Draft Information Technology Policy

Version	3.0
Draft Date	June 2014
Status	Draft
Approved By:	

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.

1.0 Introduction

Background

Purpose

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

Scope

The ICT Policy shall govern the following broad areas;

- Software Management
- IT Services Support
- IT Infrastructure Management Information Security Policy
- IT Security
- Data Management
- Remote Access Policy

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

2.0 Software Management

2.1 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.

2.2 Policy Principles

2.2.1 Business Requirements

The software development and /or Acquisition process shall begin with documented business requirements, justified by a stated business case by a Unit.
Business requirements **MUST** be signed by the division Head and submitted to the **University ICT Committee** and eventually University Management before being handed to the **Software Incubation and Innovations Unit**.

Unsigned requirements **SHALL NOT BE** considered to be Software Requirements Specification.

2.2.2 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.

2.2.3 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.

2.2.4 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.

2.2.5 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.

2.2.6 Quality Assurance

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

2.2.7 Implementation

In the implementation phase, the software shall be developed to meet the design objectives. Software shall be developed according to the Programming guidelines and include documentation in the source code.

2.2.8 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 tester / Computing Services Unit shall check that the right test environment and the test equipment are available.

2.2.9 Training

Software Incubation and Innovations Team **MUST** produce written guidance and training materials for all produced Software.

2.2.10 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

2.2.11 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.

2.2.12 Software Support

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

2.2.13 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.

2.2.14 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.

2.2.15 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.

2.2.16 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.

2.2.17 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.

2.2.18 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.

2.2.19 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.

2.2.20 Software Escrow

In case third party software is to be used for Critical processes, the vendor must either license source code to MUST or the vendor must provide accessibility to the source code through and escrow agreement with a third party. This shall be done in full agreement of the university and the vendor.

3.0 IT SERVICES SUPPORT

3.1 POLICY STATEMENT

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

3.2 POLICY PRINCIPLES

3.2.1 IT SERVICE MANAGEMENT STANDARD

IT Services support shall adhere to the ISO / IEC 2000 (IT Service Management) standard.
MUST will endeavor that its IT Service Management is periodically audited by a Professional Service Provider of ISO Certification every 5 years.

3.2.2 IT INFRASTRUCTURE SUPPORT

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

The Computing Services Unit 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.

3.2.3 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.

3.2.4 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.
The Computing Services Unit shall ensure Business Applications are maintained at the most recent version to support any changes in business processes at MUST.

Business Application upgrades must only be implemented after approval of the MUST ICT Committee and eventually University Management.

3.2.5 Electronic Mail Services

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

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.

3.2.6 E-learning Services

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

3.2.7 Trouble Shooting

IT Service disruptions shall be managed in such a manner to restore operations to normal within agreed service levels and business priorities. 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 Computing Services Unit and other MUST staff.

4.0 DATA MANAGEMENT

4.1 POLICY STATEMENT

The computing services unit 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.

4.2 POLICY PRINCIPLES

4.2.1 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.

4.2.2 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).

The Computing Services Unit shall develop data validation and Correction Procedures and guidelines, which shall be approved by the University ICT Committee and eventually University Management.

5.0 INFRASTRUCTURE MANAGEMENT

5.1 POLICY STATEMENT

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

5.2 POLICY PRINCIPLES

5.2.1 ACQUISITION OF COMPUTING EQUIPMENT

Every Unit must generate a Computing Equipment Procurement plan which **MUST be** generated in the 1st Quarter of the Financial Year and be signed by the division Head and submitted to the Computing Services Unit and eventually University ICT Committee.

The Computing Services Unit shall develop and maintain up-to-date specifications of the ICT Equipment.
All requisition of ICT Equipment must seek specification pre-approval from the Head of the Computing Services Unit.

5.2.2 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 the Computing Services Unit.

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

5.2.3 Disposal of IT Equipment

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

5.2.3 MUST Licensed Software

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

5.2.4 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.

5.2.5 Infrastructure Documentation

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

There shall be a Quarterly Internal Audit of all IT Equipment in line with Approved MUST Annual Internal Audit work plan. The report of the same shall be presented to the ICT Committee.

An updated network topology shall be maintained and easily accessible.

5.2.6 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.

5.2.7 Personal Computing Devices

The Computing Services Unit 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 Computing Services Unit 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.

5.2.8 Change Management and Configuration Control

The Computing Services Unit 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

6.0 INFORMATION SECURITY POLICY

6.1 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.

6.2 POLICY PRINCIPLES

6.2.1 Information Security Infrastructure

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

6.2.2 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.

6.2.3 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.

6.2.4 Protection of Key Data and Information

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

6.2.5 Personal Security of Information

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

6.2.6 Communications Management

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

6.2.7 Virus Protection

The Computing Services Unit 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.

6.2.8 Password and Privilege Management

The Computing Services Unit 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.

6.2.9 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.

6.3.0 Disposal of Information Storage Media

The Computing Services unit 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.

7.0 IT SECURITY

7.1 POLICY STATEMENT

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

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

The Computing Services Unit Shall also develop IT Security awareness alerts to Computing Facilities users.

7.2 POLICY PRINCIPLES

7.2.1 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.

7.2.2 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.

7.2.3 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.

7.2.4 Incident Handling

The Computing Services Unit shall investigate all reported security weaknesses and incidents reports.

Remedial action shall be authorized by the head of the Computing Services Unit

7.2.5 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.

7.2.6 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.

8.0 REMOTE CONNECTIVITY

8.1 POLICY STATEMENT

The Computing Services Unit 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.

8.2 POLICY PRINCIPLES

8.2.1 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

8.2.2 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.

9.0 ENFORCEMENT

This Policy shall be read together with the Human resource Management Manual and the staff code of conduct as if the same were in IT Policy. The offences highlighted below should be considered an addendum to the Offence Classification Schedule in the Human Resource Management Manual.

Offence	Essential Elements	Classification				
			1st Offence	2nd Offence	3rd Offence	4th Offence
Sharing Passwords & Access Tokens	Sharing System access credentials with any party	Gross Misconduct	Suspension	Termination		
Unauthorised use of Security Compromise Tools	Use of software or hardware to test or bypass security controls	Gross Misconduct	Termination			