	MOUNTAINS OF THE MOON UNIVERSITY	Document Number: MMU/ICT/002
Document Title	ICT Policy Guidelines	Effective Date: 20/10/2023
Responsible Unit	Directorate of ICT	Issue Number: 01



MOUNTAINS OF THE MOON UNIVERSITY

Information and Communication Technology Policy Guidelines

October, 2023

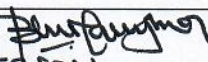
Checked by:	Approved by:  CHAIR PERSON	Date: 20-10-2023
-------------	---	---------------------

Table of Contents

CITATION	3
APPROVAL	3
Introduction	4
1. ICT Infrastructure	4
1.1 Servers and Services	4
1.2 Bandwidth	5
1.3 Network Infrastructure	5
1.4 Communication equipment	5
1.5 Power supply	5
1.6 Authorized Use	5
1.7 Data Protection	6
2. ICT Security	6
2.1 Roles and Responsibility	6
2.2 Conditions of Usage	7
2.2.1 Unacceptable Usage	7
2.2.3 Suspension and/or Termination of Access	8
2.2.4 Password Security	8
2.2.5 Computer Laboratory Facility Security	9
2.2.6 Network Control Centre/ Server Room Security	9
2.2.7 Access Control	9
2.2.8 Information Security	9
2.2.9 Hardware Security	10
3. Quality Assurance	10
4. ICT Skills Development	10
4.1 ICT Capacity Building Assessment	11
4.2 ICT Capacity building delivery methods	11
4.3 The Role of Academic Unit Responsible for ICT in Capacity Building	11
5. ICT Maintenance	11
5.1 Roles and Responsibility of The Directorate of ICT	11
5.2 Roles and Responsibility of Administrative Units and Academic Faculties	12
5.3 Roles and Responsibility of The University	12

5.4 ICT Equipment Use and Maintenance	12
6. ICT Procurement and Disposal	13
6.1 Roles and Responsibilities	13
6.2 Hardware Acquisition	13
6.3 Disposal of ICT equipment and software	14
7. Software Development and Acquisition	14
7.1 Software Development	14
7.2 Software Acquisition	15
7.3 Software Use	15
8. Website	15
9. Social Media and Email	16
9.1 Social media	16
9.2 Email	17
10. Licensing and Ownership	18
11. Bring Your Own Device (BYOD)	19
12. E-learning	20
12.1 Academic Staff	20
12.2 Technological Support for eLearning	20
12.3 Professional Development	20

[Handwritten signature]

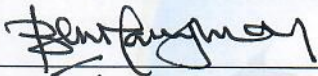
Heights for Progress

CITATION

This policy Guidelines shall be cited as the “*Mountains of the Moon University Information and Communications Technology Policy Guidelines, 2023*”

APPROVAL

Approved by the Mountains of the Moon University Council *8th meeting*



Signature

20-OCTOBER-2023

Date of Approval

ENG. DR. BEN MANYINDO
CHAIRPERSON UNIVERSITY COUNCIL

Introduction

The Information and Communication Technology (ICT) Policy Guidelines are meant to streamline the implementation of the ICT Policy. In order to access, use and benefit from available ICT resources, it is important to understand and follow the guidelines and standard Operating Procedures (SOPs). The University will continuously revise these guidelines to operationalize the ICT policy while meeting the changing trends and developments in the ICT world. These are also intended to help ensure that university staff, students and other stakeholders are able to use ICT in teaching, learning, research and community outreach activities.

The responsible unit in charge of these guidelines is the ICT Directorate, which shall be the focal point of contact for the ICT service management function within the University and shall:

- a) Provide effective ICT services and support in order to facilitate the academic, research, and administrative functions of the University.
- b) Promote effective and appropriate utilization of ICT resources
- c) Contribute towards the sustainability of the unit in order to enable the effective execution of the DICTS mandate.
- d) Promote an environmentally friendly approach to the acquisition, use, and disposal of ICT resources
- e) Coordinate and lead resource mobilization for counterpart funding for the implementation of the ICT Strategy.
- f) Specify, verify, and vet ICT standards, procedures, and best practices for all ICT deployments and operations.
- g) Have the overall ownership of the professional and technical mandate of all ICT design and developments, management, and maintenance.
- h) Operationalize and guide the ICT policy implementation

Heads of academic, administrative, in consultation with DICT will be responsible for:

- a) Integrating ICTs into their activities;
- b) Implementing the Unit specific components of the ICT Policy and Strategy;
- c) Ensuring compliance with the ICT Policy Framework; and
- d) Acting as active participants during the periodic stakeholder consultations towards supporting and facilitating the effective implementation of the ICT Policy and Strategy.

Staff, students, and the other members of the community (including Council Members) shall ensure compliance with the ICT Policies.

The following sections provides details and guidelines for implementing the policy priority areas.

1. ICT Infrastructure

The ICT infrastructure is comprised of various computing devices, systems, and network resources that support ICT services, bandwidth, and communication activities.

1.1 Servers and Services

- a) The University shall host several services locally and, in the cloud, based on approved partnerships.
- b) Access to the ICT Data Centre will be restricted and well-secured.
- c) All application software installation must not conflict with the network or system services.
- d) Whenever possible, the university will seek to integrate all services on their inception to avoid duplication.

1.2 Bandwidth

- a) The University shall strive to provide adequate bandwidth to facilitate reliable internet access and online services.
- b) All communication equipment including smartphones and laptops must be authenticated by the network Administration, whenever possible, using an Active Directory before accessing network or communication services.

1.3 Network Infrastructure

- a) The University shall operate and maintain a networking infrastructure to provide access to electronic resources
- b) The University shall develop and maintain updated structured cabling standards to ensure a uniform level of acceptable design across all units
- c) The University shall continue to invest in network infrastructure in response to anticipating growth in voice, video, data, and other network services
- d) The University will support the provision of reliable and secured near-ubiquitous Wireless Access Points across the Campuses
- e) All network equipment shall be installed, configured, and managed by Network Administrator or authorized persons under the supervision of the Director of ICT.
- f) Access to the internet and other network services must be authenticated by the centralized authentication system to limit unauthorized access to the system.

1.4 Communication equipment

- a) The University shall invest in building infrastructure to facilitate the installation of Voice-Over Internet Protocol (VoIP) and video conference facilities to improve communications and collaborations within Campus and beyond
- b) All communication equipment including smartphones and laptops must be authenticated by the network Administration before accessing network or communication services

1.5 Power supply

The University shall strive to provide a clean, reliable power supply to the Network Control Centre in order to ensure uninterrupted ICT services and access to the Internet.

1.6 Authorized Use



ICT infrastructure may only be used for authorized purposes, including conducting the University's business, academic work, or research.

Prohibited Use: The following uses of ICT infrastructure are strictly prohibited;

- a) Using ICT infrastructure to access, transmit, or store illegal, obscene, or offensive material.
- b) Using ICT infrastructure to harass, intimidate, or threaten others.
- c) Using ICT infrastructure to engage in personal business or commercial activities.
- d) Using ICT infrastructure to gain unauthorized access to other systems or networks.
- e) Using ICT infrastructure to compromise the security or integrity of other systems or networks.
- f) Using University ICT resources and emails to subscribe to personal businesses

1.7 Data Protection

Users of ICT infrastructure must take all reasonable measures to protect the confidentiality, integrity, and availability of data, including:

- a) Using strong passwords and changing them regularly.
- b) Avoiding the use of unsecured or public Wi-Fi networks.
- c) Protecting confidential information, such as personal data, financial information, or intellectual property.
- d) Using encryption where appropriate to protect data.

2. ICT Security

The purpose of these guidelines is to define approaches to ICT security in the university.

2.1 Roles and Responsibility

a) The Council Committee on Quality Assurance and ICT shall:

- (i) Undertake ownership of all cyber security risks.
- (ii) Provide leadership for the Governance of Cyber security within the University.
- (iii) Articulate the University's information on risk appetite.

b) The Directorate for ICT (DICT) 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 with the National Information Security Framework
- (iii) Maintain an updated and tested Business Continuity and Disaster Recovery Plan for all critical digital infrastructure and information assets
- (iv) Implement periodic systems and infrastructure audits based on the Plan, Do, Check, Act (PDCA) cycle
- (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 the end of staff employment contracts aligned to the Human Resource Policy
 - (xv) Secure access to all the ICT resources and enforce acceptable usage of the same by the deployment of security standards, technologies, and best practices
 - (xvi) Actively monitor availability and up-time of all core ICT resources and track conformity to SLAs.
- c) Users shall:
- a) Ensure compliance with the security policy.
 - b) Have the responsibility for portable equipment such as laptops, notepads, and mobile phones issued to them.
 - c) Pay compensation equivalent to the book value of equipment issued to them for official use in case of damage or loss.
 - d) Have the responsibility of keeping securely official data in their custody.
 - e) Take personal responsibility for loss or authorized sharing of official information, which will be regarded as negligence and shall attract disciplinary action
 - f) Report any cyber security incident to DICT

2.2 Conditions of Usage

2.2.1 Unacceptable Usage

The following activities shall be strictly prohibited, with no exceptions:

- a) Sharing of individual access passphrases.
- b) Usage of any pirated software on computing devices.
- c) Usage of any unauthorized peer-to-peer software.
- d) Any user action that contravenes the Computer Misuse Act (2011) or the Anti-pornography Act (2014).
- e) Any user action that violates the rights of any person or entity's legally registered copyright and/ or Intellectual Property
- f) Introduction of any malicious software onto any computing device or network.
- g) Any user action that disrupts the normal functioning of any computing device or network
- h) Violations of the rights of any person or company protected by Uganda's copyright, trademark, patent, or other intellectual property (IP) law and the University's Intellectual Property Policy, other relevant policies, or the University's code of conduct.

- i) Any password cracking, software spying, privilege escalation, unauthorized network port scanning and network reconnaissance, network and/or software penetration
- j) Usage of computing devices and/ or network to disrupt an external system or network.
- k) Usage of computing devices and/ or network to send out any spam.
- l) Usage of computing devices and/ or network for any gambling activity.
- m) Usage of computing devices and/ or network for any personal commercial purposes.

2.2.3 Suspension and/or Termination of Access

The following constitute the rationale for user access termination to computing resources:

- a) End of student or staff employment tenure.
- b) Request from Council, Management, Heads of Department, and/ or Human Resources Department.
- c) Occurrence of any of the unacceptable usage restrictions.

2.2.4 Password Security

- a) DICT shall implement and maintain centralized authentication, authorization, and accounting service mechanism for all network core equipment to all ICT resources.
- b) DICT shall define the password strength and lifecycle specification for all user categories from time to time
- c) All user accounts will be password protected.
- d) Password Complexity:
 - i) Passwords must be at least 8 characters long.
 - ii) Passwords must contain a combination of uppercase and lowercase letters, numbers, and special characters (e.g., @#\$%^&*).
 - iii) Staff must avoid using easily guessable information, such as personal names, birthdates, or common words.
- e) Password Protection:
 - i) Users shall not share passwords with anyone, including DICT staff.
 - ii) Passwords must not be written down or stored in an unsecured manner.
 - iii) Report any suspicious activities or suspected account compromises immediately.
- f) Password Expiration:
 - i) Passwords must be changed every 90 days.
 - ii) Systems will remember the previous 5 passwords and prevent their reuse.
- g) Account Lockout:
 - i) After five failed login attempts, user accounts will be locked out for 15 minutes to prevent brute-force attacks.
 - ii) Contact the DICT helpdesk if further assistance is required to unlock an account.
- h) Multi-Factor Authentication (MFA):
 - i) Users with escalated privileges shall use multi-factor authentication for accessing sensitive systems or data.

bm

- ii) Users must provide a second form of verification, such as a mobile phone or authentication app, along with their password.
- i) Password Recovery:
 - i) Users shall be able to recover their passwords using a secure, self-service mechanism, such as answering security questions or receiving a one-time code via email or phone.
 - ii) Passwords must be changed immediately after a password reset is performed by the DICT department or helpdesk.
- j) All default system or hardware passwords shall be changed.

2.2.5 Computer Laboratory Facility Security

Heads of Departments shall ensure that all Computer Laboratory facilities are:

- a) Compliant with 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-proof rooms.
- g) Labeled according to approved ICT nomenclature.
- h) Professionally serviced and maintained.

2.2.6 Network Control Centre/ Server Room Security

DICT shall ensure that Network Control Centre/ Server Room facilities are:

- a) Located in secure strong locations away from human or vehicle traffic.
- b) Fitted with both manual and electronic access control with CCTV monitoring and smoke detection.
- c) Protected against physical intrusion and exposure to water, dust, and fire.
- d) Protected against power fluctuations.
- e) Supported by the alternate power supply.

2.2.7 Access Control

The University 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 buildings by staff, students, visitors, and contractors.
- c) Implement CCTV for access monitoring of all buildings and entry points.
- d) Authorization: Users shall obtain prior authorization from their supervisor or other designated authority before accessing the University's ICT infrastructure remotely.
- e) Secure Connection: Remote access shall be via a secure connection, such as a virtual private network (VPN) or a secure web-based portal.

2.2.8 Information Security

- a) All sensitive, valuable, or critical data such as examination results, transcripts, and finances among others should be automatically backed up on a regular basis.
- b) It is the responsibility of the Systems Administrator to ensure that data back-ups are conducted at least once every month and that the backed-up data is kept securely on local servers, offsite venues, or on the cloud. Periodic testing of back-ups should be carried out to ensure integrity.
- c) All devices that have internet access must have antivirus software installed and updated.
- d) It is the responsibility of the Systems Administrator to ensure that antivirus software is installed and updated on all equipment with internet access.
- e) All information used within the University is to adhere to the privacy laws and the confidentiality and data privacy guidelines.
- f) Any student or employee who breaches confidentiality and privacy requirements will be subjected to disciplinary action

2.2.9 Hardware Security

- a) All hardware must be secured with appropriate access controls, including passwords, encryption, and firewalls, to protect against unauthorized access, theft, or damage.
- b) All hardware must be regularly updated with the latest security patches to prevent vulnerabilities.
- c) All hardware must be physically secured to prevent theft or damage.

3. Quality Assurance

The goal is to maintain ICT service standards, quality, and control to sustain and optimize the investment made in the ICT infrastructure. By applying these quality standards, they shall be able to resolve some issues including a lack of monitoring and evaluation system, lack of standards in hardware and software, and inadequate ICT helpdesk support.

- a) The University shall establish an ad-hoc ICT Steering Committee to support the Directorate of Quality Assurance on ICT aspects and to advise the quality of ICT services required in the University.
- b) The University shall put in place a functional and effective Quality Assurance system.
- c) The University shall strengthen the existing quality assurance and control system.
- d) The University shall put in place a monitoring and evaluation system.
- e) The University shall establish standards for hardware and software.
- f) The University shall ensure that consistent and systematic ICT facilities acquisition, maintenance, and disposal systems are established.
- g) The University shall strengthen helpdesk support.

4. ICT Skills Development

Training and skills development is imperative for the effective and successful delivery of ICT services within the University. These guidelines apply to all ICT-related capacity building that supports the various functions of the University.

4.1 ICT Capacity Building Assessment

- a) The Directorate of ICT shall coordinate the periodic assessment of existing ICT skills capacity amongst all user groups to be able to identify gaps in partnership with Heads of Administrative Departments
- b) Directorate of ICT undertakes a periodic capacity skills assessment to identify knowledge gaps within its technical staff to be able to seek appropriate capacity-building programs
- c) The Academic Department responsible for ICT, in collaboration with the Directorate of ICT, shall assess ICT skills required by students enrolled in the various programmes offered at the University.
- d) Council Committee on Quality Assurance and ICT shall undertake a periodic review of staff remuneration in comparison with the market pricing structure for similar roles and personnel.

4.2 ICT Capacity building delivery methods

- a) Directorate of ICT shall:
 - (i) Develop Capacity Building modules and courseware for identified ICT skills gaps.
 - (ii) Implement such capacity building with either internal resource personnel or with subject matter experts as per the nature of the required ICT capacity building.
 - (iii) Coordinate the identification of any external expertise for specialized training needs.
- b) The University shall ensure the presence of well-equipped ICT training computer laboratories
- c) Trainees for such capacity-building programs will be identified by the user departments in partnership with Heads of Departments.

4.3 The Role of Academic Unit Responsible for ICT in Capacity Building

The Department responsible for ICT training shall:

- (i) Work with Academic Registrar's Office to assess all programmes offered to ensure they have adequate ICT skill courses included.
- (ii) Develop required ICT skill courses in collaboration with relevant Units to be delivered as part of the curricula for programmes offered at the University.

5. ICT Maintenance

The purpose of these guidelines is to define and implement approaches to hardware maintenance and software maintenance for ICT devices.

5.1 Roles and Responsibility of The Directorate of ICT

- a) From time to time define and disseminate updated ICT equipment maintenance guidelines to all Units and Colleges
- b) Act as the central point of contact for all ICT equipment maintenance
- c) Provide technical support in the development and implementation of service and maintenance schedules for all ICT equipment

- d) Undertake a periodic assessment in all Units and Colleges to ensure compliance with the set maintenance guidelines

5.2 Roles and Responsibility of Administrative Units and Academic Faculties

All Units and faculties within the shall:

- a) Maintain records of all ICT equipment they acquire including records of manufacturer equipment warranty
- b) Liaise with the DICT in developing service and maintenance schedules on an annual basis for all ICT equipment
- c) Maintain good documentation describing the service and maintenance history for all ICT equipment
- d) Ensure all ICT equipment is placed within adequate operating environments
- e) Ensure all replacements or upgrades of any ICT equipment are undertaken with clearance from the DICT

5.3 Roles and Responsibility of The University

The University shall:

- a) Develop procedures for procurement, upgrading, replacement, and disposal of old and obsolete ICT equipment.
- b) Develop and operationalize procedures and conditions for acceptance of donated ICT equipment.
- c) Vet all used ICT equipment donated to the University before it is accepted for use.
- d) Put in place a maintenance program to ensure that the hardware is serviced and repaired regularly, once quarterly preferably.
- e) Put in place a maintenance program to ensure that the hardware is replaced in three years.
- f) Establish a revolving fund contributed by user departments to offset maintenance and replacement costs.

5.4 ICT Equipment Use and Maintenance

- a) All hardware must be used following the University's Acceptable Use Policy (AUP) and should not be used for any unlawful purposes.
- b) All hardware must be registered with the University's IT department/Stores and regularly maintained to ensure that they are functioning properly.
- c) Only authorized personnel should be allowed to install software or make changes to hardware configurations.
- d) All hardware must comply with applicable laws, regulations, and standards, including data protection and privacy laws, and the University's ICT security policies.
- e) Regular audits of hardware and software configurations must be conducted to ensure compliance with relevant regulations.
- f) All personnel who use or manage hardware must be provided with regular training and awareness sessions to ensure they are aware of the risks associated with hardware and how to mitigate them.
- g) Training and awareness sessions must also include guidelines on how to report any hardware-related incidents or vulnerabilities to the IT department.

- h) ICT equipment can be repaired in-house by a trained maintenance engineer or by a third party procured following PPDA guidelines.

6. ICT Procurement and Disposal

Procurement of all ICT equipment and services shall conform with the overall procurement of goods and services standard as aligned to the Public Procurement and Disposal of Public Assets Act (PPDA).

6.1 Roles and Responsibilities

The following roles and responsibilities shall govern the procurement of ICT equipment, software, and services within the University.

- a) Procurement and Disposal Unit
 - (i) Manage all procurement or disposal activities within the Universities in line with the PPDA (Sections 31 & 32)
 - b) User Departments
 - (i) Ensure conformity with the Procurement Policy as implemented by the Procurement and Disposal Unit
 - (ii) Ensure conformity with approved technical guidelines and standards by DICT in the procurement of any ICT equipment, software, or service
 - (iii) Will at each annual budgeting cycle plan for its specific ICT requirements for proper provisioning in a rationalized manner.
 - c) Directorate of ICT
- The Directorate of ICT shall provide technical support to all user departments as provided below:
- (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 the 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) Provide support for bulk procurement of commonly used ICT equipment and software as per business need.

6.2 Hardware Acquisition

- a) All hardware purchases must be approved by the University's IT department to ensure compatibility with existing infrastructure, security standards, and interoperability with software standards.
- b) Only authorized personnel should be allowed to purchase hardware on behalf of the University.

- c) When purchasing hardware, consideration should be given to the Total Cost of Ownership (TCO) which includes the purchase price, maintenance costs, and potential upgrade costs.

6.3 Disposal of ICT equipment and software

- a) All hardware must be disposed off in accordance with the University's environmental policies and regulations.
- b) All data on the hardware must be securely erased to prevent unauthorized access to sensitive information.
- c) All hardware that is that cannot be disposed off should be recycled or donated if possible.
- d) The university shall define the life cycle for each category of procured ICT equipment to determine the replacement cycle.
- e) Disposal of retired ICT equipment shall comply with the PPDA.
- f) Software disposal will rely on the system support cycle of the software developer company.
- g) All software must be disposed of in accordance with the University's environmental policies and regulations.
- h) All data associated with the software must be securely erased to prevent unauthorized access to sensitive information.
- i) All software licenses must be returned to the software vendor when they are no longer needed.

7. Software Development and Acquisition

The purpose of these guidelines is to define and implement approaches to software development and procurement that enhance efficiency, information security, value of university resources, and rationalization of ICT. These policies and procedures apply to all software used to support University functions and to all software developed in-house (within the University) or off-the-shelf.

7.1 Software Development

- a) DICT, shall periodically define the Systems Life Cycle methodology for:
 - (i) systems and software engineering for both in-house and outsourced development
 - (ii) acquisition of off the shelf software
 - (iii) maintenance of software
- b) All software shall 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
- c) All software under this policy shall comply to the Software Licensing and Ownership and Cyber Security Policies

- d) All acquired software shall where necessary, contain provision for technical support and upgrades
- e) All Faculties, Departments and units shall where necessary, make use of open-source software based on a risk-based assessment as referenced in the cyber security policy
- f) All Faculties, Departments, and Units undertaking the development or acquisition of any software shall ensure compliance to this policy and plan for end user training
- g) This policy does not apply to software development within Faculties for academic or educational purposes
- h) Whenever possible, all software should be integrated (or at the minimum integrable) with all existing software
- i) DICT has direct responsibility for maintaining and guiding the implementation.

7.2 Software Acquisition

- a) All software purchases must be approved by the University's ICT Directorate to ensure compatibility with existing infrastructure, security standards and interoperability with hardware standards.
- b) Only authorized personnel should be allowed to purchase software on behalf of the University.
- c) When purchasing software, consideration should be given to the Total Cost of Ownership (TCO) which includes the purchase price, maintenance costs, and potential upgrade costs.

7.3 Software Use

- a) All software must be used in accordance with the University's Acceptable Use Policy (AUP) and should not be used for any unlawful purposes.
- b) Only authorized personnel should be allowed to install software or make changes to software configurations.
- c) All software must be registered with the University's IT department and regularly maintained to ensure that they are functioning properly.
- d) Use of pirated or unauthorized software is strictly prohibited.
- e) All software must comply with applicable laws, regulations, and standards, including data protection and privacy laws, and the University's IT security policies.
- f) Regular audits of software and licenses must be conducted to ensure compliance with relevant regulations.
- g) All personnel who use or manage software must be provided with regular training and awareness sessions to ensure they are aware of the risks associated with software and how to mitigate them.
- h) Training and awareness sessions must also include guidelines on how to report any software-related incidents or vulnerabilities to the ICT Directorate.

8. Website

The University shall provide web services for purpose of disseminating information. This shall be achieved through the use of the University web pages and intranet services all under the

University's main domain name structure. The guidelines provide guidance on Maintenance, Content Management and Domain Naming of the web pages and content ownership.

9.3 Website Policy Statements

- a) The University shall ensure that the information and materials on the website are standardized, controlled, and secured according to the requirements of the management.
- b) The University shall appoint website administrators to manage the website and Faculty/Institute/Directorate/Unit web pages.
- c) The University shall provide procedures, guidelines, and specifications for preparing information to be uploaded.
- d) The University shall provide procedures, guidelines, and specifications on the type of publications allowed to be uploaded to the website.
- e) Contents of the MMU website shall be determined by respective user departments/units but will be governed by the regulations and instructions given by university from time to time.
- f) The domain naming of the MMU will be mmu.ac.ug in conformity with national and international guidelines. Subdomains may be added as the need arises for such.
- g) The ICT department will monitor the website's performance, uptime, and responsiveness.
- h) The ICT department shall ensure the Security and Privacy of the website and its users.
- i) The ICT department shall be responsible for managing the technical infrastructure supporting the university's website.
- j) The Marketing and PR department shall work closely with the website administrators to ensure that the website policy aligns with the university's branding guidelines and overall messaging strategy.
- k) The Marketing and PR department shall define the content strategy for the website.

9. Social Media and Email

The University is using various social media including WhatsApp, Facebook, Twitter, YouTube, LinkedIn and blogs in supporting the teaching and learning process. The following guidelines will help provide guidance on the use of the different social media sites.

9.1 Social media

- a) The University shall identify potential social media to be used as official social media sites.
- b) Only the official social media sites will be allowed to make use of trademarks and symbols
- c) The University shall create officially recognized pages that represent the Faculty, Department, Program, or Unit of the University.
- d) The University shall provide procedures, guidelines, and specifications on the staff's responsibility and the type of information to be posted on social media.
- e) The University shall authorize Faculty/Department/Units/Staff to post and respond to issues on the University's Social Media page based on the guidelines.
- f) Only authorized personnel shall be allowed to make postings on the official social media sites

- g) Any information shared across the social media sites shall comply to fair use and comply to the policies in the domains of Conflict of interest and trademark and symbol protection
- h) All information shared across social media sites should not make reference to any biased statements on matters such as politics, religion, race, gender, sexual orientation, inter alia; statements that contain obscenities or vulgarities
- i) All staff social media activity shall:
 - i. Respect the Laws relating to copyright and other intellectual property rights, defamation, privacy, and other applicable laws
 - ii. Not portray colleagues in an unfavorable light in respect of matters including, but not restricted to, religion, gender, sexual preference, race, nationality or disability
 - iii. Maintain adherence to the overall Confidentiality agreements and information disclosure
 - iv. Not make reference to any sensitive staff or student information.

9.2 Email

- a) Email Account Creation:
 - i) All Staff and Students shall be provided with a University email account for official communication purposes.
 - ii) Email account creation requests must be submitted through the designated process, such as an email to the IT department.
 - iii) The account creation request must include the following information:
 - 1. Full name of the employee
 - 2. Department
 - 3. Contact information (Mobile Number & Alternative email address)
- b) Email Address Format:
 - i) The email address for each staff member will follow the format: first.lastname@mmu.ac.ug
 - ii) The email address for each student will follow the format: first.lastname@student.mmu.ac.ug
 - iii) In cases where there are multiple staff members or students with the same first and last name, additional unique identifiers (e.g., middle initial or Staff/Student ID/Regno.) may be included to ensure email address uniqueness.
- c) Display Name:
 - i) The display name in the email account will be set as the Staff Member's full name (e.g., "Agaba Derrick").
 - ii) Staff Members should use their official full name as the display name to maintain professionalism and clarity in communication.
- d) Use of University Email:
 - i) The University email account should be used exclusively for official business purposes.
 - ii) Staff should refrain from using their company email account for personal communication, except where necessary and following company policies.

- a) Email Signature:
 - i) Staff Members are encouraged to include a standard email signature in their outgoing emails.
 - ii) The email signature should include the Staff Member's full name, job title, department, location of office, and any other relevant details as guided by the University's branding manual.
- f) Email Account Security:
 - i) Staff Members are responsible for safeguarding their email account login credentials.
 - ii) Staff Members adhere to the company's password policy (e.g., regular password changes, and password complexity requirements).
 - iii) Staff Members should log out of their email accounts when accessing them on shared or public devices.
- g) Email Retention and Archiving: The university may implement email retention and archiving policies in compliance with legal and regulatory requirements.
- g) Staff should be aware that their email communications may be subject to monitoring or retention as per company policies and applicable laws.
- h) Email Etiquette and Professionalism:
 - i) Staff are expected to maintain professionalism and adhere to email etiquette guidelines when communicating via the company email account.
 - ii) Use clear and concise language, appropriate grammar, and a professional tone in all email communications.
 - iii) Exercise caution when sending emails and avoid sharing sensitive or confidential information unless necessary and authorized.
- i) Email Usage Monitoring:
 - i) The University reserves the right to monitor and review employee email communications for security, compliance, and legitimate business purposes.
 - ii) Monitoring activities may include but are not limited to checking email content, attachments, and recipient lists.

10. Licensing and Ownership

The software licensing and ownership within Mountains of the Moon shall be guided by the following:

- a) All heads of units shall ensure that:
 - (i) An inventory of all software is maintained
 - (ii) All software is licensed to the responsible unit as aligned to purchase agreements.
 - (iii) All software in usage is properly managed, administered, and maintained.
 - (iv) All software in usage is approved and aligned to the information security policies.
- b) Any computing equipment that is written off, sold or given to a third party shall have all non-transferable licensed software permanently removed.

- c) Staff and students shall not be given the ability to download and install software on equipment.
- d) Software shall only be used in accordance with its license and duration.
- e) Software shall only be distributed in accordance with its license agreement.
- f) Software licensed for official purposes must not be used on personal computing devices.
- g) All software source code developed with either internal or external resources for purposes shall be owned by the and shall be handed over to DICT for good custody, backup, and patenting.
- h) All Units outsourcing software development that has source code restrictions shall ensure the usage of appropriate third-party source code escrow agents to ensure continuity

11. Bring Your Own Device (BYOD)

These procedures will provide guidance on the personal devices, such as smartphones, tablets, laptops, and other electronic devices to access the University network.

- a) The University will encourage the use of such devices by increasing the WiFi coverage around the University.
- b) The University will come up with initiatives to support and encourage students and staff in acquiring personal computing devices to facilitate their work.
- c) This policy applies to all students and staff who use personal devices on the network.
- d) Only personal devices, such as laptops, tablets, smartphones, and other approved electronic devices, which are authorized and compliant with policies, are allowed to be used on the Network.
- e) Personal devices must adhere to the University's network security requirements, including but not limited to using approved antivirus software, keeping the operating system and applications up-to-date with the latest security patches, and complying with network authentication protocols.
- f) Users are responsible for safeguarding their personal devices and protecting sensitive data.
- g) All devices must be password-protected, and users must not share their login credentials with others. Lost or stolen devices must be reported to the University's ICT Directorate immediately.
- h) Activities that violate the University's policies, including but not limited to unauthorized access to systems, sharing copyrighted material, and engaging in illegal activities, are strictly prohibited.
- i) The University shall have the right to investigate/ audit such devices in case of any malicious activity, cybercrime, or fraud that affects the University.
- j) Technical support for personal devices used under the BYOD policy may be limited to basic connectivity and network access. The ICT Directorate may not provide support for hardware repairs, software installation, or troubleshooting of personal devices.
- k) Users must comply with all applicable laws, regulations, and policies while using personal devices. Non-compliance may result in revocation of network access.
- l) The University is not responsible for any damage or loss of personal devices used under the BYOD policy. Users are solely responsible for any liability arising from their use of personal devices on the network.

12. E-learning

The University through Directorate of ICT Services shall ensure deployment and maintenance of appropriate infrastructure to enable reliable and effective access to online courseware and e-resources. The following procedures will guide the implementation of e-learning in the university

12.1 Academic Staff

- a) All programmes/course units should have online learning materials on the Learning Management System (LMS)
- b) Course leaders and academic staff should establish online presence with electronic material content on the e-learning platform
- c) The appraisal of the academic staff will also consider efforts made by the lecturer towards developing and delivering online course material.
- d) The University shall use e-learning to support both learners on ODeL and on campus delivered programmes.
- e) The distribution of the gadgets like laptops will first consider the lecturers who have developed and the ones using LMS.
- f) Lecturers will be enrolled in the course units they are teaching.
- g) Lecturers will not be allowed to access the course units which they are not teaching unless when they are Head of Departments and Faculty Deans for supervision purposes.
- h) Lecturers should keep monitoring and evaluating the quality of eLearning resources and tools regularly to ensure that they meet the required standards accepted by the University.

12.2 Technological Support for eLearning

- a) The University shall continuously equip academic units with appropriate educational technologies for delivering e-learning.
- b) DICT shall ensure that there is adequate bandwidth to support e-learning.
- c) DICT shall be in charge of all educational technologies and tools and shall ensure that they are up-to-date and in good and sound working conditions.
- d) Technical Infrastructure: The University will invest in robust and reliable technical infrastructure to support the e-learning initiatives. This includes ensuring access to adequate hardware, software, internet connectivity, and ICT support to ensure seamless e-learning experiences for learners and lecturers.
- e) DICT shall define and implement access guidelines and procedures to the e-learning content management platform for different categories of users including those with special needs.
- f) DICT and ODeL will provide training and support to teaching staff and students on the use of eLearning resources and tools.
- g) DICT will ensure that the LMS accounts are created for the people who are authorized to have access to the LMS platform and their login credentials will be given to them to enable them access the platform

12.3 Professional Development

There will be continuous professional development for teaching staff to effectively deliver e-learning. Regular training and support will be provided to the teaching staff to develop their e-learning skills and competencies, and for them to stay updated with the latest e-learning trends and best practices.

[Handwritten signature]

