KABALE UNIVERSITY

INFORMATION AND COMMUNICATIONS TECHNOLOGY SERVICES POLICY

February, 2020

ACRONYMS

BOYD	Bring Your Own Device
COBIT	Control Objectives for Information and related Technology
DICTS	Directorate of Information and Communications Technology Services
ICT	Information and Communication Technology
ISO	International Standards Organization
IT	Information Technology
LAN	Local Area Network
VLAN	Virtual Local Area Network
PPDA	Public Procurement and Disposal of Assets
RAS	Remote Access System
ToR	Terms of Reference
KAB	Kabale University
VPN	Virtual Private Network
WAN	Wide Area Network
ISP	Internet service Provider
EMIS	Electronic Management Information System
IFMIS	Integrated Financial Management Information System
FMIS	Financial Management Information System
LIS	Library Information Systems
HRIS	Human Resource Information System
AIMS	Academic Information Management System
COBIT	Control Objectives for Information and Related Technologies
SOP	Secure Operation

TABLE OF CONTENTS

ACRONYMS i

1.1.1 Introduction and Background 5

1.1.2 ICT Policy Statement; 2

1.1.3 ICT Service Mission: 2

1.1.4 Application of policy 2

1.1.5 Administration of the Policy 2

1.1.6 Breach of Policy 2

1.1.7 Revision of Policy 2

1.1.8 Scope of the Policy: 2

1.1.9 ICT CORPORATE GOVERNANCE 3

1.1.10 Introduction 3

1.1.11 Objectives 3

1.1.12 ICT Governance Structure 4

1.1.13 ICT Governance Committees and roles 4

a) ICT and Library Committee of Senate 4

b) Finance, Planning and Resource Mobilization Committee 4

c) Audit and Risk Management Committee 5

1.1.14 Roles and Responsibilities of DICTS 6

1.1.15 DICTS Resource Mobilization 6

1.1.16 ICT CAPACITY BUILDING 7

1.1.17 Objective 7

1.1.18 Skills Training Guidelines 7

1.1.19 ICT Policy Awareness 7

1.1.20 Role of DICTS 7

1.1.21 ICT OPERATIONS AND MANAGEMENT 7

1.1.22 Objective 7

1.1.23 Acceptable Use of ICT Resources 7

1.1.24 Procurement and Disposal of University ICT Assets 8

1.1.25 Printing and Photocopying 9

1.1.26 ICT Equipment Servicing, Maintenance, and Repair 9
1.1.27 Computer and Laptop Allocation 9
1.1.28 Computer Laboratory Management 9
1.1.29 Logging and Monitoring 10
1.1.30 Attendance Management 11
1.1.31 Projector use Procedure 11
1.1.32 ICT usage by Persons with Disability 12
1.1.33 ICT Asset Management 12
1.1.34 NETWORK AND COMMUNICATIONS 12
1.1.35 Local Area Network (LAN) and Wide Area Network (WAN) 12
1.1.36 Network Connection 13
1.1.37 Network Password Management 14
1.1.38 Website Management 14
1.1.39 Social Media Management 14
1.1.40 Office Telephone Sets and Intercom Usage 14
1.1.41 Email Usage and Management 15
1.1.42 Video Conferencing and Unified Communication Services 16
1.1.43 SOFTWARE AND INFORMATION SYSTEMS 16
1.1.44 Objective 16
1.1.45 Core Infrastructure Systems 16
1.1.46 Roles and responsibilities towards an Integrated MIS 16
1.1.47 Professional Software Specific for Directorates and Faculties 17
1.1.48 Integrated Financial and Academic Information Management Systems (IFAIMS) 17
1.1.49 E-LEARNING 17
1.2.0 Objective 17
1.2.1 E-learning Implementation 17
1.2.2 Laptop Scheme 18
1.2.3 ICT SECURITY 18
1.2.4 Objective 18
1.2.5 Protection of University Confidential Data 18
1.2.6 Internal Organization 18
1.2.7 Security of Mobile Devices e.g. Laptops 19

1.2.8 Human Resource Security 19
1.2.9 Access Control 19
1.2.10 Cryptographic Controls 20
1.2.11 Physical and Environmental Security 20
1.2.12 Operational Security 21
1.2.13 Communication Security 22
1.2.14 Anti-Virus and Open Source Software Installations 22
1.2.15 Security Incidence Management 22
1.2.16 ICT DATA BACKUP AND ARCHIVING 23
1.2.17 Objective 23
1.2.18 Data Backup Standards 23
1.2.19 Data Backup Selection 23
1.2.20 Backup Types 23
1.2.21 Backup Procedure 24
1.2.22 Backup Owner 24
1.2.23 Offsite Storage 24
1.2.24 Data Archiving 24
1.2.25 ICT RESEARCH AND INNOVATION 24
1.2.26 Objective 24
1.2.27 Information Technology Transfer 25
1.2.28 Role of DICTS 25
1.2.29 ICT CONSULTANCY 25
1.2.30 Objective 25
1.2.31 Consultancy Services 25
1.2.32 Role of DICTS 25
1.2.33 ICT COMMUNITY OUTREACH 26
1.2.34 Objective 26
1.2.35 ICT Out Reach Services 26
1.2.36 Role of DICTS 26
1.2.37 REFERENCES 26
1.2.38 Appendix A 28

1.1.1 Introduction and Background

Uganda has an elaborate legal and institutional framework for guiding the ICT sector. Over time, a number of policies and laws have been put in place. Examples include: The National Information Technology Policy (2011); The National e-Government Policy Framework (2011); The National Postal Policy (2012); The Analogue to Digital Migration Policy (2011); The National E-waste Management Policy (2012); The National County Code Top Level Domain Policy (2013); The National Information Technology Authority Act (2009) which led to the creation of the National Information Technology Authority – Uganda (NITA-U); The Uganda Communications Act (2013); and The Cyber Laws (Computer Misuse Act (2011), Electronic Signatures Act (2011) and Electronic Transactions Act (2011). In terms of ICT governance specifically, Uganda has several other laws and policies governing ICT, with many of them applicable to ICT in governance. These include the Uganda Communications Act, 2013, the NITA-U Act, 2009, the Computer Misuse Act 2011, Electronic Transactions Act 2011 and the Electronic Signatures Act 2011.17 Others are the Regulation of Interception of Communications Act, 2010, the Anti- Terrorism Act, 2002, and the Access to Information Act, 2005. The policies include the National ICT Policy, 2013, the Rural Communications Development Fund, 2015, National Electronic Government Policy Framework of 2010 and the Information Management Services Policy. As a Public University, Kabale engages in teaching and research of ICT but also uses ICT services in its operations with government. The purpose of this Policy therefore, is to describe and document the ICT policy and procedures that will support Kabale University goals and objectives within all teaching, learning, research, and administrative units. This is purposely geared towards increasing effectiveness and efficiency in all University functions. As such, the development of this policy took into consideration alignment to other University functional policies as well as globally recognized ICT best practices. The University will accordingly ensure the wide dissemination of this Policy to all the user group categories. The Policy will be reviewed periodically to ensure its relevance and alignment to the University goals, and emerging technological trends.

Kabale University recognizes the important role ICT plays in education and will therefore; incorporate it in all its activities. The University adopted ICT as a tool to coordinate administrative activities, enhance learning and teaching and support research.

1.1.2 ICT Policy Statement

ICT as an enhancement to educational excellence for Kabale University.

1.1.3 ICT Service Mission:

To electronically operate extensively academic and administrative activities of the University.

1.1.4 Application of Policy

The policy applies to all users of Kabale University ICT Services. These include: members of Council, Staff, Students, Contractors, Service Providers, Suppliers, Consultants, Researchers, Partners, and any other members of the Community engaged in official University activities.

1.1.5 Administration of the Policy

The Directorate of ICT Technical Services shall be responsible for implementing this policy.

1.1.6 Breach of Policy

Any failure to comply with the policy framework set out herein will be regarded as misconduct and violation of the policy. Any person violating this policy, shall be subjected to the appropriate University disciplinary mechanism and /or laws of Uganda.

1.1.7 Revision of Policy

Revision of the policy shall be after every five years.

1.1.8 Scope of the Policy

The policy covers different sections of the University; each allocated specific regulation(s). These include the following;

a) ICT Corporate Governance
b) ICT Capacity Building
c) ICT Operations and Management
d) Networks and Communications
e) Software and Information Systems
f) Electronic -Learning
g) ICT Security

h) ICT Data Backup and Archiving
i) ICT Research and Innovation
j) ICT Consultancy
k) ICT Community Outreach

1.1.9 ICT CORPORATE GOVERNANCE

1.1.10 Introduction

Information and Communications Technology (ICT) Corporate Governance is the effective and efficient management of ICT resources to facilitate the achievement of organizational goals and objectives. ICT does not exist for its own sake within Kabale University; it is there to ensure Kabale University achieves sustainable success through use of it. The University shall adopt the corporate governance of ICT framework under international agreed standards developed by COBIT.

1.1.11 Objectives

a) To align the ICT strategic goals and objectives with the University's strategic plan, goals and objectives;

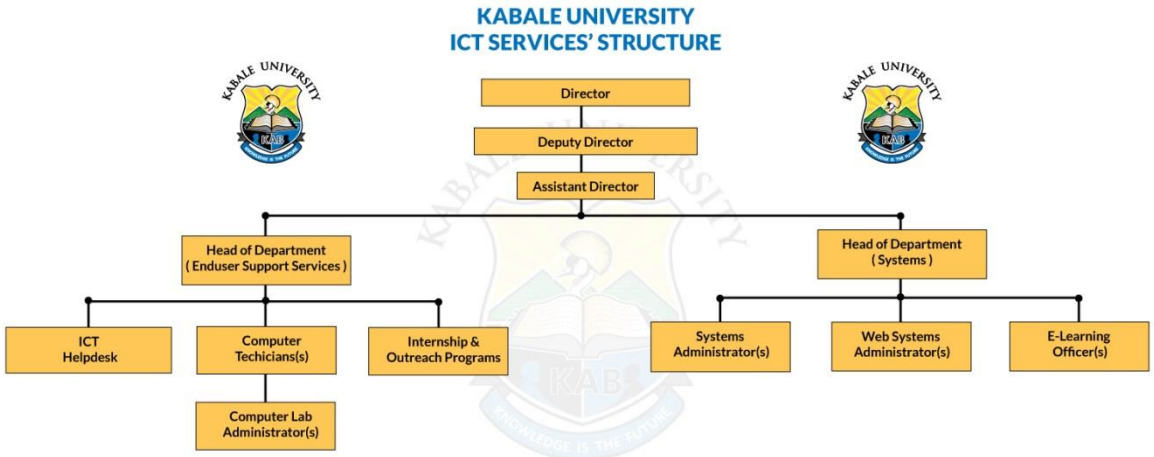
b) To ensure that ICT-related resource needs are met in an optimal manner by providing the organisational structure, capacity and capability;

c) To ensure that communication with stakeholders is transparent, relevant and timely

d) To ensure transparency of performance and conformance, and driving the achievement of strategic goals through monitoring and evaluation.

1.1.12 ICT Governance Structure

The following structure constitutes the Directorate of ICT Services for Kabale University.



1.1.13 ICT Governance Committees and roles

a) ICT and Library Committee of Senate

i. To plan and develop ICT and Library Services Policy
ii. To coordinate the activities of ICT and library service units
iii. To perform an oversight role on the activities of the ICT and library service units
iv. To ensure that the ICT and library service units offer the required services
v. To initiate policies on the use of ICT and library facilities
vi. Prepare and present periodic reports to Senate

b) Finance, Planning and Resource Mobilization Committee

i. To receive and consider the proposed budget estimates from the cost centers for approval by Council.
ii. To control the banking and investment operations of Council and to make provision for the examination of all the bills and accounts and for the discharge of liabilities incurred by the University.
iii. To control all the expenditure of the University under approved Annual Estimates.
iv. To receive and consider all requests for authorization of expenditure more than the approved Annual Estimates and make recommendations to Council.

v. To consider and propose fees and other rates to the Council
vi. To prepare and keep up to date an accurate comprehensive inventory of University property.
vii. To report to Council all matters related to finance, procurement, establishment and development.
viii. To prepare and present Quarterly Financial Reports to Council.
ix. To cause to be prepared Audited Accounts of preceding Financial Year for presentation to Council within a period of three months from the end of each Financial Year.
x. To prepare University Development Plans for an approved period and submit to Council.
xi. Receive and consider the proposed consolidated budget estimates in accordance to strategic plan, arising from the cost Centers for recommendation to Council.
xii. To advise Council and its Committees on the Financial Implications of Proposals made by Council Committees, Schools, Institutes, Departments, Directorates, Centers and other Units in respect to:
xiii. Measures Proposed for Development by the Unit concerned.
xiv. Offers of assistance, financial and otherwise from outside the University.
xv. To Explore and recommend to Council sources of revenue/resource mobilization plans, potential grant and trust funding opportunities for the University at National and International Levels.
xvi. To keep under review approved development programmes and to ascertain that the objectives of the University are being achieved and to make recommendations thereon to Council.
xvii. Take lead in University fundraising drives.
xviii. Collaborate with the Resource Mobilization Unit in writing grant applications.
xix. Ensure that University grant applications meet University fundraising requirements.
xx. To attend to such other functions as may be assigned to it by Council.

c) Audit and Risk Management Committee

(i) To formulate a policy framework for risk management based on the University Vision, Mission and Strategic Plan, as well as best practices
(ii) To receive and consider internal audit reports and work plans for submission to Council
(iii) To identify University External Auditors for appointment by Council
(iv) To receive and consider Annual Audited University Accounts and report to Council

(v) To develop and report on risk management policies, procedures, internal control systems, risk management functions and programs, for effective management of risks.

(vi) To continuously assess and monitor risk management functions, with a focus on risk identification and mitigation strategies

(vii) To formulate appropriate organizational structures and ensure adequate staff capacity of the Internal Audit Unit

(viii) To set up monitoring performance management system.

(ix) To review and make bi-annual recommendations to Council on risk management policies, procedures, and mitigation strategies

(x) Such other functions as may be assigned to it by the Council.

1.1.14 Roles and Responsibilities of DICTS

DICTS shall be the point of contact for all University ICT services and management. DICTS shall:

a) Provide effective ICT support services to the academic, research, outreach 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 an 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.

1.1.15 DICTS Resource Mobilization

a) DICTS shall become a cost center with its own budget and planning.
b) ICT contributions from functional fees on all students.

c) Income from ICT Consultancies.

d) ICT Projects.

1.1.16 ICT CAPACITY BUILDING

1.1.17 Objective

To equip students and staff with the requisite skills on a continuing basis to fully exploit the ICT environment in their different functions.

1.1.18 Skills Training Guidelines

a) Students: All University students shall be exposed to ICT skills through training.

b) Staff: All University staff shall be required to undergo ICT skills training.

1.1.19 ICT Policy Awareness

a) All new students and staff shall be briefed on ICT policies during orientation and induction period.

b) The policy shall be shared on the intranet and copies maintained in the library.

1.1.20 Role of DICTS

a) Undertake a periodic capacity skills and training needs for students and staff.

b) Prepare training materials for students and staff

c) Deliver training to students and staff

d) Evaluate trainings undertaken for relevance, quality, effectiveness, retention of knowledge, cost and value for money.

1.1.21 ICT OPERATIONS AND MANAGEMENT

1.1.22 Objective

To ensure best management practices are implemented for effective and efficient utilization of ICT systems and equipment for optimal output.

1.1.23 Acceptable Use of ICT Resources

All persons shall exercise care and attention over the use of ICT facilities. This applies to direct (University facilities) and indirect (third party equipment connected to University facilities) use of University ICT facilities.

a) All users shall comply with existing University policies.

b) All software of any equipment connected to the University ICT facilities shall be properly licensed and the terms of the license be strictly observed.

c) Users shall not access, interfere or remove any ICT facility, data or information unless they have been authorized to do so by DICTS.

d) ICT facilities shall be used in a manner that is consistent with user roles.

e) Users shall not use ICT facilities to disrupt or interfere with the use of facilities used by others.

f) All use of ICT facilities shall be in a lawful, honest, and decent manner, and shall have regard to the rights and sensitivity of other people.

g) All Users shall not create, use, or distribute materials that could bring the image of the University into disrepute.

h) Duly authorized officers of the University shall monitor and/ or access electronic data and/or information held or transiting on University ICT facilities, for individuals suspected to be in breach of the University regulations.

1.1.24 Procurement and Disposal of University ICT Assets

It is the University's policy to undertake all ICT procurements and disposals in accordance with *PPDA Act, 2014 (as amended) and PPDA regulations.* The role of ICT Directorate shall be to;

a) Conduct routine ICT needs assessment for faculties, schools, institutes and directorates for purposes of planning and budgeting.

b) Prepare quarterly, and annual ICT procurement plans for the whole University.

c) Prepare and manage overall ICT budget as per the priorities of the University.

d) Guide the preparation of ICT specifications and terms of reference for all University ICT procurements.

e) Participate in evaluation of ICT procurements.

f) Verify that supplied ICT equipment, software or services comply with the approved ICT specifications, standards and guidelines.

g) Allocate ICT assets as per the procurement plan and user needs.

h) Determine the life cycle of IT assets and advise management when due for disposal.

i) Ensure ICT assets due for disposal are cleared of any University information, and software licenses.

1.1.25 Printing and Photocopying

a) The University shall adopt a centralized printing (with some exceptions). Each member of staff shall have a unique user ID for accessing printing and copying services across the University network.

b) The Directorate of ICT services shall work and support the University towards a paperless operation through use of electronic mechanisms.

1.1.26 ICT Equipment Servicing, Maintenance, and Repair

a) The Server room equipment shall be serviced when need arises by authorized personnel.

b) Computers in computer laboratories shall be serviced during the recess term.

c) All computers and equipment in locations other than the server room and computer laboratories, shall be serviced as need arises.

d) DICTS staff are authorized to repair and service only University ICT equipment.

e) The server room shall be out of bounds for non-authorized persons.

1.1.27 Computer and Laptop Allocation

The ICT and Library Committee shall be responsible for allocating computers, laptops, and any other ICT equipment of the University.

1.1.28 Computer Laboratory Management

For proper management of computer laboratories, the following shall not be permissible;

1) Users shall not enter with food or drinks in Computer laboratories.

2) Users shall not disturb or interrupt other Computer laboratory users.

3) Users shall not modify the arrangement of laboratory equipment.

4) Users shall not conduct any form of sports betting, gambling, day trade, or access material of offensive nature.

5) Users shall not move cables, reconfigure systems, or alter ICT equipment in any way.

6) Users shall not abuse the hardware, software, or laboratory personnel.

7) Personal computers and peripheral devices are not allowed in computer laboratories.

8) Users shall not install unauthorized programs on University computer hardware.

9) Users shall not sit or rest their feet on top of computer desk(s).

10) All furniture exhibited in computer laboratories must be gender sensitive.

11) Users shall not connect personal ICT equipment such as hotspots to the University ICT network backbone.

12) Users are solely responsible for protection of passwords and login credentials needed for accessing personal email platforms, and other Management Information Systems of the University.

13) Computer laboratories shall not be points of sell or exchange for removable storage disks, and other electronic devices such as CDs, DVDs, USB drives, video tapes, audio tapes, RAM slots etc.

14) Users and Computer lab Administrators, shall not indulge in any form of commercial and classwork assignment related engagements.

15) The University shall not be responsible for any undeclared lost or stolen personal property inside the computer laboratory.

16) Do not send unsolicited bulk emails and messages either within or out the University that would be characterized by the recipients as spam.

17) Guests are not permitted to use Laboratory equipment without permission.

1.1.29 Logging and Monitoring

a) ICT shall implement network monitoring tools for immediate tracing of network bottlenecks and quick troubleshooting.

b) The University shall require that staff, students and others making use of the University's ICT-based systems are aware that activity logging takes place, and that monitoring or content inspection of an individual's activity may occur under specific circumstances.

c) Activity logs shall be properly secured and be compliant with the University's records management policy.

d) DICTS is authorized to institute automated broad sweep monitoring and content inspection processes in order to ensure proper functioning of IT systems, to validate adherence to University policy, and to guard against unauthorized activities.

e) To establish specific facts, as part of a formal investigation, where a member of staff has reasonable grounds to suspect breach of University policy or to comply with the lawful request of a third party (e.g. the police or other government agency).

f) To enable access to information crucial to the running of the University, in the absence of the individual.

g) To ensure the effective operation of a service i.e. to understand why a system appears to be performing outside its normal operational tolerances.

h) Where targeted monitoring or content inspection is authorized, it must be carried out in accordance with the ICT Privacy and Monitoring Procedure (refer to Appendix) and in accordance with the principle of minimal access to information (i.e. information so derived will be strictly controlled and only be made available to authorized recipients).

i) Members of University staff who have the capability to access activity logs or the electronics assets of others (e.g. systems administrators) must only exercise those abilities in the context of this policy.

Individuals in breach of this provision may be subject to the Staff/Student disciplinary procedures at the instigation of the staff member with responsibility for the person concerned, in addition to potential prosecution under the Regulation of Computer Misuse Act 2011.

1.1.30 Attendance Management

ICT Directorate shall work with management to implement technologies to monitor student and staff attendance while executing their roles at the University.

1.1.31 Projector use Procedure

a) Where practically possible, projectors in the University shall be ceiling mounted.

b) Heads of department shall be in charge of the projectors.

1.1.32 ICT usage by Persons with Disability

The University shall ensure a reasonable accommodation of Persons with Disability (PWD) in all its ICT planning and implementation.

1.1.33 ICT Asset Management

a) Inventory of ICT Assets: ICT Directorate shall conduct a bi-annual inventory of all University ICT assets and computers.

b) ICT Asset register: ICT Directorate shall maintain an updated list of all University ICT assets. The list may indicate name/type, serial number, engraving number, location, owner, etc.

c) Acceptable use of ICT Assets: Rules and Regulations for acceptable use of information and assets.

d) Return of Assets: All staff shall return all University ICT assets in their possession upon termination of employment or retirement. The assets shall be returned to the head of user department with clearance from DICTS and internal Audit.

e) Engraving/ Labeling of ICT Assets: All hardware assets shall be engraved in the format: *KAB/DeptName/Asset Type/Financial Year/IncrementalCountNumber*. Three-character abbreviation shall be adopted e.g. KAB/ICT/PRT/17/001, where KAB=Kabale University, Department Name= ICT, Asset Type= Printer, Financial Year =2017/2018, Increment= the count number of the asset in the department in a particular financial year. Where engraving is not applicable, an appropriate agreed method shall be adopted for the labelling.

1.1.34 NETWORK AND COMMUNICATIONS

1.1.35 Local Area Network (LAN) and Wide Area Network (WAN)

a) Network scope: All offices, departments, laboratories, conference halls, etc, shall be networked. The cabling standard used shall be category 6 and above.

b) Campus network backbone: Optic fiber cables shall be used for inter connecting all University buildings shall .

c) The network topology: The University shall implement a star topology on its network backbone

d) Cabling Security procedure: Power, telecommunications cabling carrying data and voice should be separated to guard against interference.

e) Wireless network: The University shall implement a secure wireless network.

f) WAN: The University shall connect to reliable Internet Service Provider(s).

1.1.36 Network Connection

a) All personal computers connected to the University network must have an anti-virus software package installed and enabled.

b) No unauthorized computer shall act as a gateway to the University network by virtue of offering dial-in, wireless or access to third parties.

c) No unauthorized computer system shall be used to monitor network traffic, or conduct speed or bandwidth tests. It shall not be used to interact with any other computer unless the said remote computer is offering a specific service the end user is authorized to use.

d) No unauthorized computer system shall be used to interfere with the operation of the network by acting as a network device (router, switch, hub, DNS server, DHCP server, etc). Connection of switches, routers, hubs or broadcast of any wireless signal from any such device is strictly forbidden.

e) Any computing device found to be disrupting or degrading the operation of the network service intentionally or otherwise, is subject to disconnection. In extreme cases this may be without warning.

f) The downloading, uploading and sharing of illegal, pirated or unlicensed content (images, software, music, etc, is explicitly forbidden.

g) The University shall implement a firewall system that will guard unauthorized users from accessing the network.

h) Staff Members under DICTS, with the explicit agreement of the Network Operations Manager, may be exempted from clauses (5.2.c, 5.2.e, 5.2.f).

1.1.37 Network Password Management

a) All users shall have a unique identifier (user ID) for their personal and sole use for access to all computing services. The user ID must not be used by anyone else and associated passwords shall not be shared with any other person for any reason.

b) Users shall be required to prove their identity in order to have a lost or forgotten password reset by a member of technical ICT support team. The University shall implement an automated system to minimize this requirement.

c) Individuals in breach of this regulation shall be subjected to disciplinary procedures at the instigation of the Dean/Director/head of Department with responsibility for the person concerned.

d) The University shall take legal action to ensure that its information systems are not used by unauthorized persons.

1.1.38 Website Management

a) Kabale University website shall conform with the National ICT policy and be a one stop Centre for all students, staff, and public online information needs.

b) There shall be a website committee to ensure information on the website is of quality, and reliable. The Committee shall be composed of: Director ICT Services, Communications and Branding Officer, representative from faculties, departments, schools, Institutes, units, Legal Officer, and Webmaster.

c) Communications and Branding office shall be the user department of the website. Only the Office of the Vice Chancellor or the Head of Communications and Branding unit, shall authorize the postings on the website.

1.1.39 Social Media Management

The University may use social media as one of its recognized channels of communication to the public. The Communications and Branding officer or his/her delegate shall be the authorized officer allowed to make postings on the University official social media site(s).

1.1.40 Office Telephone Sets and Intercom Usage

a) University shall install office telephone sets in various offices depending on the budget. Access of the telephone set shall be through use of Access Code /User ID loaded with

Credit limits. The amount shall depend on level and nature of position as determined by management. Access code shall be used on any telephone set across the University.

b) Intercoms shall be accessible by all staff without restrictions.

1.1.41 Email Usage and Management

a) Only full-time members of staff employed by the University and students enrolled on a program of study, are entitled to have use of a University e-mail address (mailbox). Individuals having special status may also have use of a mailbox (e.g. Chancellor, members of council, members of Contracts committee, etc).

b) Mailbox users shall take measures to ensure that their space quotas are not exceeded. Failure to do this could result in mailbox users being unable to receive messages and in extreme cases, unable to send messages.

c) Mailbox users must neither use University e-mail facilities for personal gain, or profit, nor for bring the University into disrepute.

d) Mailbox users must not attempt to impersonate the identity of others or, by any means, send or receive e-mails misrepresenting the originator or recipient addresses unless with explicit consent.

e) Any mailbox user who receives an e-mail that is clearly meant for another person must notify the sender.

f) Staff mailboxes are deleted when no longer required. For staff this is normally at the termination of employme09nt. Students mailboxes are deleted when a student completes his/her studies.

g) Individuals in breach of this regulation may be subject to disciplinary procedures at the instigation of the Dean/Director/Head of Directorate with responsibility for the person concerned. The University reserves the right to restrict or remove e-mail facilities from any person in breach of the regulation

h) The Director ICT services in consultation with the Vice Chancellor may confer special status upon an individual to permit the provision of a mailbox that would otherwise be

denied. Persons of special status must not imply or represent themselves as employees of the University.

1.1.42 Video Conferencing and Unified Communication Services

a) There shall be Implementation of a unified communications service to support new communications channels that are integrated with e-mail, online meetings, video conferencing, workplace collaborations and seamless file sharing.

1.1.43 SOFTWARE AND INFORMATION SYSTEMS

1.1.44 Objective

To implement an Integrated Management Information System for core systems for effective and efficient information management

1.1.45 Core Infrastructure Systems

a) Library Information Systems (LIBIS). It is the University policy to improve both the efficiency and effectiveness of library operations and services through the implementation of an integrated on-line Library Information System (LIBIS).

b) Academic Records Information System (ARIS). It is the University policy to enhance and streamline student education related administrative and managerial processes, and to improve academic reporting facilities at both central and faculty level through the implementation of an integrated Academic Records Information System.

c) Financial Management Information System (FMIS). It is the University Policy to enhance and streamline financial management processes and reporting facilities at both central and faculty level through the implementation of an integrated Financial Information System

d) Human Resource Information System (HRIS). It is the University Policy to enhance and streamline the human resource management and administrative processes through the implementation of an integrated Human Resource Information System.

1.1.46 Roles and responsibilities towards an Integrated MIS

a) User Directorates (Library, Academic Registrar, Human Resource, and Finance)

   i. Carry out comprehensive needs assessment of all required systems

ii. Study and map University policies

iii. Training Staff on procured system(s)

b) The Directorate of ICT services Shall;

i. Document all existing systems in use

ii. Carry out systems requirements specifications to guide procurement.

iii. Work with the consultant in design, development, testing, and commissioning of application software.

iv. Train staff on the use of procured systems/items.

1.1.47 Professional Software Specific for Directorates and Faculties

Each Directorate, School, Faculty and Institute shall identify its specific software requirements and work with the Directorate of ICT services to procure and install.

1.1.48 Integrated Financial and Academic Information Management Systems (IFAIMS)

The Directorate of ICT services shall support the University in the implementation of the government systems supporting Finance and Academic operations across its stake holders.

The Directorate of ICT services shall work with the Ministry responsible for Education for possible usage of Education Management Information System (EMIS) and any collaborations on information sharing.

1.1.49 E-LEARNING

1.2 Objective

To enable easier access to and coverage of University education by using ICT in instruction, learning, and research through the University wide implementation of Moodle E-learning platform

1.2.1 E-learning Implementation

a) The university shall run an online e-learning management system based on Moodle, and shall be hosted at an appropriate and reliable place as approved by Management and or senate.

b) There shall be an E-learning officer to manage all duties in relation to the e-Learning platform.

c) All students shall be required to take an introductory skills training in e-learning.

d) All staff shall undergo training in education technology techniques with emphasis on e-learning.

1.2.2 Laptop Scheme

All Kabale University students and staff shall be encouraged to acquire laptops.

1.2.3 ICT SECURITY

1.2.4 Objective

The objective is to reduce the risk of harm that can be caused to the University's ICT systems, information and infrastructure.

1.2.5 Protection of University Confidential Data

All staff and students are obliged to protect the following data classified as Confidential;

a) Unpublished financial information.

b) Personal data for partners, vendors, etc.

c) Patents, formulas or new technologies

d) Customer lists both existing and prospective.

1.2.6 Internal Organization

a) Asset Usage: Each ICT asset or equipment shall be assigned to a user who will be responsible for its day to day protection.

b) Segregation of duties and authorization: The initiation of an event shall be separated from its authorization. No user shall be allowed to access, modify, or use ICT asset without authorization. DICTS shall document authorization levels for all ICT processes.

c) Security incidents shall be reported to DICTS for timely intervention.

d) The Director ICT Technical Services and or Information Security Officer, shall be registered as members in specialist Information security forums and professional associations to stay up to date with relevant information security information.

1.2.7 Security of Mobile Devices e.g. Laptops

a) Cryptographic techniques like encryption should be used to protect information stored on such devices to avoid unauthorized access or disclosure

b) DICTS may provide physical locks to secure devices

c) It is the responsibility of the user of the asset to take care when using the University mobile device.

1.2.8 Human Resource Security

a) Prior to employment screening, the Human Resource Department, shall carry out background verification checks to ensure the staff is trusted to take on the role, especially if it requires handling confidential information.

b) All staff who are given access to information considered confidential should sign confidential or non-disclosure agreement. Human resource and legal Departments shall implement the regulation.

c) ICT Directorate shall conduct regular ICT security trainings for all staff, and where relevant, contractors on ICT policies and procedures as relevant to their job function

d) Upon termination of employment or change of role, the Human Resource Directorate and or Head of user Department shall in writing inform the ICT Directorate to revoke or change security rights of the staff in the system.

1.2.9 Access Control

a) Asset Users, System Users, Head of Departments, should determine appropriate access rights and restrictions for specific user roles.

b) There shall be a segregation of access controls i.e. user Departments shall make access request, Access Authorization by the supervisor or another Department, and access administration managed by the ICT Directorate.

c) Each member of staff shall be given a unique access code/User ID/Network ID, to access resources and services across the entire University through a one login policy.

This shall allow one access code to printing, telephone, information systems services, etc. with a unique code such as Employee Number.

d) DICTS shall ensure that a formal user registration, de-registration, assign of access, revoke access rights, is implemented.

e) Allocation of privileged access rights shall be controlled through formal authorization, allocated on need to use basis and shall be assigned to a user ID different from that used for regular business activities.

f) Access to University systems and applications should be controlled by secure-log-on procedure.

g) ICT Directorate shall ensure access to program source code be restricted.

1.2.10 Cryptographic Controls

The University may implement use of encryption on information transported by mobile or removable devices to ensure confidentiality and unauthorized access.

1.2.11 Physical and Environmental Security

a) In Order to secure the server room and data centers;

i. All doors should be alarmed, and monitored.

ii. Intruder detection should be installed.

iii. Physical entry codes shall be installed to ensure that only authorized personnel should be allowed access.

iv. A physical logbook and or electronic audit trail shall be maintained.

v. External party support service personnel access to server room/datacenter should be grant restricted, and only when required, the access be authorized, monitored and supervised.

vi. Shall be located in secure strong locations away from human or vehicle traffic.

vii. Shall be secured against physical intrusion, exposure to water, dust, fire, and power fluctuations.

viii. Shall be supported by alternate power supply including use of Main grid, generator, UPS battery, or solar energy (photovoltaic)

b) Clear Desk and Clear Screen.

The regulation is aimed at reducing unauthorized access to information after working hours

i. All sensitive University information shall be locked and not left on desks especially when office is vacated.
ii. All computers should be left logged off and protected with a screen password.
iii. Media containing sensitive information shall be removed from printers immediately.

a) Unattended User Equipment Management

i. Terminate all active sessions when not in use or lock screen with a password.

ii. Log off from application or network services when no-longer needed.

1.2.12 Operational Security

The objective of this regulation is to ensure correct and secure operations of information processing facilities

a) Documentation of Secure Operation: All operating procedures shall be documented and made available to all users who need them. This shall apply to software applications and hardware equipment.

b) Development, testing, and operational environments shall be separated to prevent operational problems

c) Malware control: The University shall implement malware software for detection, prevention and recovery control of malware. The software should be able to check for the installation of unauthorized software (white listing) and malicious websites (blacklisting)

d) Clock synchronization. All information systems within the University shall be synchronized to a single time source to ensure accuracy of audit logs

1.2.13 Communication Security

a) Segregation in networks: Kabale University network shall be divided into separate domains logically using VLANs.

b) Wireless network and all wireless access shall be treated as external connection and segregated from internal network not until the access has passed through the University network gateway.

c) Electronic message (email, social media) shall be protected from unauthorized access, modification or denial of service by ensuring correct addressing and transportation of the message.

1.2.14 Anti-Virus and Open Source Software Installations

a) It is the University policy that all computers using windows operating system be installed with a licensed anti-virus that shall update automatically when connected to Internet.

b) The long-term plan for the University shall be to have an open source software environment. However, the server environment shall only be open source.

1.2.15 Security Incidence Management

The objective of this regulation is to ensure a consistent and effective approach to the management of information security incidents.

a) All system users have a responsibility to report security events.

b) The first contact point for reporting security incidences is the ICT helpdesk.

c) Help desk will assess whether the reported security event amounts to security incidence and then forwards it to Information Security Incidence Team (ISIT) for analysis and review.

d) DICTS shall be responsible for collection and preservation of potential evidence.

1.2.16 ICT DATA BACKUP AND ARCHIVING

1.2.17 Objective

The primary objective of this regulation is to protect the University's data. The regulation seeks to outline the data backup and recovery controls for the University so as to ensure that the data is correctly and efficiently backed up and recovered in line with best practice.

1.2.18 Data Backup Standards

a) Critical data to the University shall be defined by the University and shall be backed up.

b) Backed up data shall be stored at a location that is physically different from its original creation and usage location,

c) Data restores shall be tested monthly

d) Procedures for backing up critical data and the testing of the procedures shall be documented.

1.2.19 Data Backup Selection

a) All data and software essential to the continued operation of the University shall be backed up

b) All supporting material required to process the information shall be backed up as well. This includes programs; control files, install files, and operating system software.

1.2.20 Backup Types

a) Full backups shall be run weekly as these datasets will be stored for a longer time period. This will also aid in ensuring that data can be recovered with the minimal set of media used at that time. Once a month, a full backup should be stored off site

b) Differential/Incremental backups shall be used for daily backups. This ensures that the backup time window is kept to a minimum during the week while allowing for maximum data protection.

1.2.21 Backup Procedure

a) DICTS shall choose between automated and manual backup procedures based on their requirements and constraints.

b) DICTS shall choose between centralized and decentralized backup procedures based on their requirements and constraints.

1.2.22 Backup Owner

a) The DICTS shall delegate a dedicated staff (s), from existing personnel to commit and adhere to each backup schedule.

1.2.23 Offsite Storage

a) Data backups shall be stored in two locations:

   i. One on-site with current data in machine-readable format in the event that operating data is lost, damaged or corrupted.
   ii. One off-site to additionally provide protection against loss to the primary site and on-site data.

b) Minimum requirements are to store the weekly, monthly and or yearly backup sets off site.

c) The site used for storing data media off-site shall meet Physical Security requirements defined within the ICT Security regulation.

1.2.24 Data Archiving

The University shall consider adopting archiving and warehousing technologies when the University data is not in constant use. This shall be in line with the data retention and destruction policy as adopted by the University.

1.2.25 ICT RESEARCH AND INNOVATION

1.2.26 Objective

To contribute towards establishing a research support center for improved research and innovations

1.2.27 Information Technology Transfer

a) ICT Directorate shall spearhead the establishment of the Center for Information Technology Transfer (CITT) for students and staff to exercise innovation and research.

b) ICT Directorate shall provide support to all students and teaching staff participating in research and innovation projects.

1.2.28 Role of DICTS

a) Equip the center with required equipment and software.

b) Build a database of research and innovation projects for students and lecturers for further research.

1.2.29 ICT CONSULTANCY

1.2.30 Objective

To contribute towards resource mobilization for funding critical ICT infrastructure projects through providing professional ICT services to community at subsidized costs

1.2.31 Consultancy Services

a) ICT Directorate shall support the University in providing professional ICT services to community, companies, NGO's in areas of training, research, design, development, and implementation of ICT services and systems.

b) Kabale University Management shall study and determine the requirements to use DICTS as a consultancy entity.

1.2.32 Role of DICTS

a) DICTS shall register as a consultancy entity under the guarantee of Kabale University.

b) DICTS using its staff, students, and University human resource, shall execute such consultancies. The funds collected from consultancies, shall be deposited to the University account

c) Determine all operational expenses arising from the execution of consultancy services.

1.2.33 ICT COMMUNITY OUTREACH

1.2.34 Objective

To contribute towards promoting University community partnerships with knowledge, skills and technology transfer in line with University Strategic plan.

1.2.35 ICT Outreach Services

a) Provide ICT skills to surrounding communities including youth, women, teachers, etc. (e-skills project)

b) Engage with community on ICT innovations that can form a bulk of future research projects for University ICT students (e-Innovations)

c) Partner with local governments and other organizations in addressing community problems with ICT solutions. (e-Solutions). University students may be attached to institutions for research projects on specific problems facing communities

1.2.36 Role of DICTS

a) DICTS shall engage in writing and implementation of proposal for funding.

b) Contribute to the realization of the strategic objective of engaging with communities and contributing to their development.

1.2.37 REFERENCES

1. Computer Misuse Act, 1998 as amended 2011.
2. Defamation Act (Criminal defamation is covered under Penal Code Act section 179 and 180)
3. Access to Information Act, 2005
4. The Uganda Communications Communication Act, 2013
5. The Uganda Telecommunication Act, September 2000
6. The Copyright and Neighboring Act, 2006
7. Public Procurement and Disposal Act,2014
8. Control Objectives for Information and Related Technologies Framework 4.1
9. International Standards Organization 27001 Framework

1.2.38 Appendix A

a) *Request for monitoring or content inspection of an individual's use of an IT system shall be logged and carried out under the following circumstances;*

A.1: To Investigate a suspected breach of University policy or the law.

A.2: To access information crucial to the running of the University.

A.3: To ascertain why an ICT system appears to be performing outside normal tolerances.

b) *In the case of A.1 above, it shall not always be appropriate or possible to inform the person(s) concerned.*

In the case of A.2 above, the person(s) concerned will be approached whenever possible prior to any third-party access and will be informed as soon as possible afterwards.

c) *In the case of A.3 above, the Director of DICTS or appointed personnel shall establish basic facts and remedy, with audit trail, without recourse to this procedure unless in so doing it becomes necessary under A.1 above.*

d) *For A.1 and A.2, for members of staff, a line manager must complete an "ICT Privacy and Monitoring Form which will be routed to the Director of Human Resources for authorization. If, in making the request, there is a conflict of interest (those involved in authorising or executing the request are the subject), the request should be sent, to a member of the University Executive Team for authorisation. Under normal circumstances, a copy of the authorized form will be routed to the Director DICTS for action.*

e) *Where the subject of the request is a student, the form will be routed to the Dean of Student for authorisation and in turn routed to the Director of DICTS for action.*

f) *For A.2 where a member of staff is absent, the line manager, with permission of the relevant Dean/Director, shall seek permission to access the staff member's electronic assets, through direct dialogue with the member of staff. Contact shall be made in accordance with the process for contacting staff at home. The permission, or reasons for the lack of it, must be noted on the "ICT Privacy and Monitoring Form". The Director of the IT Department or appointed member of staff shall arrange the approved access and maintain an audit trail of actions taken. The Director DICTS or appointed person shall be responsible for ensuring that any temporary access is revoked at the end of the specified period.*