# Mbarara University of Science and Technology

# Information & Communication Technology Policy

# Table of Contents

## List of Abbreviations and Acronyms

| | |
|---|---|
| ADB-HEST: | African Development Bank- Higher Education for Sciene and Technology |
| e-Government: | Electronic Government |
| e-Learning: | Electronic Learning |
| e-mail: | Electronic Mail |
| DHCP: | Dynamic Host Configuration Protocol |
| DNS: | Domain Name Services |
| ICT: | Information and Communications Technology |
| IP: | Internet Protocol |
| MUST: | Mbarara University of Science and Technology |
| NITA-U: | National Information Technology Authority- Uganda |
| PPDA: | Public Procurement and Disposal of Assets Authority |
| RENU: | Research and Education Network for Uganda |

## Definitions of Terms

**Academic Unit:** Faculty, Institute and other unit within the university to which ungraduated, graduate and research students are admitted.

**Administrative Unit:** Department/unit involved in performing administrative functions of the university.

**Application:** Program or set of programs that allow a user to perform a particular task

**Back up:** Copy of computer data or information taken for storage in case of loss of the original data or information.

**Bandwidth:** Measure of how much data can be transmitted over a specific connection at a specific time

**Business Requirements:** Critical activities of an organization that must be done in order to meet the objectives of the university

**Business Continuity:** Ability to ensure that the university's operations and core business functions are not severely affected by a disaster of unplanned incident.

**Cloud Computing:** Practice of using remote servers hosted on the internet to store, manage and process data, rather than a local server physical hosted within the university premises

**Disaster Recovery:** Ability for the university to maintain or quickly resume mission-critical functions following a disaster

**Hardware:** Physical, tangible components of computer systems.

**Incident:** An unplanned interruption to a university's IT service or reduction in the quality of the service.

**Local Area Network:** Computer network linking all computing devices within all buildings of a specific campus of the university.

**Network Backbone:** Network that provides connectivity to various buildings and LANs of the university.

**Physical Security:** Protection of the university's hardware, software, networks and data from physical actions and events that could cause serious damage or loss.

**Propriety Software:** Non-free software for which the software's publisher or developer retains ownership and places restrictions on its use and source code.

**Social Media:** Applications that enable users to create and share electronic content or to participate in social networking

**Software:** Set of instructions, data or programs used to operate computers and execute specific tasks.

**Special Needs:** particular requirements at the university for staff and students with learning, emotional or behavioral difficulties and physical disability

**Staff:** A person appointed by the university, as an employee, as defined in the Human Resource Manual of the university.

**Student:** A person admitted and registered by the Academic Registrar's office to undertake a specific academic program for a period of time.

**University:** Mbarara University of Science and Technology

**User:** Person who utilizes the university's computing or network services.

**Virus:** Computer program that has a detrimental effect, such as corrupting the system or destroying the data

**Web Services:** Standardized way or medium to propagate communicate between the client and server applications on the World wide web.

# Foreword

Mbarara University of Science and Technology (MUST) is committed at ensuring that Information and Communications Technologies (ICT) are continuously implemented for the better operation of the university. This is in line with the university's wider strategic plan.

It is important to note that ICT implementation requires guidance and direction within the existing local, national and international legal and regulatory frameworks. Implementing ICT by use of proven best practices makes it even easier to benefit from this continued effort.

This ICT policy shall ensure structural direction to guide the university in its quest to achieve its vision and mission statements. Clear and defined practices, roles and responsibilities provide a very important foundation for the university to achieve the benefits expected from the investment in ICT.

Mbarara University of Science and Technology's staff, students and stakeholders have an obligation to comply to this policy.

…………………………………………………………….

Vice Chancellor

Mbarara University of Science and Technology

# Preamble

Mbarara University of Science and Technology continues to provide its staff, students and stakeholders, a number of computing devices and services in light of the overall goal of streamlining effective and efficient work processes at the University.

This is in line with the university's vision to be a Centre of academic and professional excellence in Science and Technology. Appropriate and planned use and adoption of ICTs is key in enabling the university to achieve this vision by ensuring managed use of the available ICT resources and also planning for resources that might not readily be available.

This policy is a guide on how the university shall operationalize and ensure the responsible and optimum use of its ICT capacity to ensure operational excellence in consideration of consistent, fair and controlled use and adoption of ICT technologies.

The policy shall be implemented to serve the university staff, students and visitors through the existing university governance structure with MUST Computing Services as the key functional and technical unit of the university.

# 1.0 Introduction

ICT is seen as a universal enabler to functional aspects of any organization. Mbarara University of Science and Technology is committed to applying ICT in its core functional areas of teaching, learning, research, community outreach and administration.

The world continues to experience rapid advancements in ICT and its usage. People, at individual and organizational levels, continue to get even more exposed to technology. The widespread use of personal computers, the increased access to the internet/World Wide Web and the increase in wireless/ mobile communications have changed the way individuals and organizations operate.

In the world today, ICT can also be taken advantage of to achieve organizational operational excellence by increasing/improving production, efficiency and communications. It is also true that ICT has provided varied opportunities for abuse and has severally been reported as an aid to unauthorized access and use of privileged data/information and infrastructure. It is therefore prudent that the use of ICT is regulated.

The policy strives to ensure the managed use of ICT at Mbarara University of Science of Technology by covering the following broad areas.

i. ICT Governance
ii. University ICT Network Access
iii. Software Management
iv. IT Services Support
v. IT Infrastructure Management
vi. Data and Information Security
vii. ICT Procurement and Disposal
viii. Social Media
ix. Special Needs ICT use
x. ICT Skills Capacity Building

## 2.0 Policy context and Problem statement

The proliferation of ICT devices and services has made ICT technologies a very critical factor in the business processes of all organizations. Organizations spend a lot of their resources on implementing and improving their ICT infrastructural capacity to enable them achieve their primary aims and objectives. Other than organizations, private individuals also have abundant access to these technologies. This increased adoption to ICTs also provides avenues for inappropriate use and abuse of the available technologies.

Mbarara University of Science and Technology seeks to streamline and standardize the use of its ICT resources to limit abuse, unfairness and unnecessary wastage while aiming at ensuring operational efficiency and effectiveness.

## 3.0 Policy statement and justification

According to the Government of Uganda Vision 2040, the internet, information security, e-Government and the use of ICTs in Education are amongst a number of policy areas aimed at impacting growth by providing a catalytic role to other sectors.

ICT has become a central focus for most Institutions of Higher Learning. Most operations are currently facilitated by ICT. These areas include; managing academic business such as registration of students, handling of marks and making of transcripts and certificates. E-learning is also central as an instructional learning tool. Most operations in Uganda and the world at large have become digitalized. This digital revolution is necessary for adoption at all Institutions of Higher Learning.

It is in the same vein that Mbarara University of Science and Technology intends to incorporate ICT as a critical policy area.

## 4.0 Policy goal

To ensure regulated, managed and controlled use of ICT at Mbarara University of Science and Technology it its quest to become a center of academic and professional excellence in Science and Technology.

## 5.0 Objectives of the policy

a) To ensure that ICT is effectively applied as a universal enabler to the university's core functions of teaching, research, community outreach and administration.

b) To guarantee the responsible use of the university's ICT infrastructure

c) To protect and preserve the university's ICT data, information and infrastructure.

d) To ensure the availability, security and privacy of MUST's system and network infrastructure

e) To promote MUST's online visibility and the use of electronic communications

## 6.0 Legal Framework

The policy is in compliance with the following;

- The National ICT Policy (2014)
- The National Information Technology Act (2009)
- The National e-Government Policy Framework (2011)
- The National E-Waste Management Policy (2012)
- The Computer Misuse Act (2011)
- The Anti-Pornography Act (2014)
- The Electronic Signatures Act (2011)
- The Copyright and Neighboring Rights Act (2006)
- The PPDA Act, 2003
- The National Development Plan; Uganda Vision 2040
- The Universities and Other Tertiary Institutions Act, 2001
- Mbarara University of Science and Technology Manual Human Resource Manual, 2018

# 7.0 Policy Strategies

## 7.1 POLICY STRATEGY 1: ICT Governance

**POLICY OBJECTIVE: Establish a regulated and well enabled ICT governance framework and environment to ensure that the university benefits from ICT.**

### 7.1.1 The University ICT Committee

The University ICT Committee shall have its representation as determined by the University management, and shall be mandated to;

a) Oversee the development and implementation of ICT related policies for the university
b) Have an oversight on security of all ICT assets, facilities and logistical requirements.
c) Advocate for appropriate budgetary allocation of the University total budget to ICT related activities and initiatives.
d) Approve, monitor and review ICT implementation developmental projects for the university
e) Approve, monitor and review annual ICT budgets and work plans for the university

### 7.1.2 The University Computing Services

The MUST Computing Services shall provide the ICT management function of the university, and shall be mandated to;

a) Provide technical and professional leadership to ICT implementations and developments in the university
b) Operationalize the ICT policy implementation
c) Ensure optimized utilization of ICT resources in the university
d) Ensure legally and environmentally acceptable acquisition, use and disposal of ICT resources

### 7.1.3 Academic and Administrative Units

Heads of Academic and Administrative units shall in consultation with MUST Computing Services;

a) Ensure integration of ICTs into their activities
b) Comply to ICT policy framework

### 7.1.4 Staff and Students

The staff and students of the university shall comply to the ICT policy regulatory framework.

## 7.2 POLICY STRATEGY 2: University ICT Network Access

**POLICY OBJECTIVE: Establish a robust and scalable network backbone infrastructure to ensure final delivery of ICT services to staff and students.**

### 7.2.1 The University Network Backbone

a) The University shall maintain a stable and resilient physical network backbone strategically running across different geographical areas of all campuses of the university.
b) This shall act as the primary distribution channel for access of information or ICT related services to staff and students and different campuses of the university by connecting all authorized access points and areas in the university
c) As per strategy, the backbone shall be continuously reviewed to meet changes in computing needs, growth in demand and technological advances.

### 7.2.2 The University Data Center and related services

a) The university shall run a Main Data Center to act as the central physical repository facility to host university ICT network services.
b) The main data center shall be the physical nerve center of the university network backbone
c) The university shall also run data replication and auxiliary data centers/ server rooms to provide support to the main data center
d) All Domain Name Services (DNS) and Dynamic Host Configuration Protocol (DHCP) activities shall be centrally managed.
e) The university shall own its own Internet Protocol (IP) number space relevant to academics and research.

### 7.2.3 The University Local Area Network

a) For each of the university's campuses, a Local Area Network shall exist to connect all buildings on that campus.
b) All components of the Local Area Network shall connect to the University Network Backbone

### 7.2.4 The University Wireless Network Services

a) The university shall provide wireless network connectivity services for both staff and students at all its campuses
b) Only approved Wireless Access Points shall be allowed to transmit wireless signals.

### 7.2.5 The University Wide Area Network

All Local Area Networks of all campuses of the university shall be inter-connected into one virtual university network to be centrally managed at the university main campus.

## 7.3 POLICY STRATEGY 3: Software Management

POLICY OBJECTIVE: To ensure that Software acquired suitably meets the operational needs of the university

### 7.3.1 Business Requirements

a) The software development and /or Acquisition process shall begin with documented business requirements, justified by a stated business case by a Unit.
b) MUST Computing Services shall, in compliance with the university's procurement regulations, define Systems Acquisition methodology for the following categories of software;
   i. In-House development of software
   ii. Outsourced development of software
   iii. Off-the-Shelf software

### 7.3.2 Software Requirements Specification (SRS)

The SRS shall be derived from the business requirements and Risk analysis and shall define the software requirements of the systems.

### 7.3.3 System Design

The system design phase shall include the construction of High-level design documents such as flowcharts, schematics, architecture diagrams and interface descriptions. It May also include hardware or software prototypes.

The design shall follow the UML (Unified Modeling Language) artifacts which should include use of Case diagrams, activity diagrams, deployment diagrams and extent possible state diagrams.

### 7.3.4 Risk Analysis

Risk analysis shall identify the system hazards and methods of control. A preliminary risk analysis shall be created at this stage of the development process and updated as the system design evolves. The risk analyst shall define the risk mitigation strategy.

### 7.3.5 Design Review

A design review shall be held to review the Customer Requirements, Software Requirements Specification and (preliminary) Risk analysis. A design review may be held prior to, or during the implementation phase.

### 7.3.6 Quality Assurance

MUST Computing Services shall develop Software Quality Assurance Plan, verification and Validation Plan and also be responsible for at least the system level testing.

### 7.3.7 Implementation

In the implementation phase, the software shall be developed to meet the design objectives.

### 7.3.8 Testing

Testing shall be driven by a verification and validation plan and shall consist of unit (Module) testing, integration, system testing and user acceptance testing. Before starting the system test, the users / MUST Computing Services shall check that the right test environment and the test equipment are available.

### 7.3.9 Training

Software developers shall produce written guidance and training materials for all produced Software.

### 7.3.10 Deployment

The system shall be released after all tests are successfully completed. All documents (except test reports) ad software shall be placed under version control (if not already done). Test reports shall be kept in a Design History File that is organized by the release versions. Software deployment shall follow the Information Technology Infrastructure Library (ITIL) release, change and configuration processes as customized and implemented in the MUST environment

### 7.3.11 Systems Development and Maintenance

For all business application systems, system designers and developers must incorporate security mechanisms from the beginning of the systems design process through conversion to a production system.

### 7.3.12 Software Support

Owners of application must ensure that they have the required hardware necessary to host the required application. The MUST Computing Services should ensure that clients can effectively operate the software and to provide help for clients who have questions or problems with the software.

### 7.3.13 Propriety Software Procurement and Acquisition

a) University software must be procured in accordance with the University’s Procurement and Disposal regulations. This shall begin with documented business requirements justified by a stated business case by a Unit with the approval of the MUST Computing Services.

b) The MUST Computing Services will maintain an inventory of all University software including licenses, installations, licensing keys, copies of agreements, media and permitted uses.

c) All software shall be licensed and aligned according to purchase agreements or contracts

### 7.3.14 Software Installations

Software must only be installed on University computers or networks if there are the appropriate licenses and if its use is in accordance with its licensing rules.

End users are prohibited from installing software on University computers and requests for installation must be placed through the MUST Computing Services.

### 7.3.15 Permitted use of University software

All university software shall be exclusively used for academic, research, innovations or for purposes of the University's business and administration and shall be installed on university computers only.

### 7.3.16 Versions of Software

Only the current version of a software application and its immediate predecessor will be implemented and supported by the MUST Computing Services.

### 7.3.17 Disposal of Software

University software licenses must not be given away or sold for use outside the University. All software on University computers being disposed of must be securely destroyed or uninstalled. The media and licensing keys for software which is being permanently withdrawn from use must be destroyed.

### 7.3.18 Departing staff and students

Staff and students who leave the University and who have had University software installed on computers owned by them must remove all such software immediately. System Access Accounts shall similarly be suspended.

### 7.3.19 Copyrighted, Licensed or other Intellectual Property (IP)

While performing services for Mbarara University of Science and Technology, all programs and documentation generated by, or provided by staff/students and other services Providers for the benefit of Mbarara University of Science and Technology are the property of Mbarara University of Science and Technology. Mbarara University of Science and Technology asserts the Legal ownership of the contents of all information systems under its control. The ICT policy takes into considerations of the IP policy already in place.

## 7.4 POLICY STRATEGY 4: IT Services Support

**POLICY OBJECTIVE: Providing integrated ICT services to support all the university's business processes.**

### 7.4.1 IT Infrastructure Support

Computer hardware and all related peripherals shall be maintained in good working condition.

The MUST Computing Services shall develop and maintain Periodic (Daily, Weekly, Monthly, and Quarterly, Yearly) Maintenance Manuals for both the Computer Hardware and all related peripherals which shall be approved by the University ICT Committee and eventually University Management.

### 7.4.2 Web Services

MUST shall provide web services for purpose of disseminating information within the university and to the internet. This shall be achieved through the use of the university web page and intranet services all under the university's main domain name structure.

i. All official MUST web pages shall bear the distinct identity and symbolism of MUST
ii. MUST Computing Services shall manage and control all existing web services/pages under the university's domain name
iii. Only authorized personnel by the university shall be allowed to upload content to official university web pages in line with the university's communication policy.

### 7.4.3 Business Application Support

MUST shall provide Business Applications that will facilitate Teaching, Research and Administration operations.

MUST shall give special attention to use of Open Source Software. In the event of the unavailability of Open Source Software, MUST shall ensure purchase of Software or Business Applications from vendors.
MUST Computing Services shall ensure Business Applications are maintained at the most recent version to support any changes in business processes at MUST.

### 7.4.4 Electronic Mail Services

MUST Computing Services shall provide each member of staff and student with an e-mail address under the official university domain name structure.

a) Members of staff shall be recommended by the University Secretary's office before obtaining an official email account.

b) Students shall be recommended by the Academic Registrar’s office before obtaining an official email account.

The Electronic Mail service shall comprise a web interface, providing facilities for creating, addressing, sending, receiving and forwarding messages both within and outside the university network.

Account usernames and addresses will be assigned to users as appropriate.

Email distribution lists shall be created and used for purposes related to teaching, course-work, research and administration at MUST. Commercial use of mailing lists, except for authorized University business will be prohibited.

Non -acceptable Emails content NOT to be shared on email distributions shall be stipulated in the university’s communication policy.

No e-mail account, created under the university’s domain, should ever be deleted, but rather suspended if the need arises.

If a staff member’s ceases to be an employee of the university, the University Secretary shall officially inform the MUST Computing Services to suspend the e-mail account within a period of one month.

Students might be allowed to retain their MUST email accounts, as a means of retaining alumni contact, but shall NOT be accessible to information intended for active students.

### 7.4.5 E-learning Services

The university shall ensure the maintenance of appropriate infrastructure to enable reliable and effective access to online courseware and other web resources ubiquitously.

The university shall develop an appropriate Managed Learning Environment which will ensure that students and teachers are presented with an effective and authoritative system for learning and teaching. This system has to be developed in line with the proven pedagogical instructional design concepts selected by MUST. The system should also be Open Source to allow easy sustainability.

The university shall willfully supply, maintain and support appropriate and sufficient physical infrastructure (i.e. classroom, computer laboratories and learning spaces) to support access to e-learning which meet staff and student needs and expectations.

MUST shall provide central support for e-learning through staff training and development, e-learning coordination under MUST Computing Services and the establishment of a digital library by strengthening and supporting their resources and function.

The university shall make available adequate time to academic staff and recognize the staff workload associated with e-learning developments and online teaching. The university shall ensure that adequate recognition is given to academic staff for e-learning development work through the promotion process and other forms of reward such as financial incentives for content developers.

### 7.4.6 Cloud Computing

Hosting services or tasks for which the capacity is insufficient shall be outsourced.

Cloud Computing must only be implemented after approval of the MUST ICT Committee and eventually University Management.

### 7.4.7 Trouble Shooting

IT Service disruptions shall be managed in such a manner to restore operations to normal within agreed service levels and business priorities.

## 7.5 POLICY STRATEGY 5: Infrastructure Management

POLICY OBJECTIVE: Providing ICT Infrastructure that will facilitate teaching, research and administration

### 7.5.1 Acquisition of Computing Equipment

Every Unit must generate a Computing Equipment Procurement plan which **MUST be** generated for each Financial Year

The MUST Computing Services shall develop and maintain up-to-date specifications of the ICT Equipment.

All requisition of ICT Equipment must seek specification pre-approval from MUST Computing Services.

### 7.5.2 Management of IT Equipment

Periodic (Daily, Weekly, Monthly, and Quarterly, Yearly) Preventive maintenance shall be regularly performed on all Computers and Communication Systems.

Computing devices shall be configured to conserve energy through standard configuration settings or centrally controlled software managed by MUST Computing Services.

All Computers and related hardware shall be named according to an agreed naming convention.

### 7.5.3 Disposal of IT Equipment

The University shall dispose of IT equipment in ways that ensure environmental sustainability guided by the PPDA Act.

### 7.5.4 MUST Licensed Software

MUST Licensed software shall not be installed on non-MUST Computers. All Software Licenses shall be managed by MUST Computing Services.

### 7.5.5 Infrastructure Documentation

An up to date detailed inventory of IT Equipment shall be maintained by responsible departments and MUST Computing Services.

There shall be a Quarterly Internal Audit of all IT Equipment in line with Approved MUST Annual Internal Audit work plan.

An updated network topology shall be maintained and easily accessible.

### 7.5.6 Corporate Internet / Intranet

All Internet usage shall be monitored.

Access to sites that contain obscenity, pornography, material pertaining to violence or otherwise illegal material is prohibited.

### 7.5.7 Personal Computing Devices

A user of a Personal Computing device shall seek authorization from the MUST Computing Services in accordance with Procedures and guidelines to have his or her device connected to the corporate network.

A list of all Personal Computing Devices connected on the network shall be maintained and easily accessible.

### 7.5.7 Change Management and Configuration Control

MUST Computing Services shall submit all changes to be made to any of the Information Systems and Business Applications to the ICT Committee as the final authority on decision making.

A standard configuration of all ICT assets shall be maintained

## 7.6 POLICY STRATEGY 6: Data and Information Security

**POLICY OBJECTIVE: Upholding the principles of Information Security through the preservation of the confidentiality, Integrity and Availability of the university's information.**

### 7.6.1 Roles

a) The Council Committee on Audit and Risk shall provide leadership for the Governance of Cyber security within the University

b) MUST Computing Services shall;

   i. Ensure that appropriate security controls and mechanisms have been put in place
   ii. Maintain an updated ICT risk register
   iii. Implement periodic and infrastructure audits
   iv. Ensure controlled and audited usage of ICT administrative privileges
   v. Ensure the limited and controlled use of network ports
   vi. Coordinate user- security awareness and training
   vii. Develop and maintain handover mechanism for ICT equipment and information during end of staff employment contracts in line with the Human Resource Manual

c) Users shall report any cyber security incident to MUST Computing Services and ensure compliance to the Data and information security policy

### 7.6.2 Information Access

Access of university computing resources/ information shall be limited to;

- Full-time, part-time and temporary staff employed by, or working for or on behalf of the University.
- Students studying at the university.
- Contractors and consultants working for or on behalf of the university.
- Request from University Council, University Management, Heads of Department and/or University Human Resource Department

Suspension and/ or termination of access to university computing resources/ information shall be limited to

- End pf student or staff employment tenure
- Occurrence of any of the unacceptable usage restrictions
- Request from University Council, University Management, Heads of Department and/or University Human Resource Department

### 7.6.3 Unacceptable Usage

The following activities shall be strictly prohibited;

a) Sharing of individual access passwords/passphrases

b) Usage of pirated software on university computing devices

d) Contravention of the Computer Misuse Act (2011), the Anti-Pornography Act (2014), the Electronic Signatures Act (2011) and the Copyright and Neighboring Rights Act (2006)
c) Introduction of malicious software onto any university computing device/ network
d) Violation of the rights of any person or company protected by the Copyright, Trademark, Patent or other Intellectual Property law or the University's Patent, Intellectual Property, Code of conduct policies
e) Any password cracking or software spying/penetration
f) Usage of university computing devices and/ or network to disrupt external system or network
g) Usage of university computing devices and/ or network to send out any spam
h) Usage of university computing devices and/or network for any personal commercial purposes

### 7.6.4 Security of Third Party Access

Access to the university's information processing facilities by third parties will be controlled. Third parties who require access to the university's information infrastructure will be bound by a contract that defines university security requirements.

### 7.6.5 Protection of Key Data and Information

a) Key data and information will be classified, protectively marked and only accessible to those privileged to access.
b) No sensitive or confidential university information shall be stored on personal computing devices

### 7.6.6 Personal Security of Information

Security roles and responsibilities will be included in job descriptions where appropriate. These will include any specific responsibilities for the protection of particular information, passwords to information or the execution of particular processes or activities such as data protection.

### 7.6.7 Communications Management

MUST Computing Services shall implement controls to enable the correct and secure operation of information processing facilities in line with the university's Communication policy.

### 7.6.8 Virus Protection

MUST Computing Services shall design and develop a Virus protection and Management Policy, to prevent the introduction and transmission of computer viruses both within and from outside the university. This will extend to managing and containing viruses if preventive measures fail.

### 7.6.9 Password and Privilege Management

a) MUST Computing Services shall ensure that users follow good security practices in the selection, use and management of their passwords to keep them confidential.
b) MUST Computing Services shall ensure the allocation system privileges to users of computer platforms and information systems.

c) MUST Computing Services shall define the password strength and lifecycle specification for all user categories from time to time
d) All default system and hardware passwords shall be changed
e) All users shall ensure privacy of their passwords
f) All locally developed applications shall support password segregation

### 7.6.10 Unattended User Equipment

Users of the university's information processing facilities shall be responsible for safeguarding key data by ensuring that desktop machines are not left logged-on when unattended, and that portable equipment in their custody is not exposed to theft.

### 7.6.11 Disposal of Information Storage Media

MUST Computing Services shall ensure that all removable magnetic and optical media containing key data will be reused or disposed of through controlled and secure means when no longer required.

### 7.6.12 Disaster Recovery

MUST Computing services shall ensure that there is a drawn up and approved Disaster recovery and Business Continuity plan both on-site and off-site.

Procedures shall be developed to ensure continuity of ICT Services in the event of a disaster or major service disruption.

### 7.6.13 Expectation of Privacy

All authorized users will have no expectation of privacy when using MUST Information systems. MUST may log, review and otherwise utilize any information stored on or passing through its systems.

### 7.6.14 Security Testing Tools

Unless specifically authorized by the MUST Computing Services, MUST Information Systems users are prohibited from using any Hardware or Software that monitors the traffic on a network or the activity on a computer.

### 7.6.15 Incident Handling

MUST Computing Services shall investigate all reported security weaknesses and incidents reports. Remedial action shall be authorized by MUST Computing Services

### 7.6.16 Monitoring

Periodic (Daily, Weekly, Monthly, and Quarterly, Yearly) monitoring of all security related events shall be logged and audit trails saved in a centralized log location

A report of the same shall be submitted to the ICT Committee on a Quarterly basis for noting.

### 7.6.16 Back ups

MUST Computing Services shall ensure that all critical university digital data and information are regularly backed-up at the following locations;

a) On-site university facilities and media
b) Off-site facilities and in the cloud
c) The National Information Technology Authority designated sites.

### 7.6.18 Physical Security

a) The university shall define and periodically review the technology for SMART Access control for different university buildings and facilities
b) Areas within MUST premises that require restricted access must use Bio-metric, CCTV and Alarm systems.
c) Visitors to MUST premises must follow the standard check-in/check-out procedure.
d) Data Center(s)/Server(s) shall-
    i. Be located in secure locations away from human or vehicle traffic
    ii. Be fitted with both manual/electronic access control with CCTV monitoring
    iii. Be protected against physical intrusion and exposure to water, dust and fire
    iv. Be protected against power fluctuations
    v. Be air-conditioned
    vi. Be supported by alternate power supply
e) Computer Lab Facilities shall-
    i. Be routinely checked for unauthorized connections
    ii. Be accessed only by authorized students and/ or researchers
    iii. Be locked down to prevent physical theft of any component and manned by a university employee
    iv. Be protected against exposure to water leakages, fire and dust
    v. Be located in strongly burglar proofed rooms
    vi. Be labelled according to approved nomenclature
    vii. Be fitted with appropriate furniture
    viii. Be air-conditioned
    ix. Professionally serviced and maintained

## 7.7 POLICY STRATEGY 7: ICT Procurement and Disposal

POLICY OBJECTIVE: To ensure that the university obtains value for money from ICT related procurements

### 7.7.1 Responsibilities

a) The university's Procurement and Disposal Unit (PDU) shall be responsible for overall coordination and guidance on ICT procurements and disposals in line with the PPDA Act.

b) User departments shall initiate procurement and disposal requests with full technical guidance of MUST Computing Services in line with the PPDA Act

c) MUST Computing Services shall;

   i. Provide technical assistance to user departments by providing technical specifications for ICT goods and services to be procured.

   ii. Provide consultancy services to all university units on ICT needs and requirements

   iii. Certify that ICT goods and services supplied or installations/configurations are indeed as specified in the requirements

### 7.7.2 Disposal of ICT Products and Services

MUST Computing Services shall define a specific life cycle for each category of ICT product or service in order for replacements to be planned.

Disposal of ICT products shall follow the PPDA Act

Software use shall end upon the termination of the software support from the developer.

## 7.8 POLICY STRATEGY 8: Social Media

POLICY OBJECTIVE: Ensuring that the university maintains an interactive online presence on the World Wide Web

### 7.8.1 Official Social Media Accounts

For any existing Social Media platform, the university shall run only ONE official page or account to be recognized by the university.

### 7.8.2 Content on Official Social Media Accounts

i. Only official university accounts shall make use of the university's trademarks, symbols and logos.

ii. Only authorized personal by the university shall be allowed to make official posts on behalf of the university on these accounts in line with the university's communication policy.

iii. Content on the university Social media account should portray a good image of the university

## 7.9 POLICY STRATEGY 9: Special Needs ICT Use

**POLICY OBJECTIVE: To provide for the use of ICT products and services with consideration to different categories of persons with special needs.**

a) The university, from time to time, shall review the special needs of the existing staff and students

b) All ICT products and services obtained by the university should have provision for acceptable use by persons with special needs

c) Special provisions shall be made for training of staff and students with special needs on how to use ICT products and services.

## 7.10 POLICY STRATEGY 10: ICT Skills Capacity Building

**POLICY OBJECTIVE: To ensure that university staff and students are appropriately skilled to efficiently utilize available ICT resources**

### 7.10.1 ICT Skills Capacity Assessment and Delivery

a) MUST Computing Services shall co-ordinate the periodic assessment of existing ICT skills capacity amongst all user groups to be able to identify gaps in partnership with Heads od Departments

b) MUST Computing Services shall undertake periodic skills assessment to identify knowledge gaps within its technical staff

c) MUST Computing Services shall prepare, arrange, coordinate and/ or facilitate, with external expertise if need be, ICT capacity skills training sessions for all user groups

# 8.0 Implementation framework

The successful achievement of the goals and objectives of this policy shall depend on the concerted efforts of the different stakeholders who include staff/students/visitors, MUST Computing Services, the ICT Committee, University Management and the University Council. It is therefore important that there is a clear definition of the role each player shall have in ensuring the success of this policy.

For detailed Implementation Plan see **Appendix 3**

## 8.1 Institutional Framework

The following bodies/committees/institutions/departments shall be important in creating a favorable framework to improve policy formulation, coordination and implementation.

### 8.1.1 MUST Computing Services

MUST Computing Services shall be responsible for the overall coordination of formulation, implementation, review and target achievement. MUST Computing Services shall;

a) Ensure the achievement of the university's ICT vision by advising the university management on ICT matters
b) Effect university IT policies strategies and master plans
c) Coordinate the acquisition, implementation, delivery and support of the sustenance of university IT equipment and services
d) Provide technical support for university IT systems
e) Set and monitor IT standards for quality including risk management and contingency planning
f) To identify and establish IT training requirements for effective utilization of the ICT
g) Ensure data protection and information security on IT systems deployed.

### 8.1.2 ICT Committee

The University ICT Committee shall have its representation as determined by the University management, and shall be mandated to;

a) Oversee the development and implementation of ICT related policies for the university
b) Have an oversight on security of all ICT assets, facilities and logistical requirements.
c) Advocate for appropriate budgetary allocation of the University total budget to ICT related activities and initiatives.
d) Approve, monitor and review ICT implementation developmental projects for the university
e) Approve, monitor and review annual ICT budgets and work plans for the university

### 8.1.3 University Management

The university management shall provide executive vision and leadership towards the implementation of the ICT policy by providing an enabling institutional, financial and management environment.

### 8.1.4 University Council

The University Council shall act through its role as the governing body of the University which exercises general oversight over the institution and its affairs.

# 9.0 Monitoring and Evaluation

MUST Computing Services Unit shall take the lead in the monitoring and evaluation of the implementation of this policy.

The realization of the intended outputs of this policy shall be reported by MUST Computing Services providing periodic reports to management on the status of ICT in-line with the university's strategic plan and this policy.

The ICT status of the university shall be subjected to mid-term and long-term review.

## 9.1 Core Indicators

The indicators below are an extract of what shall be used for measuring the progress while implementing this policy;

a) Computer to student ratio
b) Computer to staff ratio
c) Internet bandwidth
d) Internet bandwidth per student and staff (bits/second)
e) Proportion of university network/internet downtime
f) Proportion of staff using the internet
g) Proportion of students using the internet
h) Proportion of university building infrastructure with Local Area Network
i) Proportion of university area covered by wireless internet
j) Proportion of university activities/faculties/departments/units with a web presence
k) Number of hits to university websites
l) Number of likes/interactions/views on university social media platforms
m) Proportion of university business processes that are automated
n) Proportion of academic staff using eLearning
o) Proportion of students using eLearning
p) Proportion of staff trained in different ICT capacity skills areas

## 10.0 Communication of the policy

This policy shall be made known to the staff, students and visitors of the university, through;

a) Making it visible on and able to be downloaded from the university's main web domain
b) Sending soft-copies to the relevant stakeholders through e-mail
c) Having it printed and distributed accordingly
d) Disseminated through workshops and seminars

## 11.0 Funding

The funding of this policy's implementation shall be catered for under the university's Annual ICT budget.

*Table 1: Proposed Recurrent ICT Budget for financial years 2019/2020 to 2023/2024*

| No | Item | 2019/2020 FY (UGSHS) | 2020/2021 FY (UGSHS) | 2021/2022 FY (UGSHS) | 2022/2023 FY (UGSHS) | 2023/2024 FY (UGSHS) |
|---|---|---|---|---|---|---|
| 1 | Software Licenses- Including Operating systems, Office Suites and Anti-virus software | 36,669,500 | 38,379,000 | 38,379,000 | 38,379,000 | 38,379,000 |
| 2 | Internet Subscription (monthly) | 206,040,000 | 272,073,600 | 272,073,600 | 272,073,600 | 272,073,600 |
| 3 | University Website Hosting (annually)- Includes must.ac.ug; itfc.org and Secure Socket Layer (SSL) Certificate for must.ac.ug | 4,641,000 | 4,914,000 | 4,914,000 | 4,914,000 | 4,914,000 |
| | **GRAND TOTAL** | **247,350,500** | **315,367,200** | **315,367,200** | **315,367,200** | **315,367,200** |

*Table 2: Proposed Development ICT Budget for financial years 2019/2020- 2023/2024*

| **No** | **Item** | **2019/2020 FY (UGSHS)** | **2020/2021 FY (UGSHS)** | **2021/2022 FY (UGSHS)** | **2022/2023 FY (UGSHS)** | **2023/2024 FY (UGSHS)** |
|---|---|---|---|---|---|---|
| 1 | Upgrade and Repairs of Network Infrastructure in the different university building blocks; | 18,950,000 | 18,950,000 | 18,950,000 | 18,950,000 | 18,950,000 |
| 2 | Wireless Outdoor Points To expand wireless access | 16,150,000 | 16,150,000 | 16,150,000 | 16,150,000 | 16,150,000 |
| 3 | Student Desktop Computers- To be distributed across faculties | 61,500,000 | 61,500,000 | 61,500,000 | 61,500,000 | 61,500,000 |
| 5 | Network Equipment | 39,000,000 | 39,000,000 | 39,000,000 | 39,000,000 | 39,000,000 |
| 6 | Maintenance Equipment and accessories | 4,400,000 | 4,400,000 | 4,400,000 | 4,400,000 | 4,400,000 |
| | **GRAND TOTAL** | **140,000,000** | **140,000,000** | **140,000,000** | **140,000,000** | **140,000,000** |

Extra resource mobilization shall target donors through grant applications as well as the involvement of private sector through Public Private Partnerships (PPPs).

# 12.0 Appendices

## 12.1 Appendix 1: Implementation Plan

| Policy Strategy | Years | 2019/2020 | 2020/2021 | 2021/2022 | 2022/2023 | 2023/2024 | Comments |
|---|---|---|---|---|---|---|---|
| ICT Governance | ICT Committee | | | | | | The committee does exist already but it is recommended that it is made a committee of council |
| | MUST Computing Services | Regularization and formation of University Computing Services Directorate | Demarcation and furniture fitting for the Computing Services offices at Kihumuro campus | | | | The proposed structure for MUST Computing Services has been submitted through on-going revision process of the MUST Staff Establishment |
| University ICT Network Access | University Network Backbone/ Local Area Network | Connection of the Medical Lab Sciences Block-Mbarara town campus | Connection of the Physiology Block-Mbarara town campus<br>Connection of the Faculty of Computing & Informatics Block-Kihumuro Campus | Connection of the Pharmacy Lecture Rooms Block-Mbarara town campus | Connection of the Ladies Flat-Mbarara town campus | Connection of the Ladies Flat-Kihumuro campus | The Kihumuro campus backbone connecting the Library, FAST, FAST Labs and Estates Block has been completed.<br>A number of blocks at the Mbarara town campus await connection to the backbone |
| | University Data Center | Automate the Door locking mechanism of Kihumuro Data Centre<br>Improve the power connectivity of the Mbarara town campus server room | Install CCTV surveillance cameras for the Data Center at Kihumuro campus<br>Install power backup system for Datacenter at Kihumuro | Procurement of Network & Server Equipment | Procurement of Network & Server Equipment | Procurement of Network & Server Equipment | Main Data Center at Kihumuro has been demarcated and initial equipment installed<br>Server room at Mbarara town campus also exists but is congested |

| | | 2019/2020 | 2020/2021 | 2021/2022 | 2022/2023 | 2023/2024 | Comments |
|---|---|---|---|---|---|---|---|
| | University Wireless Network Services | Expansion of wireless service coverage to Library- Kihumuro Campus<br>Expansion of wireless service coverage around Science Block-Mbarara campus | Expansion of wireless service coverage - Kihumuro Campus<br>Expansion of wireless service coverage-Mbarara campus | Expansion of wireless service coverage - Kihumuro Campus<br>Expansion of wireless service coverage-Mbarara campus | Expansion of wireless service coverage - Kihumuro Campus<br>Expansion of wireless service coverage-Mbarara campus | | Wireless network service for staff and students is present at the Mbarara town & Kihumuro campuses |
| | Bandwidth | Increase the bandwidth allocation to Mbarara town (150 Mbps) & Kihumuro campuses (50 Mbps) | Increase the bandwidth allocation to Mbarara town (200 Mbps) & Kihumuro campuses (100 Mbps) | Increase the bandwidth allocation to Mbarara town (300 Mbps & Kihumuro campuses (150 Mbps) | Increase the bandwidth allocation to Mbarara town (400 Mbps & Kihumuro campuses (200 Mbps) | Increase the bandwidth allocation to Mbarara town (500 Mbps & Kihumuro campuses (250 Mbps) | The university currently subscribes to 90Mps for the Mbarara town campus<br>And 30Mbps for the Kihumuro campus |

| | | 2019/2020 | 2020/2021 | 2021/2022 | 2022/2023 | 2023/2024 | Comments |
|---|---|---|---|---|---|---|---|
| Software Management | Academic Information Management System | Deploy newer version of the system based on new requirements from users<br>Build internal capacity to ensure ownership of system processes, data and information<br>Formalize ownership status between the university, GoU and Zeenode | Review status of system & its use and make recommendations<br>Carry out system audit | Review status of system & its use and make recommendations | Review status of system & its use and make recommendation s | Review status of system & its use and make recommendation s | The university is in the final stages of operationalizing the Academic Information Management System |
| | Library Management System | Deploy Library Management System to ensure automation of library process | Review status of system & its use and make recommendations<br>Carry out system audit | Review status of system & its use and make recommendations | Review status of system & its use and make recommendation s | Review status of system & its use and make recommendation s | In 2019/2020, in university is due to receive a Library Management System under the ADB-HEST program |

| | | 2019/2020 | 2020/2021 | 2021/2022 | 2022/2023 | 2023/2024 | Comments |
|---|---|---|---|---|---|---|---|
| | Other Software | Review status of software & its use and make recommendations<br>Make recommendations for other software necessary for teaching learning & research | Review status of software & its use and make recommendations<br>Make recommendations for other software necessary for teaching learning & research | Review status of software & its use and make recommendations<br>Make recommendations for other software necessary for teaching learning & research | Review status of software & its use and make recommendations<br>Make recommendations for other software necessary for teaching learning & research | Review status of software & its use and make recommendations<br>Make recommendations for other software necessary for teaching learning & research | The university currently operates licensed versions of Microsoft Operating System, Microsoft Office and Kaspersky antivirus software |
| IT Services Support & IT Infrastructure Management | IT Infrastructure support | Review current maintenance manual and update it<br>Hold periodic maintenance review exercises for hardware and software<br>Maintain IT equipment inventory | Review current maintenance manual and update it<br>Hold periodic maintenance review exercises for hardware and software<br>Maintain IT equipment inventory | Review current maintenance manual and update it<br>Hold periodic maintenance review exercises for hardware and software<br>Maintain IT equipment inventory | Review current maintenance manual and update it<br>Hold periodic maintenance review exercises for hardware and software<br>Maintain IT equipment inventory | Review current maintenance manual and update it<br>Hold periodic maintenance review exercises for hardware and software<br>Maintain IT equipment inventory | The Computing Services Unit currently manages IT infrastructure support but this is hampered by the unit's poor human resource structure |

| | | 2019/2020 | 2020/2021 | 2021/2022 | 2022/2023 | 2023/2024 | Comments |
|---|---|---|---|---|---|---|---|
| | Web Services | Prepare guidelines for creating, designing and updating content under the must domain. | Review current website design and content and make improvements | Review current website design and content and make improvements | Review current website design and content and make improvements | Review current website design and content and make improvements | The university operates its website under its domain name of www.must.ac.ug and also has a number of other sub-domain websites |
| | E-mail Services | Review usage and users of university e-mail services<br>Sensitization of e-mail communication etiquette | Review usage and users of university e-mail services<br>Sensitization of e-mail communication etiquette | Review usage and users of university e-mail services<br>Sensitization of e-mail communication etiquette | Review usage and users of university e-mail services<br>Sensitization of e-mail communication etiquette | Review usage and users of university e-mail services<br>Sensitization of e-mail communication etiquette | The university runs a staff and student mailing system through Google's G-Suite applications and is configured to match the university web domain |
| | E-Learning Services | Review usage, users and content of learning management system<br>Encourage and train staff and student to adopt to the learning management system and other e-learning applications | Review usage, users and content of learning management system<br>Encourage and train staff and student to adopt to the learning management system and other e-learning applications | Review usage, users and content of learning management system<br>Encourage and train staff and student to adopt to the learning management system and other e-learning applications | Review usage, users and content of learning management system<br>Encourage and train staff and student to adopt to the learning management system and other e-learning applications | Review usage, users and content of learning management system<br>Encourage and train staff and student to adopt to the learning management system and other e-learning applications | The university  runs an open-source claroline based learning management system on lms.must.ac.ug |

| | | 2019/2020 | 2020/2021 | 2021/2022 | 2022/2023 | 2023/2024 | Comments |
|---|---|---|---|---|---|---|---|
| | Cloud Computing | Review status of university cloud computing services<br>Based on existing electricity & internet environments, make recommendations for other applications that might suitably be hosted in the cloud. | Review status of university cloud computing services<br>Based on existing electricity & internet environments, make recommendations for other applications that might suitably be hosted in the cloud. | Review status of university cloud computing services<br>Based on existing electricity & internet environments, make recommendations for other applications that might suitably be hosted in the cloud. | Review status of university cloud computing services<br>Based on existing electricity & internet environments, make recommendations for other applications that might suitably be hosted in the cloud. | Review status of university cloud computing services<br>Based on existing electricity & internet environments, make recommendations for other applications that might suitably be hosted in the cloud. | Due to instabilities in the electricity and internet environments of the university the university currently host certain services in the web e.g. the websites and e-mail services |

| | | 2019/2020 | 2020/2021 | 2021/2022 | 2022/2023 | 2023/2024 | Comments |
|---|---|---|---|---|---|---|---|
| Data and Information Security | | Review of information access status for staff and students in line with Human Resource and student status<br>Communication of Unacceptable Usage activities to staff and students<br>Enforcement of password and privilege management policy<br>Approval of Disaster Recovery & Business Continuity Plan<br>Ensure Physical security guidelines as per policy<br>Effect IT security audits | Review of information access status for staff and students in line with Human Resource and student status<br>Communication of Unacceptable Usage activities to staff and students<br>Enforcement of password and privilege management policy<br>Ensure Physical security guidelines as per policy<br>Effect IT security audits | Review of information access status for staff and students in line with Human Resource and student status<br>Communication of Unacceptable Usage activities to staff and students<br>Enforcement of password and privilege management policy<br>Ensure Physical security guidelines as per policy<br>Effect IT security audits | Review of information access status for staff and students in line with Human Resource and student status<br>Communication of Unacceptable Usage activities to staff and students<br>Enforcement of password and privilege management policy<br>Ensure Physical security guidelines as per policy<br>Effect IT security audits | Review of information access status for staff and students in line with Human Resource and student status<br>Communication of Unacceptable Usage activities to staff and students<br>Enforcement of password and privilege management policy<br>Ensure Physical security guidelines as per policy<br>Effect IT security audits | |

| | | 2019/2020 | 2020/2021 | 2021/2022 | 2022/2023 | 2023/2024 | Comments |
|---|---|---|---|---|---|---|---|
| ICT Procurement and Disposal | | Implement ICT product procurement and Disposal as per PPDA Act and the policy<br>Advocacy of aggregation of ICT product procurements to ensure benefits of economies of scale | Implement ICT product procurement and Disposal as per PPDA Act and the policy<br>Advocacy of aggregation of ICT product procurements to ensure benefits of economies of scale | Implement ICT product procurement and Disposal as per PPDA Act and the policy<br>Advocacy of aggregation of ICT product procurements to ensure benefits of economies of scale | Implement ICT product procurement and Disposal as per PPDA Act and the policy<br>Advocacy of aggregation of ICT product procurements to ensure benefits of economies of scale | Implement ICT product procurement and Disposal as per PPDA Act and the policy<br>Advocacy of aggregation of ICT product procurements to ensure benefits of economies of scale | |
| Social Media | | Ensure that the university is visible active on interactive social media platforms like Facebook, Twitter, Instagram, WhatsApp etc | Ensure that the university is visible active on interactive social media platforms like Facebook, Twitter, Instagram, WhatsApp etc | Ensure that the university is visible active on interactive social media platforms like Facebook, Twitter, Instagram, WhatsApp etc | Ensure that the university is visible active on interactive social media platforms like Facebook, Twitter, Instagram, WhatsApp etc | Ensure that the university is visible active on interactive social media platforms like Facebook, Twitter, Instagram, WhatsApp etc | |
| Special Needs ICT use | | Ensure that all ICT products and services consider usage by person with special needs | Ensure that all ICT products and services consider usage by person with special needs | Ensure that all ICT products and services consider usage by person with special needs | Ensure that all ICT products and services consider usage by person with special needs | Ensure that all ICT products and services consider usage by person with special needs | |

| | | 2019/2020 | 2020/2021 | 2021/2022 | 2022/2023 | 2023/2024 | Comments |
|---|---|---|---|---|---|---|---|
| ICT Skills Capacity Building | | Assessment of existing ICT skills gaps amongst all ICT user groups<br>Arrange and facilitate ICT Skills capacity training exercise | Assessment of existing ICT skills gaps amongst all ICT user groups<br>Arrange and facilitate ICT Skills capacity training exercise | Assessment of existing ICT skills gaps amongst all ICT user groups<br>Arrange and facilitate ICT Skills capacity training exercise | Assessment of existing ICT skills gaps amongst all ICT user groups<br>Arrange and facilitate ICT Skills capacity training exercise | Assessment of existing ICT skills gaps amongst all ICT user groups<br>Arrange and facilitate ICT Skills capacity training exercise | |