Mbarara University of Science and Technology

Draft Information & Communication Technology Policy

Version	3.0
Draft Date	February 2018
Status	Draft
Approved By:	University ICT Committee

Table of Contents

Definitions

User	A Person granted rights to use a system
Administrative User	A user with privileges to alter system settings
External User	Any user of Mbarara University data who is not a member of Staff
Information System	Is a Conceptual term used to identify collection of Computer hardware, software and network connections which together form the single, integrated system on which resides the Institutional database
Business Application	A set of programs designed to help an organization enhance productivity.

Abbreviations

CCTV	Closed Circuit Television
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Services
E-Learning	Electronic Learning
ICT	Information and Communications Technology
IT	Information Technology
IP	Internet Protocol
MUST	Mbarara University of Science and Technology
PDU	Procurement and Disposal Unit
PPDA	Public Procurement and Disposal of Assets Authority
SPOC	Single Point of Contact
VOIP	Voice over Internet Protocol

1.0 Introduction

1.1 Background

1.1.1 Purpose

This document articulates MUST's direction on appropriate use of organizational ICT resources.

1.2 Scope

The ICT Policy shall govern the following broad areas;

i. ICT Governance
ii. University ICT Network Access
iii. Software Management
iv. IT Services Support
v. Data Management
vi. IT Infrastructure Management
vii. Information Security Policy
viii. IT Security
ix. Remote Access Policy
x. ICT Procurement
xi. Social Media
xii. Special Needs ICT use

1.3 Legal Framework

The policy is in compliance with the Following Laws;

- National ICT Policy (2010)
- The Digital Signatures Act, 2010
- The Computer Misuse Act, 2010
- The Communications Act, 1997
- The Telecommunications Policy
- The Access to Information Act, 2005
- The Copyright and Neighboring Rights Act, 2006
- The Electronic Media Statue 1996
- The Electronic Transaction Act 2010
- The PPDA Act, 2003

2.0 ICT Governance

2.1 Policy Statement

The use of ICT requires a regulated and coordinated environment. A well enabled ICT governance framework ensures that the university benefits from efforts of investing into ICT products and services and also manages the resultant risks from these efforts.

2.2 Policy Principles

2.2.1 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

2.2.2 The University Computing Services

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

a) Provide ICT services to staff and students of the university and relevant to the academic, research and administrative functions of the university
b) Provide technical and professional leadership to ICT implementations and developments in the university
c) Operationalize the ICT policy implementation
d) Ensure optimized utilization of ICT resources in the university
e) Ensure legally and environmentally acceptable acquisition, use and disposal of ICT resources

2.2.3 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

2.2.4 Staff and Students

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

3.0 University ICT Network Access

3.1 Policy Statement

To ensure final delivery of ICT services to staff and students, the university shall ensure structured means of delivering these services through a well-established network backbone infrastructure.

3.2 Policy Principles

3.2.1 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.

3.2.2 The University Data Center and related services

a) The university shall run a Main Data Center to act as the central repository for all university databases and web hosting 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.

3.2.3 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

3.2.4 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.

3.2.5 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.

4.0 Software Management

4.1 Policy Statement

The University shall ensure that all produced software complies with user requirements and is secure. That the University meets its legal and contractual obligations, obtains value for money, and operates effectively and securely in the licensing, procuring and management of software.

4.2 Policy Principles

4.2.1 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

4.2.2 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.

4.2.3 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.

4.2.4 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.

4.2.5 Design Review

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

4.2.6 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.

4.2.7 Implementation

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

4.2.8 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.

4.2.9 Training

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

4.2.10 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

4.2.11 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.

4.2.12 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.

4.2.13 Propriety Software Procurement and acquisition

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 Computing Services Unit.

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

4.2.14 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 Computing Services Unit.

4.2.15 Permitted use of University software

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

4.2.16 Versions of Software

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

4.2.17 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.

4.2.18 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.

4.2.19 Copyrighted, Licensed or other Intellectual Property

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.

5.0 IT Services Support

5.1 Policy Statement

The MUST Computing Services shall provide an integrated service based on approved system frameworks that support MUST business processes.

5.2 Policy Principles

5.2.1 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.

5.2.2 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.

5.2.3 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.

5.2.4 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.

5.2.5 E-learning Services

The University shall operate an E-Learning software platform and facilities in accordance with the university's E-Learning policy.

5.2.6 Trouble Shooting

IT Service disruptions shall be managed in such a manner to restore operations to normal within agreed service levels and business priorities. IT services will be provided through a service management framework following best practice. Under the framework a single point of contact (SPOC) shall interface between MUST Computing Services and other MUST staff.

6.0 Data Management

6.1 Policy Statement

The MUST Computing Services shall develop a data standards manual, which shall be approved by the University ICT Committee and eventually University Management. All MUST data shall be in a format described in the data standards manual.

6.2 Policy Principles

6.2.1 Data Administrators

These shall be responsible for Electronic data storage ensuring accessibility and availability of the stored data to authorized users and providing appropriate back-up procedures and guidelines which shall be approved by the University ICT Committee and eventually University Management.

6.2.2 Data Integrity, Validation and Correction

Applications that capture and update MUST data shall incorporate edit and validation checks; to assure accuracy and integrity (Consistency of the data).

7.0 Infrastructure Management

7.1 Policy Statement

MUST shall provide an ICT Infrastructure that will facilitate teaching, research and administration Support

7.2 Policy Principles

7.2.1 Acquisition of Computing Equipment

Every Unit must generate a Computing Equipment Procurement plan which MUST be generated for each Financial Year and be signed by the division Head and submitted to the Computing Services Unit and eventually University ICT Committee.

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.

7.2.2 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.

7.2.3 Disposal of IT Equipment

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

7.2.4 MUST Licensed Software

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

7.2.5 Corporate Telephony (VoIP)

The University shall ensure provision of Telephony Services for all Staff to support the Communication Services.

All Staff shall be allocated a secret Telephone access pin Code known to the employee who will be responsible for its protection and the related costs at all times.

7.2.6 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.

7.2.7 Corporate Internet / Intranet

The Computing Services Unit shall develop guidelines and Procedures on usage of University Computing Facilities.

These shall be approved by the University ICT Committee and eventually University Top Management

All Internet usage shall be monitored.

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

7.2.7 Personal Computing Devices

MUST Computing Services will develop procedures and guidelines for all users, who wish to use Personal Computing Devices on the University network.

The Procedures and guidelines will be approved by the ICT Committee and finally submitted to University Management for approval

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.

7.2.8 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

8.0 Information Security Policy

8.1 Policy Statement

MUST shall uphold the principles of Information Security through the preservation of the confidentiality, Integrity and Availability of the university's information.

The University is committed to protect both its key data and information and to minimize the impact of any security incidents.

8.2 Policy Principles

8.2.1 Information Security Infrastructure

An Information Security Infrastructure will be developed to support Information Security.

8.2.2 Information Access

Access of university 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.

8.2.3 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.

8.2.4 Protection of Key Data and Information

Key data and information will be classified, protectively marked and only accessible to those privileged to access.

8.2.5 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.

8.2.6 Communications Management

MUST Computing Services shall implement controls to enable the correct and secure operation of information processing facilities.

8.2.7 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.

8.2.8 Password and Privilege Management

MUST Computing Services shall ensure that users follow good security practices in the selection, use and management of their passwords to keep them confidential.

The Computing Services Unit shall ensure the allocation system privileges to users of computer platforms and information systems.

8.2.9 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.

8.3.10 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.

9.0 IT Security

9.1 Policy Statement

MUST management recognizes the need to protect her IT resources against various security risks that could lead to data loss.

MUST Computing Services shall develop Guidelines and procedures to support IT Security Function which shall be approved by the University ICT Committee and then University Management.

MUST Computing Services shall also develop IT Security awareness alerts to Computing Facilities users.

9.2 Policy Principles

9.2.1 Disaster Recovery

The Computing services shall ensure that there is a drawn up and approved Disaster recovery 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.

9.2.2 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.

9.2.3 Security Testing Tools

Unless specifically authorized by the Computing Services Unit, 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.

9.2.4 Incident Handling

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

9.2.5 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.

9.2.6 Physical Security

Areas within MUST premises that require restricted access must use Bio-metric, CCTV and Alarm systems.
Visitors to MUST premises must follow the standard check-in/check out procedure.

10.0 Remote Connectivity

10.1 Policy Statement

MUST Computing Services shall develop procedures and guidelines to support remote connectivity.
The Procedures and guidelines shall be approved by the University ICT Committee and eventually University Management.

10.2 Policy Principles

10.2.1 Remote Access

All new remote connectivity will go through the approved procedures and guidelines mentioned above.
Periodic (Daily, Weekly, Monthly, and Quarterly, Yearly) IT Security checks shall be regularly performed on all Computers and Communication Systems.

The reviews are to ensure that all access adequately matches business requirements, and that the principle of atleast access is followed

10.2.2 Cloud Computing

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.

11.0 ICT Procurement and Disposal

11.1 Policy Statement

The university shall aim at obtaining value for money from ICT related procurements through the university's standard procurement operating procedures in line with the PPDA Act.

11.2 Policy Principles

11.2.1 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

11.2.2 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.

12.0 Social Media

12.1 Policy Statement

In order for the university to maintain an interactive online presence on the web, it shall run different relevant Social Media accounts to keep in touch with stakeholders of the university.

12.2 Policy Principles

12.2.1 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.

12.2.2 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
iii. Content on the university Social media account should portray a good image of the university

13.0 Special Needs ICT Use

13.1 Policy Statement

Use of ICT products and services at MUST shall take into consideration the different categories of persons with special needs. These include those with physical conditions like visual, motor and hearing impairments.

13.2 Policy principles

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.

14.0 Enforcement

This Policy shall be implemented and monitored by MUST Computing Services, Human Resource Department and the University ICT Committee.

MUST Computing Services shall ensure that this policy is disseminated and all relevant stakeholders are sensitized.

Violations of sections of this policy shall be handled appropriately as guided by existing disciplinary mechanisms and procedures set by the university.