MAKERERE UNIVERSITY

INFORMATION & COMMUNICATION TECHNOLOGY POLICY

APRIL 2016 - 2020

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

AFRINIC	African Network Information Center
BYOD	Bring Your Own Device
CCTV	Closed Circuit Television
DICTS	Directorate for ICT Support
DNS	Domain Name Services
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communications Technology
IP	Internet Protocol
LAN	Local Area Network
PDCA	Plan, Do, Check, Act
PPDA	Procurement and Disposal of Public Assets Act
WAN	Wide Area Network

FOREWORD

The adoption and utilization of Information and Communications Technology (ICT) within Makerere University is aligned to the University Strategic Plan. The implementation of ICT requires an overall guiding framework to ensure that it's well-managed, complies with legal and regulatory requirements, creates value, and supports the realization of the University's objectives based on globally accepted best practice, guidelines and principles.

In line with the above, the Makerere University ICT Policy provides a structure for all the relevant ICT policies to support the achievement of the ICT Vision. Broadly, the policies here within spell out best practice, define roles and responsibilities of all user groups as well as provide guidance in the delivery, implementation and usage of ICT.

Lastly, I wish to acknowledge the efforts of the Directorate for ICT Support in the coordination of the development of the ICT policy. We all have an obligation to the University to comply with this Policy.

……………………………

Chair

Makerere University Council

PREAMBLE

The purpose of this Policy is to describe and document the ICT policies and procedures that will support Makerere University goals and objectives within all the teaching, learning, research and administrative units. This geared towards increasing effectiveness and efficiency in all University functions. As such, the development of these policies took into consideration alignment to other existing University functional policies as well as globally recognized ICT practices. The University will accordingly ensure the university-wide dissemination of this Policy to user group categories.

The Policies will be reviewed periodically to ensure they remain relevant and aligned to the goals of the University.

GENERAL SCOPE

The ICT policy applies to all Makerere University Departments, Colleges and Units and covers these areas:

i. ICT Governance
ii. University Data Communications
iii. Cyber Security
iv. Software Development and Acquisition
v. ICT Service Management
vi. ICT Skills Capacity Building
vii. ICT Services Support
viii. Telecommunications and Unified Communications
ix. ICT Procurement
x. Social Media
xi. Software Licensing and Ownership
xii. Information Systems and Data Warehousing
xiii. Special Needs ICT Usage

1.0 ICT GOVERNANCE POLICY

1.1 Introduction

Effective ICT Governance provides a conducive environment for the alignment of all ICT investments in a rationalized manner that is aligned towards enabling an organization meet its goals and objectives. This also contributes to the attainment of value for money, management of risks and effective ICT utilization.

1.2 Policy Objective

To provide for the centralized effective Governance of all ICT related matters within the University in a rationalized and harmonized manner.

1.3 Policy Scope

This policy applies to all ICT related matters within the University.

1.4 Policy Statements

1.4.1 The Council Committee on Quality Assurance, ICT and Gender

The Council Committee on Quality Assurance, ICT and Gender shall have its representation as determined by the University Council. The Committee shall:

a) Advise and monitor the implementation of the ICT Strategy and Policy;

b) Ensure provision of resources within the University Budgeting process for implementation of the ICT Strategy through:

   i. Ring fencing three percent (3%) of the University total budget towards ICT spending. This budget includes the budget for DICTS plus the ICT budget components in all Colleges and Units of the University.

   ii. Inclusion of one percent (1%) ICT support within all University Grants

c) Monitor development and innovations in ICT sector, in order to advise on implementation of innovative and sustainable ICT solutions aligned to the University's strategic goals;

d) Undertake advocacy for the adoption and utilization of ICT within the University; and

e) Act as Champion Agents in the enforcement of the ICT Policy.

1.4.2 Directorate for ICT Support

The Directorate for ICT Support (DICTS) shall as the focal point of contact for the ICT Service

Management function within the University. DICTS shall:

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

1.4.3 User Forum

The University shall establish the User Forum (UF) that will be a representation of responsible Principal/ Head of Department from all the teaching, learning, administration and research domain units as a platform for end user satisfaction. With DICTS as the secretariat, the UF shall:

a) Provide a forum for the continuous evaluation and assessment of existing ICT services and infrastructure;
b) Identify and communicate to DICTS any emerging needs across the University domain areas;
c) Act as Change Agents during the introduction of new innovation or new ICT services; and
d) Act as the link for the university-wide user community engagement with DICTS as regards the ICT Service Provision.

1.4.4 Heads of Teaching, Learning, Administration and Research Units

The Principals/ Heads of Departments shall in consultation with DICTS:

a) Integrate ICTs into their activities;

b) Implement the Unit specific components of the ICT Policy and Strategy;

c) Ensure compliance to the ICT Policy Framework; and

d) Act as active participants during the periodic stakeholder consultations towards supporting and facilitating the effective implementation of the ICT Policy and Strategy.

1.4.6 Staff and Student Community

The Staff and Student Community shall ensure compliance to the ICT Policies.

1.5 Policy Approach

The Unit responsible for ICT has direct responsibility for maintaining and guiding implementation of this policy.

2.0 UNIVERSITY DATA COMMUNICATIONS NETWORK POLICY

2.1 Introduction

a) Makerere University has over the years integrated the use of ICT in all its major operational areas: teaching, learning, administration and research. The fast rate of innovation has led to newer and more effective technological developments that have greater value. At the core of this infrastructure is the Data Communications Network that has evolved into the backbone for the provision and usage of daily utilized ICT services. This Policy sets out to achieve a rationalized infrastructure approach that will lead to the emergence of centralized network management through the Network Operations Center. This does require an appropriate policy to guide the development, maintenance and usage of the University 'backbone.

b) The university data communications network shall be broken down into the following areas:

i. ICT Infrastructure Rollout
ii. Digital network
iii. University Wide Area Network
iv. Campus Local Area Networks (LANs)
v. MAK Wireless Access provision
vi. Remote Access
vii. Access to Computing infrastructure and ICT services

2.2 Objectives

The objective of this Policy is to guide the development, rollout, maintenance and usage of the University Backbone to ensure resiliency, stability and higher uptime rates. This is all geared towards ensuring the usage of the backbone is aligned to the goals of the University as laid out in the University Strategic Plan.

2.3 Scope

This policy applies to user categories within the teaching, learning, administration and research units of the University as well as any contractors and authorized third party relations.

2.4 Policy Statements

2.4.1 Broad Network Policy

2.4.1.1 The Backbone

The University shall provide a resilient, secured and stable fast data communications network as an enabler to the processing, storage, dissemination and accessing of information or ICT enabled services as relates to the various needs of the teaching, learning, administration and research domains.

2.4.2 ICT Infrastructure Rollout

2.4.2.1 ICT Provision Plan

The University shall prepare a five (5) year ICT infrastructure rollout plan aligned to the University Strategic Plan. The plan will take into consideration the ever changing University computing needs, growth in demand usage of the backbone as well as technological advances that introduce smarter and innovative practices. At the core of this plan, is the alignment to the existing resource provision to ensure value for money as well as achieve sustainability.

2.4.3 Backbone expansion

(a) The unit responsible for ICT-DICTS, shall develop and maintain an updated University wide Enterprise Architecture as the blueprint for alignment of business requirements and ICT investments;

(b) All new backbone expansions shall be approved by Unit responsible for ICT to ensure alignment to the existing network design;

(c) The University shall establish and maintain a Data Center to act as the only central repository for all university databases and web hosting;

(d) Introduction of new technology within the network management or provision shall undergo professional testing to ensure compliance with existing standards and performance requirements;

(e) Heads of Departments will at each annual budgeting cycle shall plan for its specific ICT requirements for proper provisioning in a rationalized manner; and

(f) The University shall develop and maintain updated structured cabling standards to ensure a uniform level of acceptable design across all units.

2.4.4 Digital Network

2.4.4.1 Definition

The University Network will be defined as all such equipment involved in the transmission and routing of all digital communications within the University at all campuses.

2.4.4.2 Digital network overall components

a) The management of the entire digital network infrastructure shall be vested with the Unit responsible for ICT;

b) The Unit responsible for ICT shall periodically define the methodology for access to external data destinations and data routes;

c) The University shall establish central monitoring and control the University-wide digital network

d) All Domain Name Services (DNS) activities hosted within the University shall be centrally managed;

e) All core network components shall be designed to support redundancy for continued service provision;

f) The Network Backbone shall connect to all authorized access points and areas within the University;

g) All forms of access and usage of the backbone shall be managed by the Unit responsible for ICT;

h) The University shall ensure ownership of its own Internet Protocol (IP) number space in line with the African Network Information Center (AFRINIC) requirements and domain name ownership in line with the Internet Corporation of Assigned Names and Numbers (ICANN).

2.4.5 University Wide Area Network

2.4.5.1 Definition

The University Wide Area Network (WAN) refers to all the aggregated inter-connected campuses on the virtual one-network University domain.

2.4.5.2 University WAN components

a) All the external University campuses shall be interlinked onto the Main Campus Backbone with provision for survivability

b) All WAN data interlinks shall be based on resilient optical fibre or equivalent high capacity transmission media as specified by the Unit responsible for ICT

c) All WAN data interlinks shall be aligned to authorized University ICT configuration baselines to ensure consistency in security and performance.

2.4.6 Campus Local Area Network

2.4.6.1 Definition

The computer network within each campus, building shall form a Campus Local Area Network (LAN) and will have a designated technical administrator under the supervision of the Unit responsible for ICT.

2.4.6.2 Structure of Campus LANs

a) The University shall provide secured and resilient University LANs

b) All Campus LANs will ensure compliance with approved University ICT structured cabling standards and network configurations

c) All Campus LAN extensions or modifications shall require approval from the Unit responsible for ICT

d) The Network health monitoring and technical support shall be the responsibility of the Unit responsible for ICT.

2.4.7 MAK Wireless Access Provision

2.4.7.1 Definition

This refers to the provision of connectivity to the internet using wireless technology through authorized Access Points.

2.4.7.2 Structure of MAK Wireless Access

a) The University will support the provision of reliable and secured near-ubiquitous Wireless Access Points across the University Campuses;

b) Only approved Wireless Access Points shall be allowed to transmit wireless signals;

c) The configuration of such Wireless Access Points shall comply with approved network and security configurations to achieve consistency and performance standards;

d) The Wireless Access health monitoring and technical support shall be the responsibility of the unit responsible for ICT.

2.4.8 Remote Access

2.4.8.1 Definition

The University will support the provision of remote access for approved University resources. This supports the provision of access to network resources to authorized users across public internet infrastructure with consideration for information security.

2.4.8.2 Structure of Remote Access

a) The Unit responsible for ICT shall define and implement the remote access methodology, technology and standard as the requirements to ensure privacy and security

b) Remote Access shall only be provided to:

   i. Users approved by the Unit responsible for ICT as per the business need requirement

ii. Students or lectures within the open and distance learning programmes

c) All approved users for the remote access functionality shall consent to the Cyber Security Policy requirements for remote connections; and

d) The remote access usage monitoring shall be the responsibility of the Unit responsible for ICT.

2.4.9 Access to Computing Infrastructure and ICT Services

2.4.9.1 Server rooms and Network Equipment

a) Access to University Server rooms and other network equipment installations shall be secured and only allowed to authorized personnel;

b) Unauthorized movement of any network equipment and/or installation shall be only as authorized by the Unit responsible for ICT;

c) All network equipment and/or installation shall be labelled according to the University approved ICT nomenclature specification;

d) The Unit responsible for ICT shall maintain an updated Network Equipment asset register;

e) All University units shall maintain a service schedule for all network equipment;

f) All ICT equipment to be installed onto the university network shall comply with approved University specifications as spelt out by the Unit responsible for ICT from time to time;

g) All installations or modifications of any network equipment shall be approved and supervised by the Unit responsible for ICT;

h) All installations of network equipment by academic staff for educational purposes shall be authorized by the Unit responsible for ICT;

i) The Unit responsible for ICT shall define and manage all Service Level Agreements with third party service providers for bandwidth provision and any other ICT related service;

j) All external third party connections to the University network shall comply with the University ICT Policies;

k) All contractors or third party access to any server room or network equipment installation shall be authorized and supervised by the Unit responsible for ICT.

2.4.9.2 ICT Services

a) The provision of secured University E-mail services and related storage quotas will be centrally defined, managed and periodically reviewed by the Unit responsible for ICT;

b) All Makerere University websites and portals will be centrally hosted;

c) The University will establish and maintain an effective dedicated web cache management service to optimize bandwidth provision;

d) The Unit responsible for ICT shall centrally manage the provision of computing resources to all user groups within the research, teaching, learning and administration units of the University;

e) The University shall ensure the provision of a secure and efficient university intranet and web portal and its universal access

f) The Provision of ICT services will take into consideration the needs of:

   i. special user groups

   ii. guest access

g) Access to ICT services such as e-mail will be provided to authorized users as stated within the University Cyber Security and Internet Policy

h) The University reserves the right to audit, without prior notice, any ICT equipment connected to its networks for the purposes protection against exploitable security vulnerabilities

2.5 Policy Approach

The Unit responsible for ICT –DICTS, has direct responsibility for maintaining and guiding implementation of this policy.

3.0 CYBER SECURITY

3.1 Introduction

Cyber security in this context refers to the protection of university digital infrastructure and information assets against any compromise or attack that may affect its confidentiality, integrity and/ or availability.

3.2 Policy Object

To ensure the protection, resiliency and stability of all University ICT infrastructure, the information held there within and services against any cyber threats.

3.3 Policy Scope

This Policy applies to all University owned ICT infrastructure, digital information and services.

3.4 Policy Statements

3.4.1 General use and ownership policy

3.4.1.1 Roles

a) The Council Committee on Quality Assurance, ICT and Gender (CQAICT) shall:

i. Undertake ownership of all cyber security risks

ii. Provide leadership for the Governance of Cyber security within the University

iii. Articulate the University's information risk appetite

b) The Directorate for ICT Support (DICTS) shall:

i. Ensure that the appropriate security controls and mechanisms have been put in place based on a formal periodic risk assessment;

ii. Maintain an updated ICT risk register in line with the following from the National Information Security Framework

iii. Maintain an updated and tested Business Continuity and Disaster Recovery Plan for all critical University digital infrastructure and information assets

iv. Implement periodic systems and infrastructure audit based on the Plan, Do, Check, Act (PDCA) cycle

v. Maintain updated and documented secure configurations baselines for all hardware and software

vi. Develop and implement a patch management plan

vii. Implement network filtering to protect the network against malware related threats

viii. Ensure the controlled and audited usage of ICT administrative privileges

ix. Implement monitoring and real time analysis of all ICT network device event security logs with a centralized mechanism

x. Ensure the limited and controlled use of network ports and controls

xi. Ensure the implementation of appropriate Wireless Access Provision protection mechanisms

xii. Coordinate and lead the rollout of periodic cross-cutting security awareness and training

xiii. Ensure all ICT equipment is installed with the appropriate active malware protection that is continuously updated

xiv. Develop and maintain a handover mechanism for ICT equipment and information during end of staff employment contracts aligned to the University Human Resource Policy

xv. Secure access to all the university ICT resources and enforce acceptable usage of the same by the deployment of security standards, technologies and best practices.

c) Users shall:

i. Ensure compliance to the cyber security policy

ii. Report any cyber security incident to DICTS

3.4.2 Conditions of Usage

3.4.2.1 Unacceptable Usage

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

a) Sharing of individual access passphrases

b) Usage of any pirated software on University computing devices

c) Usage of any unauthorized peer to peer software

d) Any user action that contravenes the Computer Misuse Act (2011) or the Anti-pornography Act (2014)

e) Any user action that violates the rights of any person or entity's legally registered copyright and/ or Intellectual Property

f) Introduction of any malicious software onto any University computing device or network

g) Any user action that disrupts the normal functioning of any university computing device or network

h) Violations of the rights of any person or company protected by Uganda's copyright, trade mark, patent, or other intellectual property (IP) law and the University's Intellectual Property Policy, other relevant policies, or the University's code of conduct.

i) Any password cracking, software spying, privilege escalation, unauthorized network port scanning and network reconnaissance, network and/or software penetration

j) Usage of university computing devices and/ or network to disrupt an external system or network

k) Usage of university computing devices and/ or network to send out any spam

l) Usage of university computing devices and/ or network for any gambling activity

m) Usage of university computing devices and/ or network for any personal commercial purposes

3.4.2.2 Suspension and/or Termination of Access

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

a) End of student or staff employment tenure

b) Request from University Council, University Management, Heads of Department and/ or University Human Resource Department

c) Occurrence of any of the unacceptable usage restrictions

3.4.3 Bring Your Own Device (BYOD)

The University shall allow the usage of personal devices on the university network as long as such complies with the University policies and offers a similar level of protection as specified by the Unit responsible for ICT. Such usage will be subject to the following:

a) No sensitive or confidential university information shall be stored on such devices

b) The University will provide an acceptable level of protection for such personal devices as defined by the Unit responsible for ICT from time to time;

c) The University shall have the right to investigate/ audit such devices in case of any malicious activity, cybercrime or fraud that affects the University.

d) Registered with DICTS.

3.4.4 Password Policy

3.4.4.1 Rules

a) The Unit responsible for ICT-DICTS, shall define the password strength and lifecycle specification for all user categories from time to time

b) All default system or hardware passwords shall be changed

c) All users shall ensure the privacy of their passwords

d) The Unit responsible for ICT shall implement and maintain centralized authentication, authorization, and accounting service mechanism for all network core equipment to all ICT resources

e) All locally development applications shall support password encryption and user role segregation

3.4.5 Computer Lab Facility Security

Heads of Departments shall ensure that all Computer Lab Facilities are:

a) Compliant to ICT approved baseline setup and configurations

b) Routinely checked for unauthorized connections

c) Accessed only by authorized students and/ or researchers

d) Locked down to prevent physical theft of any component

e) Protected against exposure to water leakages, fire and or dust

f) Located in strongly burglar proofed rooms

g) Labelled according to approved ICT nomenclature

h) Professionally serviced and maintained

3.4.6 Data Center/ Server Room Security

The Unit responsible for ICT shall ensure that Data Center/ Server Room facilities are:

a) Located in secure strong locations away from human or vehicle traffic

b) Fitted with both manual and electronic access control with CCTV monitoring

c) Protected against physical intrusion and exposure to water, dust and fire

d) Protected against power fluctuations

e) Supported by alternate power supply

3.4.7 Access Control

The University shall:

a) Define and periodically review the technology for SMART Access control for different categories to take advantage of new ICT innovations

b) Maintain a smart access control to govern access to all university buildings by both staff, students, visitors and contractors

c) Implement CCTV for access monitoring of all university buildings and entry points

3.5 Policy Approach

The Unit responsible for ICT has direct responsibility for maintaining and guiding implementation of this policy

4.0 SOFTWARE DEVELOPMENT AND ACQUISITION POLICY

4.1 Introduction

The University has over the years been acquiring, developing and making software to support various University functions in an uncoordinated manner. There is therefore need to achieve a defined common methodology for both development and off the shelf software towards achieving improve usage and rationalization of University resources.

This policy assists you in standardizing software development, resulting in better resource utilization, a more consistent outcome and a higher-quality software product delivered to end users.

4.2 Policy Objective

The objective of the policy is to define and implement software development and acquisition methodology to increase efficiency, information assurance, value for university resources and enhance rationalization of ICT.

4.3 Policy Scope

The policy refers to all software used to support university functions with either developed internally (in house or outsourced) or off the shelf software.

4.4 Policy Statements

The following statements govern the implementation of this policy

a) The Unit responsible for ICT-DICTS, shall periodically define the Systems Life Cycle methodology for:

   i. systems and software engineering for both in-house and outsourced development

   ii. acquisition of off the shelf software

    iii. maintenance of software

b) All software shall undergo testing and quality assurance before installation in any production environment within the University and ensure provision for:
    i. Information classification
    ii. Usage of the least privilege principal
    iii. Segregation of roles
    iv. Audit trails

c) All software under this policy shall comply to the Software Licensing and Ownership and Cyber Security Policies

d) All acquired software shall where necessary contain provision for technical support and upgrades

e) All university, Colleges, Departments and units shall where necessary make use of open source software based on a risk based assessment as referenced in the cyber security policy

f) All University Colleges, Departments, Units undertaking the development or acquisition of any software shall ensure compliance to this policy and plan for end user training

g) This policy does not apply to software development within Colleges for academic or educational purposes

4.5 Policy Approach

The Unit responsible for ICT has direct responsibility for maintaining and guiding implementation of this policy.

5.0 ICT SERVICE MANAGEMENT POLICY

5.1 Introduction

The University shall ensure the provision of the ICT Service within the University as well as define a Unit responsible for ICT as the central coordination point of contact for all ICT support. The ICT support shall cater for all areas under the University network, computing devices, hardware, software and implementation of ICT initiatives, projects and programs at all campuses and their related technical support.

5.2 Policy Objective

The objective is to define and implement an effective ICT Service Management and Support approach that is aligned to the Vision of the University Strategic Plan where ICT is identified amongst the key components in the support of the University's goals and objectives.

5.3 Policy Scope

This Policy provides for the centralized management, responsibility and support of all ICT related matters within the University. It's cognizant that the ownership of all University ICT assets is vested with the University Council as referenced in Section 74 (1) of The University and Other Tertiary Institutions Act 2001 (As Amended In, 2003 And As Amended In, 2006).

5.4 Policy Statements

5.4.1 Roles

a) The University shall define and implement an appropriate ICT Service Management process and procedure aligned to the goals and objectives of the University

b) The Unit responsible for ICT shall define and implement a Business Model for the provision of ICT services to external clientele.

c) The unit responsible for ICT shall additionally device a business unit that shall generate resources to improve the welfare of its personnel.

5.4.2 ICT Services Support

The ICT Services Support will be defined as such operations carried out by authorized personnel to ensure efficiency, stability and continuity of any ICT service or equipment to ensure it meets its intended user requirements. In line with this, this policy will apply to all University owned ICT applications and devices.

5.4.2.1 Responsibilities of ICT Services Support personnel

The ICT Services Personnel (system administrators, ICT Lab attendants, ICT technicians, Web administrators) employed by the University within all Departments and Colleges shall functionally report to the Unit responsible for ICT. Accordingly, the University shall provide the necessary work tools, safety gear and training for all ICT services support personnel. Accordingly, such personnel shall:

a) Ensure protection mechanisms exist against ICT devices tampering, alteration or theft;
b) Ensure ICT protection controls exist to safeguard security of systems and information;
c) Provide assistance and guidance towards compliance of ICT policies;
d) Provide technical support in line with approved ICT procedures for any system, service, device downtime or breach;
e) Ensure installation and configuration of all hardware and software is aligned to approved ICT standards;
f) Ensure safe custody and authorized usage of all University software licenses, copyright and usage keys.

5.5 Policy Approach

The Unit responsible for ICT has direct responsibility for maintaining and guiding implementation of this policy.

6.0 ICT SKILLS CAPACITY BUILDING POLICY

6.1 Introduction

The adoption of Information and Communications Technology (ICT) products and tools will require the attendant training to enable effective usage. This requires a dedicated approach within the University to be able to plan for such gaps and develop as well as implement the training as per and when the need arises. This will target all users within the University amongst the staff and student community.

6.2 Policy Objectives

The purpose of the policy is to:

a) Empower the Unit responsible for ICT to:
    i. plan and implement capacity building for ICT skills to achieve coherency and efficient utilization of resources
    ii. undertake capacity building towards improvement of technical capacities of its staff as per and when need arises;

b) Provide for the University Council Committee on Quality Assurance, ICT and Gender to periodically review DICTS staff remuneration to ensure retention and recruitment of qualified staff as aligned to the University Human Resource Policy.

6.3 Policy Scope

This policy applies to all ICT related capacity building that supports the various functions of the University.

6.4 Policy Statements

6.4.1 ICT Capacity Building Assessment

a) The Unit responsible for ICT shall:

   i. Coordinate the periodic assessment of existing ICT skills capacity amongst all user groups to be able to identify gaps in partnership with Heads of Departments

   ii. Undertake a periodic capacity skills assessment to identify knowledge gaps within its technical staff to be able to seek appropriate capacity building programs

b) University Council Committee on Quality Assurance, ICT shall undertake a periodic review of staff remuneration in comparison with market pricing structure for similar roles and personnel.

6.4.2 ICT Capacity building delivery methods

a) The Unit responsible for ICT shall:

   i. Develop Capacity Building modules and courseware for identified ICT skills gaps

   ii. Implement such capacity building with either internal resource personnel or with subject matter experts as per the nature of the required ICT capacity building

   iii. Coordinate the identification of any external expertise for specialized training needs

b) The University shall ensure the presence of well-equipped ICT training computer labs

c) Trainees for such capacity building programs will be identified by the user departments in partnership with Heads of Departments.

6.5 Policy Approach

The Unit responsible for ICT has direct responsibility for maintaining and guiding implementation of this policy in line with the University Human Resource Policy.

7.0 TELECOMMUNICATIONS AND UNIFIED COMMUNICATIONS POLICY

7.1 Introduction

Telecommunications and Unified Communications services will provided to support the communication needs required for the smooth operations of the University amongst all Departments and Colleges. In this context, this will include unified communications services based on the existing University digital network as well as the traditional telephone services.

7.2 Policy Objective

To provide for the use of Unified Communications service alongside the traditional telephony services towards implementation of an ICT enabled communications service aligned towards supporting the University objectives. As such, the policy shall apply to all University Departments and Colleges.

7.3 Policy Scope

This Policy applies to all telecommunications and unified communications service provision that meets that supports the various functions of the University.

7.4 Policy Statements

7.4.1 Roles and Responsibilities

a) The Council Committee on Quality Assurance, ICT and Gender

The Council Committee shall support and promote the usage of Unified Communications service within the university.

b) **The Unit Responsible for ICT**

The Unit responsible for ICT shall:

i. Design and implement the university wide telephony service and numbering plan to support both intercom services and external calls

ii. Design and implement university wide unified communications service to support new communications channels integrated with e-mail, online meetings, video conferencing, workplace collaboration and seamless file sharing

iii. Ensure proper license usage for all unified communications components

iv. Ensure manage and take up responsibility for all infrastructure required to provide a smooth user experience as relates to communications services

v. Provide the required timely technical support through the IT services help desk for all communications related downtime

vi. Approve and provide technical assistance for any expansion of the communications services within the university

vii. Set and periodically review communications services technical specifications (hardware, consumable, software) as well as configuration and installation guidelines to ensure uniformity for the service provision and compatibility with existing infrastructure

viii. Undertake routine maintenance, upgrade and daily monitoring of the communications service usage

ix. Manage and maintain service level agreements will all suppliers of the required communications service, equipment and software

x. Provide technical guidance and authorization in the design and provision of any radio communications service within the University.

7.4.2 Guidelines on Usage

i. All Departments and Colleges will ensure the appropriate protection of desk sets. DICTS will not be responsible for any damaged or stolen desk sets

ii. All Departments and Colleges shall acquire any telecommunications or communications service centrally through guidance from the Unit responsible for ICT

iii. Any configuration change, software upgrade or cabling change will only be undertaken by authorized personnel by the Unit responsible for ICT.

7.5 Policy Approach

The Unit responsible for ICT has direct responsibility for maintaining and guiding implementation of this policy

8. ICT PROCUREMENT POLICY

8.1 Introduction

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

8.2 Policy Objective

To guide the procurement of all University ICT equipment and services towards ensuring standardization of all ICT related assets, transparency, timely delivery, quality assurance, value for money as well as compatibility with existing infrastructure and services.

8.3 Policy Scope

This policy will apply to all University Departments and Colleges at all campuses.

8.4 Policy Statements

8.4.1 Roles and Responsibilities

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

a) Makerere University Procurement and Disposal Unit

   i. Manage all procurement or disposal activities within the Universities in line with the PPDA (Section 31 & 32)

b) User Departments

   i. Ensure conformity with the University Procurement Policy as implemented by the Procurement and Disposal Unit

   ii. Ensure conformity with approved technical guidelines and standards by DICTS in the procurement of any ICT equipment, software or service

c) Unit Responsible for ICT

   The Unit responsible for ICT shall provide technical support to all user departments as provided for below:

i. Technical assistance in the development of specifications for any ICT equipment, software or service

ii. Technical assistance in the identification of user department ICT needs

iii. Ensure and verify that supplied ICT equipment, software or services comply with the approved ICT specifications, standards and guidelines

iv. Ensure that installation and configuration of any procured ICT equipment, software or service complies with the approved ICT specifications, standards and guidelines

v. Maintain an updated inventory of all ICT hardware and software indicating the life cycle

vi. Provide support for bulk procurement of commonly used ICT equipment and software as per business need.

8.4.2 Disposal of ICT equipment and software

a) The University shall define the life cycle for each category of procured ICT equipment to determine the replacement cycle

b) Disposal of retired ICT equipment shall comply with the PPDA

c) Software disposal will rely on the system support cycle of the software developer company.

8.5 Policy Approach

The Unit responsible for ICT has direct responsibility for providing ICT technical advisory support and guidance in the implementation of this policy.

9. SOCIAL MEDIA POLICY

9.1 Introduction

Social media is referred to as any web software that provides electronic social interaction amongst its subscribers and communities.

9.2 Policy Objective

To guide the appropriate usage of social media by Makerere University staff as well as enhance personal and professional reputations online.

9.3 Policy Scope

This policy applies to all University staff and official social media sites.

9.4 Policy Statements

The following statements shall govern both the usage of official university social media sites as well as staff social media activity:

a) University Official Social Media Sites:

   i. Only the university official social media sites will be allowed to make use of university trademarks and symbols

   ii. Only authorized personnel by the University shall be allowed to make postings on the university official social media sites

   iii. Any information shared across the university social media sites shall comply to fair use and comply to University policies in the domains of Conflict of interest and University trademark and symbol protection

   iv. All information shared across the university social media sites should not make reference to any biased statements on matters such as politics, religion, race, gender, sexual orientation, inter alia; statements that contain obscenities or vulgarities

b) All staff social media activity shall:

   i. Respect the Laws relating to copyright and other intellectual property rights, defamation, privacy, and other applicable laws

   ii. Not portray colleagues in an unfavorable light in respect of matters including, but not restricted to, religion, gender, sexual preference, race, nationality or disability

   iii. Maintain adherence to the overall University Confidentiality agreements and information disclosure

   iv. Not make reference to any sensitive staff or student information

c) This policy does not apply to the use of social media for educational purposes as referenced in the University E-learning policy

9.5 Statement of Liability

The University shall not be liable for any errors, omissions, loss or damage, including indirect and/or consequential loss and/or damage claimed or incurred due to any use of any social media site that does not comply with this Policy or the policies cited herein.

9.6 Policy Approach

The University will identify the appropriate unit for maintaining and guiding implementation of this policy.

10.0 SOFTWARE LICENSING AND OWNERSHIP POLICY

10.1 Introduction

All software and its related licenses', copyright, intellectual property and source code used by the University shall be owned as assets of the University.

10.2 Policy Objective

To ensure that all software in use throughout the university is correctly licensed and owned by the University

10.3 Policy Scope

This policy covers all software used within all teaching, learning, research and administration units of the university.

10.4 Policy Statements

The following statements shall govern the software licensing and ownership within the University

a) All heads of units shall ensure that:

  i. An inventory of all software is maintained

  ii. All software is licensed to the responsible University unit as aligned to purchase agreements

  iii. All software in usage is properly managed, administered and maintained

  iv. All software in usage is approved and aligned to the university information security policies

b) Any computing equipment that is written off, sold or given to a third party shall have all non-transferable licensed software permanently removed

c) Staff and students shall not be given the ability to download and install software on university equipment

d) Software shall only be used in accordance with its license and duration

e) Software shall only be distributed in accordance with its license agreement

f) Software licensed for official purposes must not be used on personal computing devices

g) All software source code developed with either internal or external resources for University purposes shall be owned by the University and shall be handled over to DICTS for good custody, backup and patenting.

h) All University Units outsourcing software development that has source code restrictions shall ensure usage of appropriate third party source code escrow agents to ensure continuity

10.5 Policy Approach

The University reserves the right to audit, without prior notice, any ICT equipment connected to its networks for the purposes of software license validation.

The Unit responsible for ICT has direct responsibility for maintaining and guiding implementation of this policy.

11.0 INFORMATION SYSTEMS AND DATA WAREHOUSING POLICY

11.1 Introduction

The University has over the years has been acquiring, developing and making operational different information systems to support the different unit processes and needs. Such systems work in isolation which leads to duplication of data and resources. Data Warehousing will support the harmonization of resources, increase ICT investment value, allow for accurate reporting and enable information/ data consistency.

11.2 Policy Objective

The objective of the policy is to define and implement:

a) Data Warehousing for Makerere University to achieve centralized management of information systems within a central data repository
b) Interoperability between University information systems

11.3 Policy Scope

The policy refers to all existing and future information systems as well as related databases used for University business improved business intelligence and decision making.

11.4 Policy Statements

The following statements govern the implementation of this policy

a) The University shall from time to time define the
   i. appropriate Data Warehousing framework aligned to the Cyber Security Policy
   ii. data management standards
   iii. Interoperability framework for the secure and reliable communication between all University Information Systems
b) All University Colleges, Departments, Units undertaking the development of any information system shall ensure compliance to this policy
c) The University shall ensure the provision of the appropriate ICT infrastructure and capacity for the data warehouse

11.5 Policy Approach

The Unit responsible for ICT has direct responsibility for maintaining and guiding implementation of this policy.

12.0 SPECIAL NEEDS ICT USAGE POLICY

12.1 Introduction

The provision of ICT services should take into consideration the needs of special user groups to enhance teaching and learning. This takes into consideration the visually, motor and auditory impaired user groups. Globally, the development in ICT supports the extension of access to all users.

12.2 Policy Objective

The objective of the policy is to define and implement provisions for ICT usage for special user groups within the teaching, learning and research units of the University towards enabling equal access to information and knowledge.

12.3 Policy Scope

The policy refers to ICT facilities, equipment and services within all the teaching, learning and research units of the University.

12.4 Policy Statements

The following statements govern the implementation of this policy

a) The University shall:

   i. from time to time define the appropriate technology aligned to needs of special user groups

   ii. provide the provision of staff & end user training

   iii. ensure the provision of the appropriate access for special user groups for all University web based systems

   iv. ensure the provision of appropriate digital mechanisms within the Library for special user groups

b) All University Colleges, Departments, Units shall ensure compliance to this policy

c) The University shall ensure the provision of the appropriate access for special user groups for all University web based systems

12.5 Policy Approach

The Unit responsible for ICT has direct responsibility for maintaining and guiding implementation of this policy.

13.0 ICT MAINTENANCE POLICY

The usage of ICT devices within the University will require a well-planned maintenance plan so as to ensure its safe and proper usage. This relies on the cooperation of all units to ensure proper asset and inventory management on which such maintenance can be achieved through a central coordination role.

13.1 Policy Objectives

The purpose of the policy is to ensure that all ICT equipment is regularly maintained to ensure all systems run smoothly with less downtime.

13.2 Policy Scope

This policy applies to all ICT equipment owned by the University within the various units and colleges.

13.3 Policy Statements

13.3.1 Roles and Responsibility

a) The Unit responsible for ICT shall:

  i. From time to time define and disseminate updated ICT equipment maintenance guidelines to all Units and Colleges

  ii. Act as the central point of contact for all University ICT equipment maintenance

  iii. Provide technical support in the development and implementation of service and maintenance schedules for all University ICT equipment

  iv. Undertake a periodic assessment in all Units and Colleges to ensure compliance with the set maintenance guidelines

b) Units and Colleges

  All Units and Colleges within the University shall:

  i. Maintain records of all ICT equipment they acquire including records of manufacturer equipment warranty

  ii. Liaise with the unit responsible for ICT in developing service and maintenance schedules on an annual basis for all ICT equipment

  iii. Maintain good documentation describing the service and maintenance history for all ICT equipment

  iv. Ensure all ICT equipment is placed within adequate operating environments

  v. Ensure all replacements or upgrades of any ICT equipment is undertaken with clearance from the unit responsible for ICT

14.0 STATEMENT OF ENFORCEMENT OF POLICY

a) DICTS shall in partnership with the Committee on Quality Assurance, ICT and Gender be responsible for monitoring the implementation and compliance of these policies and where necessary shall take appropriate remedial measures

b) DICTS will ensure the policies' enforcement and university wide dissemination as well as awareness sensitization of this policy

c) Violations of any the policy areas listed here within shall be addressed by the appropriate University mechanism as guided by the Council Committee on Quality Assurance, ICT and Gender.