (2009)
iv. MUHAS Cooperate Strategic Plan (2014/2015 to 2023/24
v. MUHAS ICT Strategic Plan (2015/16 – 2019/20)

9. EFFECTIVE DATE FOR THE POLICY

The policy will be effective upon such date approved by the University Council or such date stated by the University Council for the policy to become effective.

10. NEXT REVIEW DATE

The MUHAS ICT policy and procedures will be reviewed after every three years or when deemed necessary to assess the effectiveness of its implementation and determine policy areas that need to be revised. The periodic review will ensure the policy is in line with the University, national and international changes that might have taken place.

11. POLICY OWNER

The University Council shall own the MUHAS ICT Policy.

12. CONTACT PERSON

The contact person for issues related to the ICT policy and procedures shall be:

The Director, Information and Communication Technology (DICT)
Muhimbili University of Health and Allied Sciences
P.O. Box 65001
United Nations Road, Dar es Salaam, Tanzania.
Email: dict@muhas.ac.tz
Telephone: +255 22 2152271 Ext. 1032