MAKERERE UNIVERSITY

INFORMATION AND COMMUNICATION TECHNOLOGY POLICY FRAMEWORK

MARCH 2020

Contents

ABBREVIATIONS AND ACRONYMS

AfDB	African Development Bank
AFRINIC	African Network Information Center
BYOD	Bring Your Own Device
CCTV	Closed Circuit Television
CQAICT	Council Committee on Quality Assurance, ICT and Gender
DICTS	Directorate for ICT Support
DNS	Domain Name Services
HEST	Higher Education Science and Technology
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communications Technology
IP	Internet Protocol
LAN	Local Area Network
MOOCS	Massive Open Online Courses
PDCA	Plan, Do, Check, Act
PPDA	Procurement and Disposal of Public Assets Act
REN	Research Education Networks
RENU	Research and Education Network for Uganda
SIDA	Swedish International Development Corporation Agency
UF	User Forum
WAN	Wide Area Network

FOREWORD

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

In line with the above, the Makerere University ICT Policy Framework provides a structure for all the relevant operational ICT policies to support the achievement of the ICT Vision. Broadly, the policies listed herein 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.

The University Council considered and adopted the Policy and Strategic plan in May 2016. Subsequent to this approval, however, it was observed that there needed to be further stakeholder consultation, especially with regard to how ICT could be harnessed to strengthen and support the University's research agenda. The other reason for the review was to realign the Policy Framework and Strategic Plan, so that they are in agreement, and to bring out clearly the commitment of Makerere University leadership in ensuring ownership and sustainability of the ICT agenda.

To this end, a multi-stakeholder workshop was held in January 2018 and the recommendations from the workshop have informed production of this revised version of the Policy Framework. Further to this, the Strategic Plan has also been realigned with the Revised Policy and an Implementation matrix has been developed to clearly spell out the activities to be implemented, the expected outcomes and the funding required to achieve those outcomes over the policy period.

The University Council is totally committed to the fulfillment of its obligation as spelt out in this ICT Policy Framework and will work with Management to ensure that ICT's become an inseparable part of the culture of doing business in the institution.

Lastly, I wish to acknowledge the efforts of the team that has undertaken this review, led by Prof. Tonny Oyana, the Principal of COCIS, and supported by DICTS and the Chairman of the ICT Committee on QA, ICT and Gender. We all have an obligation to the University to own with this Policy and to champion its full operationalization and implementation.

Chair

Makerere University Council

EXECUTIVE SUMMARY

Currently, Makerere University is one of the leading research driven universities in Africa that has embraced ICT use in its core business processes. In order to remain globally competitive and relevant, Makerere University needs to review its current ICT strategic policy and standardize the ICT operating procedures for enhanced service delivery. To this end, the University initiated a review of its current ICT policy and strategic plan through a number of activities that included multi-stakeholder engagements. The ICT Multi-stakeholder Workshop involving the major University business process owners and key decision makers from Government and civil society was held in January 2018 to validate the policy and set ICT strategic direction for Makerere University.

The overall ICT policy is to enable and facilitate the core functions of Research and Innovations, Teaching and Learning, Knowledge Transfer and Partnerships, Inclusiveness and Gender Mainstreaming, as well as other cross cutting issues. This policy is built around the following five priority thematic areas:

1. **ICT Management and Organizational Context**
2. **Research and Innovations**
3. **Teaching, Learning and Support Services**
4. **ICT Infrastructure**
5. **ICT Inclusiveness and Gender Mainstreaming**

Issues and recommendations highlighted in Situational Analysis call for:

a. Strategic intervention to provide guidance on strategic planning for ICT establishment and maintenance at the University; and

b. Operational intervention to provide guidance to managers at all levels and users on acceptable ICT practices at the University and in the country, in order to minimize risks and enhance sustainability of ICT capabilities of the University.

Accordingly, the MAK ICT Policy is categorized into two namely; MAK ICT Strategic Policy and MAK ICT Operational Policies. In order to facilitate steady growth of the core functions of Makerere University, there is need to articulate strategic focus areas for ICT intervention, such that all ICT investments directly address the hindrances to effective and efficient service delivery in the core functions of Makerere University.

INTRODUCTION

BACKGROUND

ICT is increasingly playing a critical role in enhancing the efficiency of operations in higher institutions of learning. Hence, institutions that have harnessed the potential of ICT have realized significant improvements in efficiency of their business operations.

The Uganda Vision 2040 recognizes the role of ICT in enhancing learning and preparing citizens that are equipped with ICT skills that are responsive to national and global needs. In addition, the National Development Plan 2015/16-2019/20 (NDPII) identifies ICT as one of its primary growth enablers of economic and social transformation. The National ICT policy 2015/16-2019/2020 also emphasizes the need of integrating ICTs in the teaching and learning, as well as the research and innovations processes of higher institutions of education.

In support of this national agenda the ICT support function of Makerere University has been guided by a set of three ICT policies since 2001: the ICT policy and Master plans 2001-2004; 2005-2009 and 2010-2014. Evidently, there has been a regular review of the policies in cognizance of the rapidly emerging technological trends and changing environments. This has impacted on the ability of ICT to effectively support the core business functions of the University. Makerere University aims to provide innovative teaching, learning, research and services responsive to national and global needs. To achieve this, there is a need to review and realign the Makerere ICT policy with the University business functions and the University Strategic plan.

Therefore, the purpose of this document is to describe the ICT strategic policy direction as well as the operational policies and standard procedures/guidelines that will support Makerere University goals and objectives. This will help improve effectiveness and efficiency in all University functions.

MAKERERE UNIVERSITY ICT GOALS & OBJECTIVES

Vision statement

"… **University-wide access to, and utilization of information and communication technology** to enhance the position of Makerere University as a leader of academic excellence and Innovations, and its contribution to the sustainable development of society."

Mission statement

To leverage ICT as a key enabler for the establishment of a conducive environment to support the effective and efficient operations of the teaching, learning, administration and research domain areas of the University.

Objectives

The broad objectives of this strategic plan are to:
  a) Enhance research and innovation using ICT as an Enabler;
  b) Integrate ICT within teaching and learning;
  c) Improve web management and engagement;
  d) Adopt University Administrative Information Systems;
  e) Build robust ICT digital infrastructure;
  f) Enhance Information Assurance;
  g) Achieve efficient ICT Service Provision.

GOVERNANCE

Governance Framework

The continued adoption and utilization of ICT within Makerere University will gradually lead to the reliance on the well- functioning of ICT for its continued operations as well as survivability. As such, it is important to ensure that all ICT initiatives are aligned to the goals of the university in order to guide strategic investment. Achieving this requires collaboration amongst all key stakeholders as well as support from the highest level of Governance within the University straight from development of this strategy to approval, implementation and monitoring. Collaborations with the right strategic external partners likewise introduce opportunities for growth and innovation towards creating a positive impact. Whereas the implementation of this strategy is achieved through the Directorate of ICT Support, the strategy requires identification of various stakeholder roles to guide harmonious collaboration. To this end, the following have been identified:

The Council ICT, Quality Assurance and Gender Committee
The Council ICT, Quality Assurance and Gender Committee has representation from University Senate as well as representatives from relevant Government Ministries. The Committee shall:
a) Oversee, champion and monitor the implementation of the ICT Policy and Strategic Plan;
b) Coordinate with the Council Committee on Finance and Administration to ensure adequate budgetary allocation to facilitate implementation of the ICT Strategic Plan.

Directorate of ICT Support
The Directorate of ICT Support (DICTS) shall perform the roles and act as the focal point of contact for the ICT Service Management function within the University.
a) Define Service Level Management for the provision of ICT services;
b) Coordinate the operational implementation of the ICT Strategy and ICT Policy Framework; and
c) Coordinate all ICT related activities within the University.

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 areas. 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 IT Service Provision.

Heads of Teaching, Learning, Administration and Research Domain Areas
The Principals/ Heads of Departments shall:
a) Integrate ICTs into their activities;
b) Implement the unit specific component of the ICT Strategy;

c) Ensure compliance to the ICT Policy Framework, including Plagiarism control; and
d) Act as active participants during the periodic stakeholder consultations towards supporting and facilitating the effective implementation of the ICT Strategy.

Staff and Student Community

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

SITUATIONAL ANALYSIS

Currently, Makerere University is one of the leading research driven universities in Africa that has **embraced ICT use in its core business processes**. In order to remain globally competitive and relevant, Makerere University needs to review its current ICT strategic policy and standardize the ICT operating procedures for enhanced service delivery. To this end, the University initiated a review of its current ICT policy and strategic plan through a number of activities that included multi-stakeholder engagements. These provided an overview of the ICT policy gaps and challenges that need to be addressed in the following priority thematic areas:

- ICT Management and Organizational Context
- Research and Innovations
- Teaching, Learning and Support Services
- ICT Infrastructure
- ICT Inclusiveness and Gender Mainstreaming

The multi stakeholder engagements were guided by recommendations from the following reports:

1. The Uganda Vision 2040
2. The National Development plan II
3. The National ICT Policy
4. The Makerere University Strategic Plan 2008/09-2018/19
5. The current Makerere University ICT Policy
6. The current ICT Strategic Plan 2016-2021
7. SIDA ICT assessment report 2015
8. Rapid ICT assessment report 2017 (Tusu-report)
9. Management Response to the embassy 2017
10. Visitation Committee recommendations on ICT services.

Findings and recommendations from the multi-stakeholder engagements are summarized in tables 1 to 5 with respect to the priority thematic areas.

Table 1: ICT Management and Organizational Context

Identified Challenges and Gaps	Recommendations for inclusion in the ICT policy and/or the ICT Strategic Plan
- Inadequate ICT governance structure - Lack of ownership and sustainability of ICT interventions	Establish a Vice Chancellor ICT level committee to guide management on ICT policy implementation, ownership and sustainability; and clearly specify its roles

Identified Challenges and Gaps	Recommendations for inclusion in the ICT policy and/or the ICT Strategic Plan
• DICTS mandate is not fully exercised	• Empower DICTS to fully exercise its mandate through adequate resource allocation to ICT services • Fill staffing structures at DICTS, colleges and other units; and develop their ICT capacity. • Enforce an appropriate sharing formula of resources for ICT sustainability with emphasis to supporting research and innovations.
• Misalignment of the National ICT policy and Makerere ICT policy framework	• Ensure alignment of Government/National ICT policy and Makerere ICT policy framework.
• Lack of compliance and adherence to ICT operational standards	• Identify best practices and ICT operational standards among peer universities • Establish ICT operational standards and enforce compliance to these standards.

Table 2: Research and Innovations

Identified Challenges and Gaps	Recommendations for inclusion in the ICT policy and/or the ICT Strategic Plan
• The lack of a clear definition of the gender mainstreaming terrain across the university in relation to ICT and the research/learning environment	• Engender the ICT policy on all services, systems and infrastructure including the concerns of persons with special needs.
• Limited internet access and low bandwidth for research and learning. • Network infrastructure can't support the transfer, publishing and sharing of large datasets, tutorials, video and web-conferencing, You-tube and other related services among users. This is a barrier to collaborative research and learning.	• Ensure alignment of the ICT policies to support all selected/prioritized avenues of research and learning at the University. • Define policies that will facilitate ICT-enabled research collaborations with Government, industry or private sector and other high-educational institutions. • Explore mechanisms of fully utilizing research educational networks (RENs) such as RENU that offer subsidized bandwidth for research entities, so as to provide a reliable platform for research collaboration between Makerere and other institutions.
• Lack of a clear institutional mechanism/framework for management of research data to provide guidance on ownership,	• Develop a policy on the management of research data and accommodate all aspects associated with ownership, storage, and sharing/dissemination of ICT resources; Open

storage and sharing/dissemination of research resources and ICT resources in the university.	Data Access (ODA); and Intellectual Property Rights (IPR) • Develop an integrated university-wide ICT platform for managing data on research initiatives in the University. • Clearly define minimum ICT skills requirements for the different user-groups in the policy document.
• Lack of knowledge on the computing resources needed by researchers.	• Devise a mechanism for addressing ICT training needs for all categories of users (researchers, students, lecturers, administrators and ICT personnel) in the ICT policy and strategic plan.
• There is lack of access to basic computing equipment.	• Devise a prioritize mechanism that will address the requirement for end-user access to basic computing resources as well as their maintenance and sustainability beyond donor support.

Table 3: Teaching, Learning and the Support Environment

Identified Challenges and Gaps	Recommendations for inclusion in the ICT policy and/or the ICT Strategic Plan
• There is a relaxed mechanism of adopting MUELE as the university's collaborative e-learning platform in all schools and colleges, since some schools or lecturers are enthusiastic about the use of MUELE yet others hardly endeavor to adopt it. • Limited basic literacy on developing digital or e-learning content, which results in the relaxed mode of adoption of e-learning content among lecturers. • Limited literacy on using e-learning and e-library resources.	• Develop and establish a mechanism of enforcing adoption of MUELE as a pedagogical environment to enable a vibrant, active and collaborative learning environment. • Upgrade the mandatory faculty pedagogical training course that is to be rolled out to all University staff (especially those that have no pedagogical background) to include: (a) emerging e-learning technologies as a crucial component; and (b) basic digital literacy and e-learning content development as training solutions so as to enhance e-learning adoption. • Conduct ICT training for all categories of users, i.e. all students and all staff categories (support, administrative, and academic).
• There are hardly incentives for developing e-learning content, yet the procedure is time consuming; copyright aspects associated with it are implicit; and it is quite demanding to	• Develop a policy (as part of the overall University ICT policy) to provide guidance on aspects associated with developing and maintaining e-learning content to address pedagogical content and instructors' course

Identified Challenges and Gaps	Recommendations for inclusion in the ICT policy and/or the ICT Strategic Plan
maintain an active and collaborative e-learning profile for a specific course unit.	design, ownership, and sharing of electronic content for learning as well as MOOCs.
• The current mechanism for assessing the learning environment in the university (including course units and lecturers) is not comprehensive enough, since few students participate in the process and the sampling approach used to select those who participate in the evaluation is not appropriate.	• Develop a digital or online or e-assessment tool as a support system to MUELE, so as to allow all students to appropriately assess the learning environment of the University (including course units and lecturers or educators) to ensure that quality learning and education services are provided.
• Limited connectivity issues within the university and limited access to online resources that the university has subscribed to.	• Establish technological spaces that can promote active and student-centered learning strategies. • Devise mechanisms of increasing accessibility to online resources and increasing connectivity (regardless of location) in order to promote mobile learning, distance learning, and research. • Establish a Bring Your Own Device (BOYD) policy to encourage and accommodate users who access university e-learning resources and electronic databases using their personal devices. • Explore mechanisms of availing international roaming services such as "eduroam" to all staff and students.
• Lack of a reliable university-wide integrated repository for research projects, dissertations, and theses for students that can be accessed by all authorized staff and students in order to guard against plagiarism of research and other assignments.	• Engage with the library ICT team so as to ensure that planned ICT initiatives to support research are interoperable and coherent with the ongoing e-library initiative and are in line with the library resources policy that is being developed, so as to increase accessibility to e-learning resources.

Table 4: ICT Infrastructure

Identified Challenges and Gaps	Recommendations for inclusion in the ICT policy and/or the ICT Strategic Plan
• The ICT backbone and end-user access infrastructure is obsolete, since approximately 90% of the switching devices are obsolete as networks and core switches were procured before 2008.	• Develop a clear policy on the review and assessment of ICT infrastructure. • Develop and implement an ICT Infrastructure sustainability plan for the University beyond 2021.

- Lack of a plan to guide prioritization of University-wide ICT infrastructure upgrades, replacement and procurement etc.
- The University ICT-Infrastructure is inadequately secured (in terms of hardware, software and related platforms).
- There are no guidelines for determining the kind of end-user equipment needed for optimal performance and service delivery.
- SIDA does not fund basic ICT infrastructure and further guidance is needed on the sharing formula for resources and technology fee to support Research and Education.

- Develop a clear maintenance and sustainability policy for university ICT infrastructure.
- Develop a capacity development programme for both users and technical ICT personnel
- Incorporate penalties for incidents of service breach in all ICT policies
- Develop a clear policy on minimum ICT competence levels for different user groups (researchers, students, lecturers and administrators).
- Develop a shared data repository and computational centre to support teaching and learning, research and innovations and knowledge transfer.
- Perform service usage assessment for different user groups to determine the kind of end-user equipment needed for optimal performance and service delivery.
- Review and update the business continuity and disaster recovery plan for all ICT services.
- Develop a clear sharing formula for the technology fee and other resources to support Research and Education.

Table 5: ICT Inclusiveness and Gender Mainstreaming

Identified Challenges and Gaps	Recommendations for inclusion in the ICT policy and/or the ICT Strategic Plan
	• Reinstate the University Gender Mainstreaming committee (as stipulated in the Makerere University Gender Equality policy) and ensure that its members and its representatives of Council, ICT, and Quality Assurance are skilled in gender inclusive strategies.
• The University ICT Infrastructure and services are not gender inclusive, since they are not tailored enough to accommodate critical special needs of particular groups.	• Use existing ICT platforms and engage the University Gender Equality team to conduct a comprehensive situational analysis on the gender terrain at Makerere University so as to ascertain priority areas of inclusion, such that an intersectional approach is used in developing all ICT infrastructure and services to accommodate concerns of persons with special needs and issues related to gender mainstreaming.

- Coordinate all key stakeholders to develop a mandatory course on ICT for gender and special needs inclusiveness, and ensure that all categories of staff and students undertake training in this course.

Table 6: SWOT Analysis

Strengths	Weaknesses
• Strong partnership with other universities. • A nucleus of adaptive and skilled personnel. • Versatile and robust ICT infrastructure. • Departmental ICT labs • Abundant supply of bandwidth from RENU. • Strong support of ICT at Council level and Executive Management • Strong student commitment for ICT utilization. • Reputation as the oldest University and well established institution in the country and region. • Reliable backbone infrastructure. • Existence of ICT structure - DICTS • Existing enterprise systems (Libhub, etc.)	• Inadequate access to latest ICT equipment. • Inadequate staff to support ICT. • Inadequate backup facilities for Business continuity and Disaster Recovery. • Unreliable power supply. • Lack of external training in emerging technologies. • Ineffective University-private sector interactions or partnerships. • Standalone ICT systems that are not linked.
Opportunities	**Threats**
• Student partnership support – ICT fee. • Presence of Alumni network. • Support from Government programmes (HEST) and Education Development partners (SIDA, AfDB, etc.) • International linkages and collaborations. • Improved communication services. • Proliferation of mobile devices • Emerging innovation hubs within the University.	• Unreliable power supply. • Expanding student demands for ICT. • Inadequate and aging equipment in ICT labs. • Increased competition from many private Universities (e.g. those that offer a laptop per student) • ICT Network not well secured.

- Rollout of Academic Information Management System (AIMS) in pipeline.

RATIONALE FOR THE MAKERERE UNIVERSITY ICT POLICY

The overall ICT policy is to enable and facilitate the core functions of Research and Innovations, Teaching and Learning, Knowledge Transfer and Partnerships, Inclusiveness and Gender Mainstreaming, as well as other cross cutting issues. This policy is built around five thematic areas highlighted in the Situational Analysis. Three of the thematic areas (i.e. ICT Management and Organizational Context, ICT Infrastructure, and ICT Inclusiveness and Gender Mainstreaming) because of their relevance in enhancing service delivery towards achieving academic and research excellence in Makerere University.

Issues and recommendations highlighted in Situational Analysis call for:
   A. Strategic intervention to provide guidance on strategic planning for ICT establishment and maintenance at the University; and
   B. Operational intervention to provide guidance to managers at all levels and users on acceptable ICT practices at the University and in the country, in order to minimize risks and enhance sustainability of ICT capabilities of the University.

Accordingly, this MAK ICT Policy is categorized into two:
   A. MAK ICT Strategic Policy – presented in the next section
   B. MAK ICT Operational Policies – presented in sections 1 to 15

MAK ICT STRATEGIC POLICY

In order to facilitate steady growth of the core functions of Makerere University, there is need to articulate strategic focus areas for ICT intervention, such that all ICT investments directly address the hindrances to effective and efficient service delivery in the core functions of Makerere University. Thus, the strategic focus areas are articulated below and categorized according to the five thematic areas of this policy.

ICT Management and Organizational Context

The major barrier to effective and efficient business-IT alignment at Makerere University is the relaxed ICT governance structure and operational mechanism, which has greatly impacted compliance and adherence to desired ICT practices at institutional and national level. Thus, the need to strengthen ownership and sustainability of ICT interventions. To address this gap, MAK shall:

Strategic Focus Areas for ICT Management and Organizational Context
   a) Standardize ICT operations or practices across all units in the University, so as to achieve a more dynamic and efficient ICT management and organisational functionality;
   b) Establish a Vice Chancellor ICT level committee with clearly defined roles to guide management on ICT policy implementation, ownership and sustainability;

c) Strengthen the capabilities of ICT across the University to support intellectual, social and community engagement;
d) Enhance alignment of business processes with ICT's to enable swiftness;
e) Consolidate and integrate current platforms to provide consistency of user experience;
f) Provide an uncomplicated and consistent experience for users;
g) Provide opportunities to develop practical skills in the workplace; and
h) Develop and maintain ICT operational policies to streamline and standardize business-IT alignment aspects in the University.

Research and Innovations

Makerere University ICT policies are not aligned to support all selected/prioritized avenues of research and learning to enable her realize the vision of academic and research excellence. The University also lacks a university-wide integrated research data repository or management framework and has limited access to Internet, basic computing equipment, adequate bandwidth, and computing resources for enabling a real-time collaborative and multidisciplinary research environment that delivers working solutions to societal/community and organizational problems in the country. Therefore, MAK shall:

Strategic Focus Areas for Research and Innovations
a) Provide a flexible and secure ICT infrastructure and an Information System framework to support and sustain an excellent research base at the University, so that institutional requirements and aspirations can be met;
b) Align ICT policies to support all selected/prioritized avenues of research and learning to enable the University realize its vision of academic and research excellence;
c) Define policies that will facilitate ICT-enabled research collaborations with Government, industry or private sector and other high-educational institutions in Uganda;
d) Support the research community by providing technical support and guidance to different categories of users, drawing upon international research networks and funder requirements, and working with others to apply these throughout the research lifecycle;
e) Engage the research community to increase awareness about significant developments in ICT, information processing and governance that could support and enhance research activities and innovations.

Teaching, Learning and Supporting Environment

The University has a flexible framework for establishing a Learning Management System and other educational technologies that enable a reliable and agile teaching and learning environment for equipping students with knowledge and practical skills relevant to address contemporary issues in society and enterprises. To curb this, MAK shall:

Strategic Focus Areas for Teaching and Learning Environment
   a) Ensure that the University ICT infrastructure is agile and capable of swift change so that future requirements of the University and those of individual learners can be met with minimal impact;
   b) Facilitate seamless communication in support of learning and teaching;
   c) Identify and bring to the University's attention technological innovations that could enhance the learning experience; and
   d) Engage with academic staff and students to understand learner needs.

ICT Infrastructure

The University's ICT backbone and end-user access infrastructure is obsolete and inadequately secured, yet there is no guideline for determining infrastructure requirements for optimal performance and service delivery; and no plan to guide prioritization of infrastructure maintenance. To overcome this, MAK shall:

Strategic Focus Areas for ICT Infrastructure
   a) Provide the technology, infrastructure and expertise to enable University staff and those engaged by IT Services to be effective in their jobs;
   b) Contribute to the effective operations of the University through the appropriate deployment of technologies to enable business change and drive efficiencies;
   c) Provide an ICT and information management infrastructure to fully support existing and future requirements;
   d) Provide an effective and trusted infrastructure for an integrated management information system that allows business units to collect and process information in line with their strategic and operational requirements; and
   e) Ensure that confidentiality, reliability and availability of information systems and the information held and/or processed by those systems are protected and maintained.

ICT Inclusiveness and Gender Mainstreaming

The University ICT Infrastructure and services are not inclusive because they are not tailored to accommodate critical special needs of particular groups. Thus, there is need for a clear definition of the gender mainstreaming terrain across the university in relation to ICT, which can inform the shaping of ICT infrastructure and services. To attain this, MAK shall:

Strategic Focus Areas for ICT Inclusiveness and Gender Mainstreaming
   a) Conduct a comprehensive situational analysis on the gender terrain to ascertain priority areas of inclusion, such that an intersectional approach is used in developing all ICT infrastructure and services to accommodate concerns of persons with special needs and issues related to gender mainstreaming; and
   b) Establish a reliable and accommodative feedback and control mechanism for managing ICT concerns associated with inclusiveness and gender mainstreaming.

MAK ICT OPERATIONAL POLICIES

To address the gaps in the five thematic areas and achieve the recommendations arising from the Situational Analysis, there is a need to harmonize and standardize ICT operational practices across all Colleges and Units to accomplish the core functions of the University. To this end, efforts were made to assess existing operational challenges; explore best practices through benchmarking with peer universities; evaluate changing business environment and emerging technology trends; and adopt recommendations from the multi-stakeholder review workshop. For example; under operational challenges, it was observed that there is: inadequate articulation of ICT at all management levels; limited appreciation of the importance of ICT amongst users; and inadequate resource allocation, including financing and human resources.

At a national level there is a National ICT Policy Framework. It is important to align and adapt current national ICT policies to accommodate existing institutional ICT gaps, opportunities and challenges at Makerere University. At University level some policies exist (such as the Acceptable Use of ICT Resources Policy, Data Security Policy, Web-Content Publishing Policy, among others) that need to be reviewed and aligned to the National ICT Policy Framework. This will further strengthen and standardize ICT operations in the five thematic areas:

1. **ICT Management and Organizational Context**
    a. ICT Governance
    b. ICT Service Management and Support
    c. Information Systems and Data Management
    d. Cyber Security
    e. Software Development, Acquisition, Ownership and Licensing
    f. ICT Procurement
2. **Research and Innovations**
    a. ICT Support to Research
    b. High Performance Computing
    c. Social Media
3. **Teaching and Learning and Support Environment**
    a. ICT Skills Capacity Building
    b. Multimedia Instructional Technology and Management
    c. Social Media Usage
4. **ICT Infrastructure**
    a. E-learning support infrastructure and instructional technology
    b. University Data Communications
    c. Telecommunications and Unified Communications
    d. Specialized equipment
5. **ICT Inclusiveness and Gender Mainstreaming**
    a. 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 Vice Chancellor Level committee

The Vice Chancellor level committee shall:

a) Be led by the chairperson Makerere University Council and will take ownership of University ICT policy Framework and Strategic Plan.

b) Advise and guide management and Makerere university council on the implementation of the ICT strategic Plan of the University.

c) Work in conjunction with the already established council committee on Quality Assurance, ICT and Gender in expediting its mandate.

d) Provide a clear sharing formula for the technology fee, especially direct investment in research and education.

1.4.2 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

     iii.   With the guidance of DICTS develop and implement an ICT Infrastructure sustainability plan for the University.

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.

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

1.4.4 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.

1.4.5 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:
- ICT Infrastructure Rollout
- Digital network
- University Wide Area Network
- Campus Local Area Networks (LANs)
- MAK Wireless Access provision
- Remote Access
- 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 periodically perform University-wide ICT infrastructure capacity planning for both core and access/end-user equipment.

(b) 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;

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

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

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

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

(g) 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) Controlled and Designated Wireless Access Points shall be set up 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:

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

    b. 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.

2.4.10 E-Learning Infrastructure support
2.4.10.1 Definition
This refers to the provision of hardware and Electronic content management platforms that enable electronic learning and access to educational data over the University network.

2.4.10.2   E-Learning Infrastructure
The Unit responsible for ICT shall;

a) Define and implement the underlying E-Learning Infrastructure (hardware and electronic content management platform technologies) in support of E-Learning.

b) Provide a Learning Management System that enables the provision of Massive Open Online Courses (MOOCS).

c) Define and implement access guidelines and procedures to the E-Learning content management platform for different categories of users including those with special needs.

d) Define and implement a clear BOYD policy for mobile devices accessing institutional E-Learning content both on and off the University network.

e) Acquire or develop digital tools for assessing the responsiveness and usability of the electronic learning environment.

f) Establish technological spaces designed to promote active and student centered learning strategies.

g) In conjunction with the Department of distance and lifelong learning, introduce mandatory basic digital literacy training for all faculty and students across board irrespective of their training background.

h) Provide secure, wired and wireless access to authorized users of the E-Learning platform.

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 improved 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 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 Directorate for ICT Support shall periodically perform service usage assessment for different user groups to determine the kind of end-user equipment needed for optimal performance.
c) The Unit responsible for ICT shall define and implement a Business Model for the provision of ICT services to external clientele.
d) 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.

M

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) Set minimum ICT skills requirements for the different user groups (students, lecturers and administrative staff) for utilization of University ICT services and systems.

   c) 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 & 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 and 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 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 with 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 with fair use and comply with 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 MANAGEMENT POLICY

11.1 Introduction

The University has over the years 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 Management 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 Management 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 Management 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) A clear needs assessment following approved guidelines from DICTS must be undertaken before any University system is implemented.
  c) All University Colleges, Departments, Units undertaking the development of any information system shall ensure compliance to this policy.
  d) 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 for special needs user groups.
    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.
    v. Periodically undertake a situational analysis of the gender terrain at the University to ascertain areas lacking ICT inclusiveness for special needs 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 ICT SUPPORT TO RESEARCH POLICY

ICT services shall enable the research and learning environment through the provision of a complete E-learning system (Hardware and E-Learning platform), Research management system and E-Library services.

14.1 Policy Objectives

The purpose of the policy is to ensure that ICT services enable the research and learning environment within the University.

14.2 Policy Scope

This policy applies to all ICT equipment and services owned by the University.

14.3 Policy Statements
14.3.1 Roles and Responsibility

a) The Unit responsible for ICT shall:
i. Provide technical support in the development and implementation of systems and services that support research and learning within the University; E-Learning platform, Research management system and E-Library services.
ii. Enable research collaboration through network level interlinks with Government, Industry and other research institutions at subsidized rates through a Research Education Network service (REN).
iii. With guidance from the Directorate of Research and Graduate Training (DGRT) provide electronic research data management guidelines and procedures pertaining to the transmission, sharing and storage of electronic research data over the University network.
iv. Enable research and learning through the provision of stable wired and wireless internet access to all categories of researchers (students and lecturers).
v. Enable research and learning through the provision of access equipment (computers) for all categories of learners including those with special needs.
vi. Periodically assess the functionality and quality of end-user access equipment and make necessary changes where need be.

15.0 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 of 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.