



KIBABII UNIVERSITY

**Information and Communication
Technology (ICT)
Policies and Procedures Manual**

©KIBU, 2023



**Kibabii ISO 9001: 2015 Certified
Knowledge for Development**

KIBABII UNIVERSITY – ISO 9001:2015 QUALITY MANAGEMENT SYSTEMS		
ISSUE FOR USE ON:	MAIN TITLE: Information and Communication Technology (ICT) Policies and Procedures Manual	REF: KIBU/AFD/POL/017

**INFORMATION AND COMMUNICATION TECHNOLOGY
(ICT)
POLICIES AND PROCEDURES MANUAL**


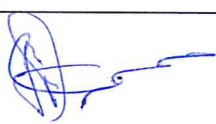
Approved by: Prof. Donald N. Siamba Management Representative	Sign: 	Date: 22/9/2023
Authorized by: Prof. Isaac Ipara Odeo Vice Chancellor	Sign: 	Date: 22/09/23



Table of Contents

FOREWORD.....	viii
ACKNOWLEDGEMENTS	ix
ICT Directorate Mandate.....	x
Mission Statement.....	x
Vision Statement.....	x
Philosophy.....	x
Core Values of the ICT Directorate	x
Key Principles	x
DEFINITION OF TERMS	xi
ACRONYMS	xii
CHAPTER ONE: GENERAL PROVISIONS	1
1.0 Introduction.....	1
1.1 Purpose.....	1
1.2 Policy Objectives	2
1.2.1 General Objectives.....	2
1.2.2 Specific Objectives	2
1.3 Rationale	2
1.4 The Policy Framework.....	3
1.4.1 Policy Statements.....	3
1.4.2 Scope.....	5
1.4.3 Responsibility	5
1.4.4 Interpretation.....	5
1.4.5 Delegation	5
1.4.6 Amendments and Review	5
CHAPTER TWO : SPECIFIC ICT POLICIES.....	6
2.1 ICT Services Management Policy	6
2.1.1 Introduction.....	6
2.1.2 Purpose.....	6
2.1.3 Administration of the Policy	6



2.1.3.1 Legal and Policy Framework	6
2.1.3.2 Implementation Framework	6
2.1.6 Capacity Building	10
2.1.7 DICT Sustainability	11
2.1.8 Resource Ownership	11
2.1.9 Service Level Agreements (SLAs) and Service Charters	11
2.2: ICT EQUIPMENT USE POLICY	12
2.2.1 Introduction.....	12
2.2.2 Purpose.....	12
2.2.3 Responsibilities.....	12
2.2.4 General Principles and Guidelines.....	12
2.2.5 Enforcement.....	13
2.3: CHANGE MANAGEMENT POLICY	14
2.3.1 Introduction.....	14
2.3.2 Purpose.....	14
2.3.3 Changes to the IT infrastructure	14
2.3.4 Change Management Group	14
2.3.5 Change Management Process	15
2.4: ICT RESOURCE ACQUISITION POLICY	17
2.4.1 Introduction.....	17
2.4.2 Purpose.....	17
2.4.3 Make or Buy	17
2.4.5 Outsourcing of Services.....	17
2.5: ICT RESOURCE OUTSOURCING AND COLLABORATION POLICY	18
2.5.1 Introduction.....	18
2.5.2 Purpose.....	18
2.5.3 Procedure for Outsourcing of ICT Services from the University	18
2.6: ANTI-VIRUS POLICY.....	19



2.6.1 Introduction.....	19
2.6.2 Purpose.....	19
2.6.3 General Policy.....	19
2.6.4 Rules for Virus Prevention.....	19
2.6.5 ICT Directorate Responsibilities.....	20
2.6.6 Department and Individual Responsibilities.....	21
2.6.7 Enforcement.....	21
2.7: BACKUP POLICY.....	22
2.7.1 Introduction.....	22
2.7.2 Purpose.....	22
2.7.3 Data Back-Up.....	22
2.7.4 Backup Schedule.....	22
2.7.5 Managing Restores.....	24
2.8: E-MAIL ACCEPTABLE USE POLICY.....	26
2.8.1 Introduction.....	26
2.8.2 Purpose.....	26
2.8.3 Account Activation/Termination	26
2.8.4 General Expectations of End Users	26
2.8.5 Appropriate Use	27
2.8.6 Inappropriate Use.....	27
2.8.7 Monitoring and Privacy	28
2.8.8 Reporting Misuse	28
2.8.9 Disclaimer	28
2.8.10 Failure to Comply	29
2.9: HELP DESK TRIAGE POLICY.....	30
2.9.1 Introduction.....	30
2.9.2 Purpose.....	30
2.9.3 General Guidelines.....	30



2.9.4 Priority Categories	30
2.9.6 Contact Information.....	31
2.10: SYSTEM CONTROLS AND SECURITY POLICY	33
2.10.1 Introduction.....	33
2.10.2 Purpose.....	33
2.10.3 Objectives	33
2.10.4 Systems Security Control Policy	33
2.10.5 Physical Security.....	34
2.10.6 Passwords.....	34
2.10.7 Data Security.....	34
2.10.8 Copyright and License Agreements.....	34
2.10.9 Internet	34
2.10.10 Email.....	35
2.10.11 Monitoring and Evaluation	35
2.11: WEBSITE POLICY.....	37
2.11.1 Introduction.....	37
2.11.2 Purpose.....	37
2.11.3 University Website Information Standards.....	37
2.11.4 Restrictions	37
2.11.5 Copyright and Trademark—All Pages.....	38
2.11.6 Web Oversight	39
2.11.6.1 Role of University Webmaster.....	39
2.11.6.2 Role of the Director of ICT.....	39
2.11.7 Enforcement and Notification.....	40
2.11.8 Social Media	40
2.12: ICT DISASTER MANAGEMENT POLICY.....	41
2.12.1 Introduction.....	41
2.12.2 Objectives of the Disaster Management Policy.....	41



2.12.3 Disaster Planning	42
2.12.4 Disaster Preparation	44
2.12.5 Replacement Equipment	44
2.12.6 Backups	44
2.12.7 Backup Procedure	45
2.12.8 Initiation of Emergency Procedures.....	45
2.12.9 ICT Disaster Management Team	45
2.12.10 ICT Disaster Management Recovery Plan.....	45
2.12.11 Equipment Protection.....	46
2.12.13 Initiation of Recovery Procedures	46
2.12.14 Site Preparation	47
2.12.15 System Platform Recovery Procedures.....	47
2.12.16 Critical Applications	47
2.12.17 Restoration of the Data Center.....	47
2.12.18 Maintaining the ICT Disaster Recovery Plan	47
APPENDIX 1: REFERENCES	49
APPENDIX 2: ICT EQUIPMENT USE AGREEMENT	50
APPENDIX 3: DECLARATION TO ADHERE TO KIBU ANTI-VIRUS POLICY	51
APPENDIX 4: DECLARATION OF UNDERSTANDING KIBU SERVER BACKUP POLICY	
52	
APPENDIX 5: E-MAIL USER AGREEMENT	53

FOREWORD

Kibabii University having realized the critical role of Information and Communication Technology (ICT) in higher education, is committed to the application of ICT for enhancing administrative efficiency and to optimize learning experiences. The University ICT Policy and Procedures Manual is modeled around access, economy, efficiency, effectiveness, relevance, transparency, privacy, accountability, sustainability, learner-centred, pedagogically driven and quality assurance as the guiding principles. The ICT applications cover the areas like system management, research, teaching and learning, student evaluation, support services, community engagement, student data management, human resource development networking and quality assurance.

As an ongoing process, ICT applications shall take note of the rapid pace of technology changes. In this regard, ICT Policy management shall be integrated with the ICT standard Operating Procedures into a one stop document (Manual) to ensure integrity, security and legitimate applications of ICT. In addition, the Manual will effectively facilitate the establishment and fostering of national and international networks to ensure innovative changes in providing quality education. The University shall therefore take appropriate measures for the capacity building of academic and administrative staff to effectively use ICT in all University operations.



Prof. Isaac Ipara Odeo
Vice Chancellor



ACKNOWLEDGEMENTS

Kibabii University ICT Policies and Procedures Manual has been developed from a consultative process involving key stakeholders at the University including the Vice Chancellor, the Deputy Vice Chancellors, Registrars, Finance Officer, Deans of Faculties/Schools, Directors, Heads of Department, lecturers and students. I would like to take this opportunity to thank all persons involved in the development of this Manual. I wish to particularly acknowledge the contribution of the Directorate of ICT and the ICT Committee that drafted this Policy document.



Prof. Donald Siamba

Deputy Vice Chancellor (AFD)



Kibabii ISO 9001: 2015 Certified
Knowledge for Development

Page ix

ICT Directorate Mandate

Mission Statement

To cost effectively enhance the quality of teaching, learning, research and administration through the infusion integrated ICT tools.

Vision Statement

To achieve excellence in transmission and enhancement of new knowledge in Science, Technology and innovation through the use of ICT.

Philosophy

The Directorate holds the view that ICT is a critical catalyst for sustainable utilization of material and human resource for posterity of the universe.

Core Values of the ICT Directorate

- a) Excellence
- b) Accountability and Transparency
- c) Integrity
- d) Social Responsibility
- e) Innovation
- f) Academic Freedom

Key Principles

This Policy shall be guided by the following key principles:

- a) Mainstreaming of ICT in the University;
- b) Seamless integration of ICT;
- c) Inclusion, flexibility and support of other quality management systems;
- d) Adherence to best practices & policies; and
- e) Economies of scale and customer value propositions.

DEFINITION OF TERMS

- ICT** - In this Policy refers to all information and communications technology hardware and software, data and associated methodologies, infrastructure and devices that are owned, controlled or operated by the University.
- User** - Means anyone who operates or interfaces with ICT. It includes University staff, officers and students or any other member of the University.
- Authorized User** - Means a members of the University staff or student allowed to use ICT resources.
- Information System** - An individual or collection of computing and networking equipment and software used to perform a discrete business function. Examples include the eLearning System, ERP System and associated PC or set of desktop computers used to perform general duties in a Department.
- Unit** - A part of Kibabii University that has administrative and financial duties to comply with the University's information security policies.
- Kibabii University Data** - Data in any format collected, developed, maintained or managed by or on behalf of the University, or within the scope of University activities. The terms 'data' and 'information' are used interchangeably in the context of the information security program.

ACRONYMS

ANSI	-	American National Standards Institute
CMG	-	Change Management Group
CD	-	Compact Disk
DVD	-	Digital Video Disk
ICT	-	Information & Communication Technology
ICTCC	-	ICT Council Committee
IICTIC	-	ICT Implementation Committee
ICTSC	-	ICT Steering Committee
IRM	-	Information Resource Management
ISP	-	Internet Service Provider
KENET	-	Kenya Education Network
KIBU	-	Kibabii University
LAN	-	Local Area Network
MIS	-	Management Information System
SMTP	-	Simple Mail Transfer Protocol
STEP	-	Skills Training for End-users Project
TCP/IP	-	Transport Control Protocol/Internet Protocol
UPS	-	Uninterrupted Power Supply
VSAT	-	Very Small Aperture SATellite
WAN	-	Wide Area Network
WWW	-	World Wide Web

CHAPTER ONE: GENERAL PROVISIONS

1.0 Introduction

The University has steadily expanded ICT resources and services since its inception. The number of computers in the University has grown to over 400 desktops most of which are networked. The ICT network comprises a fiber optic backbone and several Ethernet LANs that cover the academic and administrative blocks. The LANs are managed from a central server room which hosts various servers, switches, routers and other data terminal equipment. The University subscribes to a bandwidth of 607 mbps internet connectivity via a leased line from Kenya Education network (KENET). Additionally, the University has acquired licensed software and support staff. Therefore, there is need to develop policies as framework to aid the University in sustaining the expansion, effective management and optimum utilization of ICT resources. It will also guide acquisition, further development, administration, maintenance and usage of the ICT facilities. With adequate investments in ICT, the Policy document and Procedure Manual can be implemented to the advantage of the University customers.

In order to provide a one stop reference point, several specific policies and procedures have been developed and combined/compiled to form the Information and Communication Technology Policies and Procedures Manual herein referred to as 'the Manual' to ensure consistency and harmony in the application of ICT at Kibabii University.

Unless otherwise expressly provided, employees of the University shall be required to observe the provisions of the policies and procedures provided in this Manual. In addition, employees will be required to comply with relevant provisions of other policies, procedures, rules and instructions issued by the University and Government from time to time.

Where a conflict arises between the provisions of the policies and procedures in this Manual with any other Manual, such conflicts will be referred to the Vice Chancellor for guidance.

Copies of this Manual are the property of the University and it is the responsibility of the Deputy Vice Chancellor/Administration, Finance and Development to ensure that all employees have access to the Manual.

1.1 Purpose

This framework of Policies and Procedures is intended to be an enabling mechanism for efficient service delivery, information sharing, electronic operations, and reducing information-related risks to acceptable levels.



1.2 Policy Objectives

The objectives are categorized into general and specific objectives

1.2.1 General Objectives

To support the strategic vision of KIBU by improving operational efficiency and exchange of information so as to maintain a competitive edge.

1.2.2 Specific Objectives

The specific objectives of KIBU ICT Policy are to:

- i. Provide cost effective information and communication technology facilities, services and automation;
- ii. Enhance customer satisfaction;
- iii. Identify priority areas for ICT development;
- iv. Encourage innovations in technology development, use of technology and general work flows;
- v. Help Staff and students to adapt to new circumstances and provide tools and models to respond rationally to challenges posed by ICT; and
- vi. Promote information sharing, transparency and accountability.

1.3 Rationale

Some major reasons for formulating this ICT Policy are:

- i. **Rapidly changing technology.** As technology changes, planning becomes increasingly important in order to avoid incompatibility and inaccessibility. It is now asserted that the world is in the nanotechnology. Networked organizations are the order of the day, and developing institution-wide network systems requires Policy framework;
- ii. **ICT expertise scarcity.** The severe scarcity of adequately trained and experienced analysts, software engineers, systems and network managers, coupled with their long training cycles constrains ICT developments and therefore requires that priorities be established within an ICT Policy;
- iii. **Scarcity of support resources.** Limited availability of financial and managerial resource is the other reason for high level ICT planning guided by sound policies;
- iv. **General growth.** The development of academic programs, courses, services, research programs, educational technological activities, policies and methods as well as the growth of the number of students and faculty will depend on the availability of ICT services and systems. Understanding this dependency at an early stage is critical to the success of an ICT Policy; and

- v. **Integration of KIBU – National ICT Policy.** In line with the National ICT Policy, KIBU needs to develop an institutional Policy that will guide the governance and implementation of ICT infrastructure.

1.4 The Policy Framework

The following Policy statements provide a foundation for the development of the specific ICT policies that may be developed as need arises. Such policies may include but not limited to the following:

- i. ICT Services Management Policy
- ii. ICT Equipment Use Policy
- iii. Change Management Policy
- iv. ICT Resource Acquisition Policy
- v. ICT Resource Outsourcing and Collaboration Policy
- vi. Anti-Virus Policy
- vii. Backup Policy
- viii. E-Mail Acceptable Use Policy
- ix. Help Desk Triage Policy
- x. System Controls and Security Policy
- xi. Website Management Policy.
- xii. Disaster Recovery Policy.

These Policies will be formulated, approved by the management and incorporated to main Policy document as Sections.

1.4.1 Policy Statements

In order to ensure focused implementation of ICT Policy the following articles of Policy Statements are hereby declared; it is the University Policy to:

- i. Assure availability of all anticipated ICT services/systems at any workplace in the University, and for selected services, to locations outside the University through Common Network Services. Common Network Services (Network Infrastructure), mainly comprising physical network infrastructure (wiring, switches, routers, servers, etc) and communication protocols (TCP/IP), from the collective/systems, and in conformity with The National ICT Policy and International standards;
- ii. Assure availability and controlled usage and changes of basic User-level Data Communication and telecommunication Services such as e-mail, Access-to-Internet/Extranet/Intranet services and telecommunication terminal equipment which actually are major ‘elements’ of the low-level network & communication services;
- iii. Promote office computing in all offices. This applies to lecturers, researchers, administrators, managers, as well as to secretarial and clerical workers. Major office computing applications are: word processing, electronic e-mail, spreadsheet processing,

- data and document storage and retrieval desktop publishing, access-to-internet and intranet;
- iv. Continuously improve both the efficiency and effectiveness of library operations and services through the implementation of an integrated on-line library information system;
 - v. Enhance and streamline education related administrative and managerial processes and to improve academic reporting at both central and faculty level through the implementation of an integrated academic records information management system;
 - vi. Enhance and streamline financial management processes and reporting at both central and faculty levels through the implementation of an integrated financial information management system. Given the decentralized nature of budgetary management, it is the University Policy to make these functions also available to faculties and other cost centers;
 - vii. Enhance and streamline the human resource management and administrative processes through the implementation of a human resource information system;
 - viii. Enhance and streamline the property and asset management and administrative processes through the implementation of an asset and inventory information system;
 - ix. Promote the development of ICT infrastructure in all areas of teaching, research and extension by creating technical, organizational and management structures;
 - x. Harness ICT potential in enhancing online and blended learning in order to maximize flexibility in education and reach out to a wider coverage of prospective learners;
 - xi. Ensure that all students and staff are trained on a continuing basis to equip them with the requisite skills to fully exploit the ICT potential in their different functions, in order to make the entire University fraternity “IT Complaint”;
 - xii. Ensure sustainable management of the institution’s ICT resources through the creation of appropriate Policy guidelines and regulations, advisory and operational organs that will cater for the broad interests of all users. Such Policy guidelines and regulations herein referred to as Sections will consequently be part and parcel of the ICT Policy;
 - xiii. Establish an ICT Committee as an advisory management organ which will constitute the necessary subcommittee and task forces to develop the Policy guidelines and regulations, maintain and implement the ICT Policy. The committee will be chaired by the Deputy Vice Chancellor Administration Finance and Development (AFD) and will comprise members appointed by the University Vice Chancellor;
 - xiv. Establish a Directorate of ICT services under the office of Deputy Vice Chancellor AFD. The primary function will be to offer User-support, network and communication services to the academic and administrative functions. It will also offer professional and skilled based training to students and staff. The functions and structure of the Directorate are herein outlined in the ICT Services management Policy Section;
 - xv. Harness the power of information and mass communication media including TV, Radio and Print media to enhance its image and broadcast programmes that augment its academic, research and extension pursuits. Towards this end the University may establish a media house that will produce and air such programmes; and

- xvi. Provide for the growth of its ICT resources and their financial sustainability through adequate funding and appropriate operational mechanisms.

1.4.2 Scope

ICT Policies and Procedures Manual applies to all employees, students, suppliers, contractors and any other parties who rely on access to KIBU ICT services.

1.4.3 Responsibility

The Deputy Vice Chancellor (Administration, Finance and Development) shall make the Manual available to all employees. It will be the responsibility of all employees to read and understand the Manual and any other subsequent amendments therein.

1.4.4 Interpretation

The interpretation of the Manual shall rest with the Vice Chancellor. The Vice Chancellor will seek guidance from the Council or any relevant Government agency on any matter that may not be covered by these policies and procedures.

1.4.5 Delegation

The Council may delegate any of its functions and powers under this Manual to a Committee of the Council or the Vice Chancellor. The Vice Chancellor may delegate his duties and powers under these regulations to any officer of the University as may be appropriate.

1.4.6 Amendments and Review

The Manual maybe amended from time to time as and when necessary with the University ICT Committee. Such changes will require authorization of the Council and will be communicated to employees in writing by the Vice Chancellor.

The Council reserves the right to initiate and approve a revision, revocation or addition to the policies contained in this Manual.

This Manual will be reviewed after every five (5) years or as need arises taking into considerations the emerging issues.

CHAPTER TWO : SPECIFIC ICT POLICIES

The specific ICT Policies development based on the Policy statements are presented as Sections.

2.1: ICT Services Management Policy

2.1.1 Introduction

Information processing and communication services from vital resource to KIBU that must be carefully planned, deployed and maintained. Structure to plan, organize and coordinate such services and policies that govern them must therefore, be put in place.

2.1.2 Purpose

The purpose of the ICT Services Management Policy is to establish a structured framework and guidelines for the planning, deployment, maintenance, and governance of information processing and communication services at KIBU. This policy aims to ensure the efficient and effective management of vital ICT resources to support the institution's mission and objectives while promoting accountability, security, and reliability in service delivery.

2.1.3 Administration of the Policy

The Policy will be administered by the ICT Committee of the University Management Board who shall ensure that ICT Policy decisions are driven by real ICT needs and the desire to improve the institution's performance and education and science competence. It shall foster a climate in which innovation through ICT can develop.

2.1.3.1 Legal and Policy Framework

The Policy shall be interpreted in accordance with the following:

- i. The Constitution of Kenya, 2010;
- ii. The Universities Act, 2012;
- iii. KIBU Charter, 2015;
- iv. KIBU Statutes, 2021; and
- v. National Information, Communication and Technology Policy, 2019

2.1.3.2 Implementation Framework

2.1.3.2.1 Administrative Structure

The following organs of the University shall be responsible for the implementation of this Policy:

a) The University Council

The Council shall be responsible for the general direction, coordination and overall management of the University's ICT operations.



b) University Management Board

The University Management Board will coordinate and control the planning development, management and delivery of ICT services in University.

c) The University Senate

The University Senate will Provision of advisory and technical support for Policy implementation of ICT services in University.

d) The ICT Committee

The ICT Committee will oversee implementation of the ICT Policy.

f) The Directorate of ICT

This Directorate will be responsible for the implementation and day to day ICT activities. The Directorate will generally provide ICT services to students and staff who fall mainly in the Academic, Administration and Finance, and Planning, Research and Extension divisions. It will actively offer professional training to the University and the surrounding community, conducts research, and offer consultancy services in the area of ICT. Owing to shortage of sufficient expertise in the region and country as a whole the Directorate may draw expertise from and form synergies with the teaching Departments in the area of computing.

The specific functions of DICT will be to:

- i. Provide computing services to the University through sustainable automation of all information generation, processing and communication operations;
- ii. Design, develop and implement viable state-of the art systems in the University;
- iii. Ensure a well maintained and up-to-date ICT infrastructure in order to continuously support the University in accomplishing its teaching and research functions;
- iv. Ensure that staff can adequately make use of modern ICT technologies by providing demand driven ICT training;
- v. Be a centre for professional training and technology transfer in ICT;
- vi. Undertake research, development, innovations and technology transfer;
- vii. Provide consultancy services on ICT to organizations both at the regional, national and global levels;
- viii. Establish and maintain sustainable linkages and collaborations with ICT industry players in order to foster research and extension; and
- ix. Provide technical support to the ICT Committee in formulation of ICT Policy guidelines and regulations.

Administrative Structure

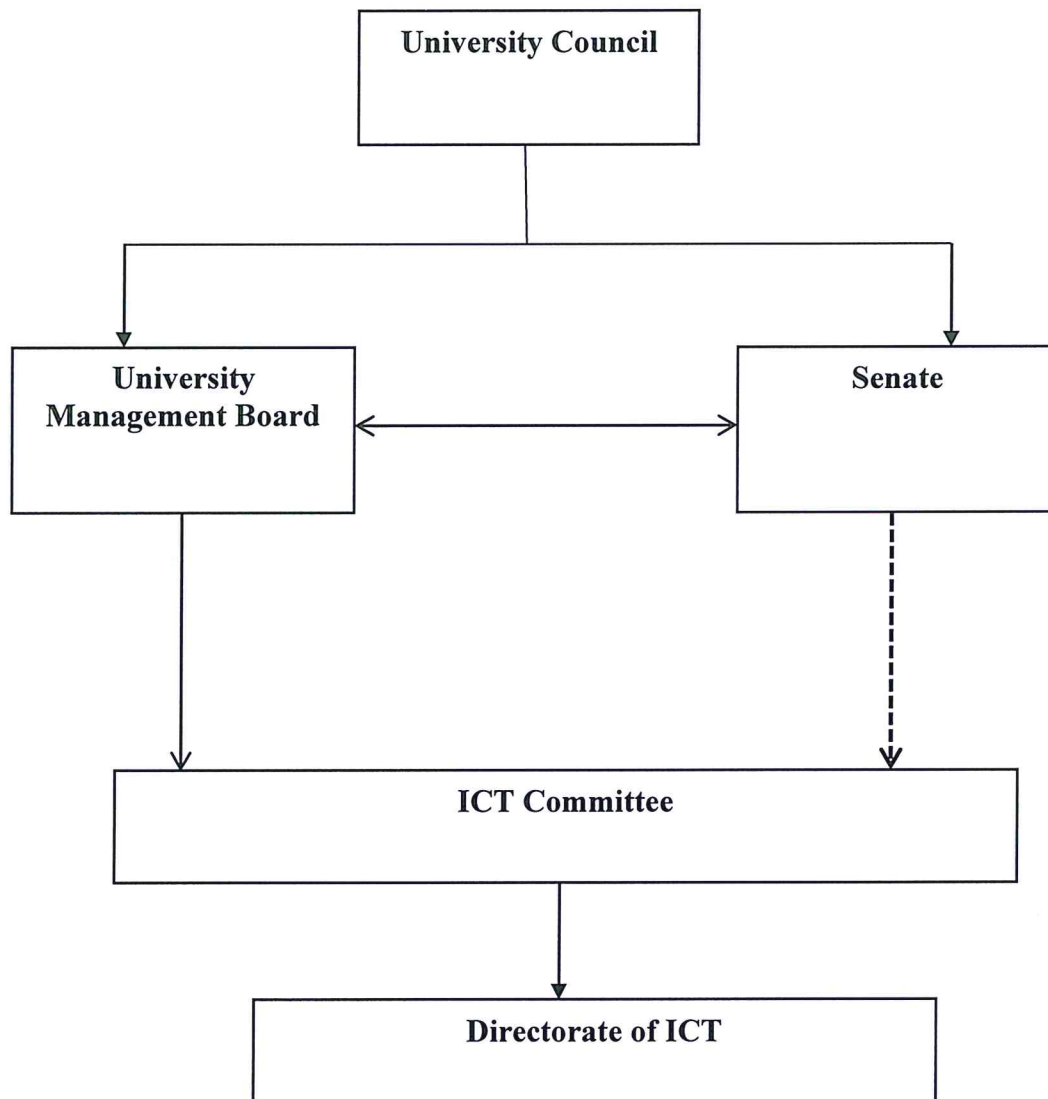


Figure 1: Administrative structures

2.1.3.2.2 Management Structure

The Management Structure for direct implementation of the Policy shall be as follows:

a) The Council

The University Council as supreme governing body and the ultimate authority shall be responsible for:

- i. Approval of the Policy;
- ii. Ensuring that the institution fulfills its responsibilities in the implementation of this Policy; and
- iii. Monitoring the implementation of the Policy through annual progress reports. Council will discharge this responsibility through the administrative and management structures of the University.

b) The Vice-Chancellor

The Vice-Chancellor shall:

- i. Be the custodian of this Policy; and
- ii. Appoint ICT Committee.

c) The Deputy Vice Chancellor (AFD)

As the Head of the Division, the Deputy Vice Chancellor/Administration, Finance and Development to ensure that all employees have access and ensure proper implementation of the Policy.

d) The Director ICT

DICT will be managed by an appropriately skilled team headed by a Director to be appointed on three (3) year term basis renewable once. The Director will be backed by an elaborately structured pool of specialists and secretariat staff. The staff may be seconded from the teaching Departments.

It is clear that the functions of DICT are cross-cutting in nature. The Director will report directly to the Deputy Vice Chancellor, AFD.

d) Chairpersons/Heads of Departments

The Chairpersons/Heads of Departments ensure that ICT equipment is well managed and used and report any malfunction and misuse of ICT equipment.



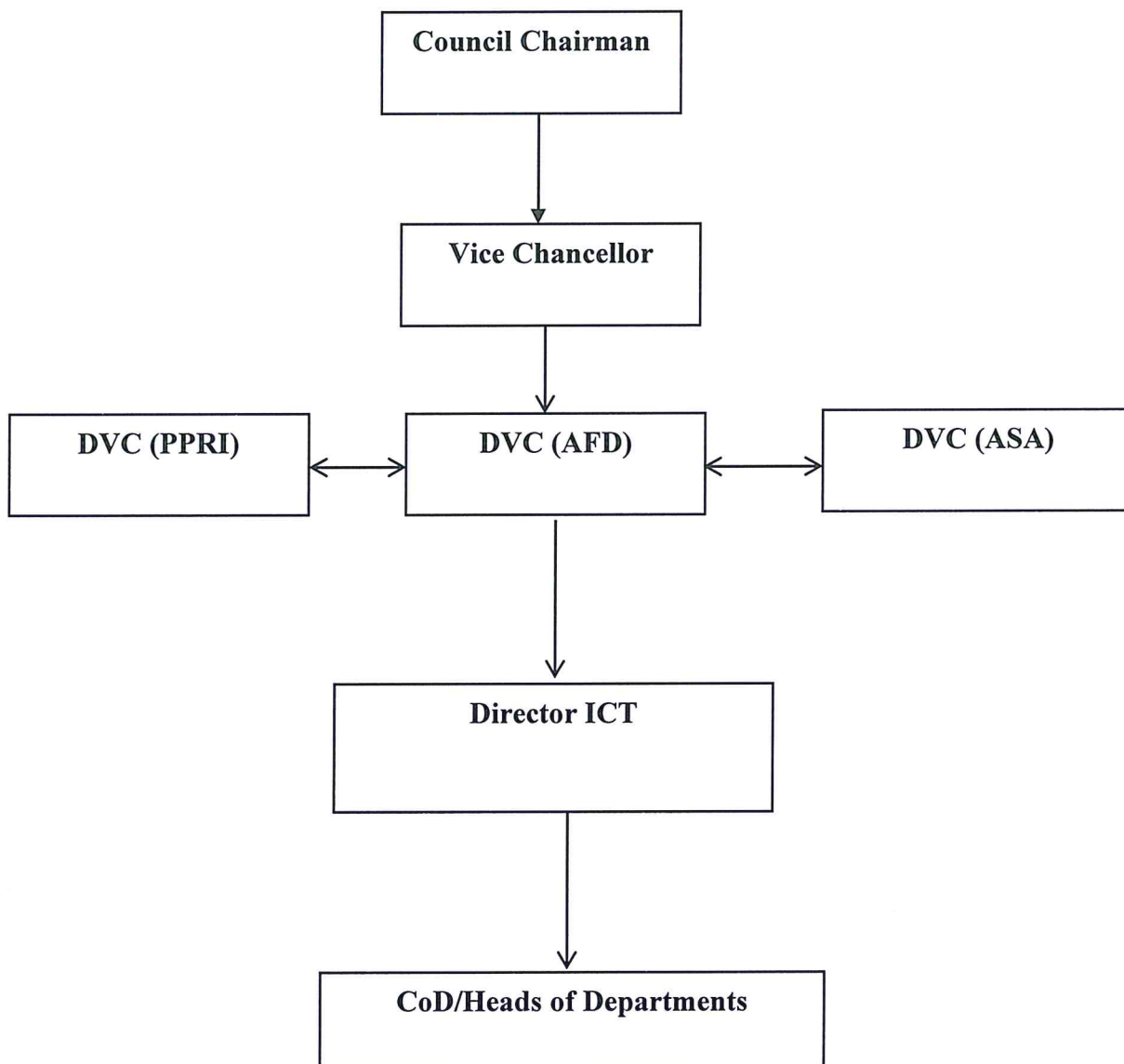


Figure 2: Management structures

2.1.6 Capacity Building

To keep up with rapid technology changes:

- i. The ICT director in conjunction with user Departments shall regularly determine the overall ICT training and capacity building needs for technical employees and other staff;
- ii. The director with the assistance of all ICT Directorates' technical staff shall regularly review emerging technologies and assess internal capacities available for in-house training. In absence of relevant internal capacity, the training services will be outsourced; and
- iii. The University will provide the employees with ICT skills and capabilities necessary for use in emerging technologies introduced for use by its employees.

2.1.7 DICT Sustainability

In order to sustain the operations of the various sections of DICT and be able to maintain quality service, the section will generate enough funds to cater its own operational expenses, in principle, researchers, lecturers, students and other personnel may not have to pay for services on delivery but arrangement must be made through backup resources to improve the ICT sections. Such funds may be drawn from student fees, income generated from training and consultancy and any other viable source of income.

2.1.8 Resource Ownership

This may apply to:

- i. All mobile computing and storage devices used by Kibabii University constituency in the performance of their duties, and to all Kibabii University Restricted Data when accessed through, or stored on, mobile computing and storage devices, regardless of the device's ownership;
- ii. Kibabii University Restricted Data may not be released for storage on, or access through, devices that do not meet the following requirements:
 - a) Restricted Data stored on mobile computing and storage devices must be encrypted;
 - b) Any and all mobile computing devices used within Kibabii University information and computing environments must meet all applicable UF encryption standards. mobile computing devices purchased with Kibabii University funds, including, but not limited to contracts, grants, and gifts, must also be recorded in the unit's information assets inventory;and
 - c) Kibabii University information security policies applicable to desktop or workstation computers apply to mobile computing devices.
- iii. For each ICT resource (Device), an 'owner' will be defined. Ownership of specific ICT resources will be determined by the University Management. For example, the Finance Department would be the owner of the finance database server computer and the financial database. However, the expertise to manage such resources will be drawn from DICT. Ownership of common ICT resources (e.g. communication infrastructure) will be delegated to DICT; and
- iv. All in-house developed systems will remain the property of KIBU and and all efforts will be made to protect the innovation (no person has the right to copy or distribute such systems to other parties).

2.1.9 Service Level Agreements (SLAs) and Service Charters

In order to continuously offer quality services to its clients DICT will enter into Service Level Agreements (SLAs) and sign Service Charter with its clients. This will ensure that the Directorate will always meet its client's needs.



2.2: ICT EQUIPMENT USE POLICY

2.2.1 Introduction

As part of its educational mission Kibabii University acquires and maintains computers and develops computer systems and networks. These Information Technology resources are intended for University-related purposes, including direct and indirect support of the University's instruction, research, and service missions; University administrative functions; student and campus life activities; and the free exchange of ideas within the University community and among the University community and the wider local, national, and world communities", to clarify on the specific functions and authorised activities.

2.2.2 Purpose

The purpose of this policy is multi-faceted, encompassing several key objectives. First, it serves to establish clear guidelines for the appropriate and responsible utilization of computing and networking resources by Kibabii University's academic, administrative staff, and students. Second, it provides a framework for addressing external complaints related to perceived or actual misuse of ICT equipment. Third, the policy is designed to safeguard the privacy and integrity of data stored on ICT equipment. Additionally, it aims to mitigate potential risks and losses stemming from security threats, including virus attacks and network compromises. Furthermore, the policy strives to minimize disruptions and ensure the high availability and efficiency of the network, which is essential for the university's operations. Lastly, it promotes user awareness and responsibility in protecting the university's ICT equipment.

2.2.3 Responsibilities

- i. The Holder of a computer account or computer system connected to the University is responsible for the actions associated with the computer account or computer system;
- ii. Users must ensure that they use all reasonable means to protect their equipment and (if applicable) their account details and passwords;
- iii. Engaging in any activities referred to in the unacceptable use Policy is prohibited and may result in a temporary revocation of access to all electronic resources or disciplinary action being taken; and
- iv. Users are expected to assist ICT support staff with investigations into suspected violations or breaches of security.

2.2.4 General Principles and Guidelines

- i. All users shall ensure that ICT equipment is fitted with effective power surge protectors;
- ii. All University Computers shall have working surge protected UPS which will be tested from time to time;
- iii. The University shall at all times have an ICT workshop room where regular testing, repairing and servicing of the ICT equipment shall be done;



- iv. Only authorized users shall have access to ICT equipment. Access and privileges on ICT equipment shall be managed by the ICT Service Unit. Authentication of users shall be enforced where applicable;
- v. ICT equipment and resources provided by University to its staff and students remains University property at all times;
- vi. All the users of ICT equipment shall adhere to properly documented operational guidelines to ensure safe usage of ICT equipment. The guidelines shall be managed by the ICT Service Unit;
- vii. Users must adhere to the confidentiality rules governing the use of passwords and accounts and details of which must not be shared;
- viii. Passwords must not be disclosed to anyone even if the recipient is a member of IT services support staff. Temporary password provided by IT Services support staff to users must be changed immediately following a successful login;
- ix. Users must respect the rights, privacy and property of others;
- x. University ICT equipment are intended to be used for University purposes only. Where private user is permitted, it must be in consistent with the terms of University rules and guidelines and terms of service and staff respectively; and
- xi. The University shall at all times maintain the non-interruptible power supply to the ICT equipment.

2.2.5 Enforcement

- i. Violation of this Policy will be handled in accordance with procedures established for staff or student discipline.
- ii. The ICT Services Unit and ICT Committee will ensure that the above guidelines are adhered to.
- iii. The University Administration Division will ensure that all the staff and students sign the ICT Equipment Use Agreement upon admission to KIBU

2.3: CHANGE MANAGEMENT POLICY

2.3.1 Introduction

ICT infrastructure is critical to the effective operation of KIBU. The University strives to continually maintain and improve this vital resource. However, as our infrastructure continues to grow, it becomes more and more complex. As our interdependencies – between systems, between people, and between people and systems – continue to grow, it is prudent that the most well-intentioned change can cause unexpected hardship to technology users if the implications of the change are not mapped out in advance.

2.3.2 Purpose

The purpose of the Change Management Policy is to manage changes in a rational and predictable manner so that staff can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of our vital ICT infrastructure. The purpose of this Policy is not to frustrate changes or to question the rationale of changes. Rather, it is to make sure that changes have their intended impact while avoiding unintended consequences.

2.3.3 Changes to the IT infrastructure

Changes to the IT infrastructure can be necessary for many reasons, ranging from the need to fix a hardware problem to the need to update software. Here is a non-exhaustive list of change sources:

- i. Periodic maintenance;
- ii. User requests;
- iii. Hardware and/or software upgrades;
- iv. Acquisition of new hardware and/or software;
- v. Other changes or modifications to the infrastructure;
- vi. Environment changes (such as changes to the electrical system); and
- vii. Operations scheme schedule changes.

2.3.4 Change Management Group

The ICT Implementation Committee will constitute a Change Management Group (CMG) comprising ICT experts and other stakeholders in KIBU. The CMG will receive all requests for change. Requests for changes must be made through the change request form.

The CMG will have the following terms of reference.

- i. They will meet once a week to review all requests for change with the requestors;
- ii. They will be responsible for mapping out the potential impact of the change of various stakeholders;
- iii. They will be responsible for communication with all stakeholders' critical information about how a given change will impact their work;

- iv. They will establish the urgency and potential impact of a proposed change. High impact changes, for example, might require downtime outside of regular maintenance cycles;
- v. For changes to critical hardware and software systems, the group will establish testing and approval critical in advance of making the change to the IT infrastructure; and
- vi. The group will be accountable for all changes. The group will maintain a change log that documents all requests for change, plans and scheduling for the change, and outcomes.

2.3.5 Change Management Process

The change management process will include the following steps. Each of these steps must be completed for every change.

- i. **Requestor fills out change management form:** The form includes space for detailed description of the proposed change, the systems involved, the business units impacted, and the location impacted. The requestor also makes an initial estimation of the urgency and potential risk of the change, how much implementing the change will cost, and how much downtime the change may require;
- ii. **The CMG review and approves the change:** At its regular meeting the change management group will review the Request for Change. The group will evaluate the requestor's proposal in light of their knowledge of KIBU technologies, business processes, and interdependencies. They may adjust some of the estimates;
- iii. **The CMG may send the request back to the requestor for further detail and study, if needed:** Reasons for sending a request back can include the following:
 - i. Inadequate planning;
 - ii. Inadequate fall back plans (in case change fails);
 - iii. The timing of the change will negatively impact a key business process, such as year-end accounting;
 - iv. Adequate resources are not readily available for the project; and
 - v. Staff is not available to make the change in the time specified.
- iv. **The CMG assigns responsibility for making the change:** If the request is approved, the change management group will assign responsibility for making the change to qualified personnel. They will establish specifications and testing requirements depending on the nature of the change;
- v. **The CMG will communicate with stakeholders:** The change management group will make sure that all stakeholders are aware of the nature and potential impact of the proposed change. For change requiring downtime outside of regular maintenance cycles the group will also get feedback from stakeholders on appropriate scheduling downtime;
- vi. **The CMG will track progress on the proposed changes and have final approval:** Personnel tasked with working on the change will report back to the group regarding progress on planning and testing. When the proposed change has been tested, and appropriate fallback has been planned in case of a problem, the group will approve the changes. They will schedule the change – if it requires time outside of regular maintenance cycles – and will communicate with stakeholders; and



- vii. **The CMG will perform a follow-up on all changes:** At their regular change management meetings, the change management group will perform post-mortems on all changes. Successful changes, as well as reasons why a change did not go through as planned, and lessons learned from the experienced will be included in the change log.

2.4: ICT RESOURCE ACQUISITION POLICY

2.4.1 Introduction

ICT resources are capital intensive, thus their acquisition needs to be well planned, controlled and coordinated. Clear Policy guidelines need to be drawn to guide acquisition of such resources.

2.4.2 Purpose

This Policy will put in place guidelines to procedures and processes to be followed whenever ICT equipment and services are being acquired.

2.4.3 Make or Buy

For each ICT service or application the University management will take the decision whenever it should be developed 'in-house' or acquired from external sources based on the following key considerations.

Key factors that favor the *make decision* includes the following:

- i. A customized ICT application or service that is totally responsive to the institution's very specific needs;
- ii. Increase ease in developing software due to the growth of Rapid Application development tools and systems;
- iii. Ease of adapting software to rapidly changing user needs without having to coordinate the requirements with vendors; and
- iv. Developing professional competence in software development.

Key factors that favor the *buy decision* include the following:

- i. Ability to gain access to specialized skills that cannot be retained or for which there is insufficient need to have continuously available;
- ii. Cost of building software is still extremely costly;
- iii. Staff utilization; and
- iv. Ability to make short-term commitment for ICT development support instead of having to make major investment in staff recruitment and professional training.

2.4.5 Outsourcing of Services

Owners are allowed to hire certain support services from external professional providers only if cost-effective and if the expertise involved is not (yet) available in the University and will (cannot) not be developed by DICT.

2.5: ICT RESOURCE OUTSOURCING AND COLLABORATION POLICY

2.5.1 Introduction

KIBU has a fully fledged data centre that provide technology services, with inbuilt infrastructure requirements such as reliable power supplies, precision cooling system, fire suppression system, CCTV surveillance system and centralised monitoring equipment. The data centres is designed to support IT business continuity and are therefore managed by teams of specialist ICT staff. The services available at the data centre can be utilized by other external entities, partners and collaborators either for commercial or research collaboration purposes.

2.5.2 Purpose

This Policy will put in place guidelines to procedures and processes to be followed whenever data centre services are being provided to other entities.

2.5.3 Procedure for Outsourcing of ICT Services from the University

The procedure below will be followed in Outsourcing of ICT services and collaboration engagements with the University

2.5.3.1 The University will receive the service request from the entity requesting for the service.

The request shall be made to the Office of the Vice Chancellor;

2.5.3.2 Upon receipt of the request, the Directorate of ICT will assess viability of provisioning the service to the external entity;

2.5.3.3 The Directorate will prepare a report be presented to the University management board for consideration and decision making; and

2.5.3.4 The outcome of the UMB recommendation shall be communicated to the interested party in writing.

2.6: ANTI-VIRUS POLICY

2.6.1 Introduction

A virus is a piece of potentially malicious software that will cause some unexpected or undesirable event. Viruses can be transmitted via e-mail or instant messaging attachments, downloadable Internet files, diskettes, and CDs. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user. A virus infection can be very costly to KIBABII UNIVERSITY in terms of lost data, lost staff productivity, and/or lost reputation (e-mail attachments).

2.6.2 Purpose

As a result, one of the goals of KIBU is to provide a computing network that is virus-free. The purpose of this Policy is to provide instructions on measures that must be taken by KIBU employees to help achieve effective virus detection and prevention.

2.6.3 General Policy

- i. The most current available version of the anti-virus software package will be taken as the default standard and shall be installed in a University's Application Server;
- ii. All computers attached to the KIBU network must have standard, supported anti-virus software installed. This software must be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date (current definitions taking updates of previous date);
- iii. Any activities with the intention to create and/or distribute malicious programs onto the KIBU network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited;
- iv. If an employee receives what he/she believes to be a virus or suspects that a computer is infected with a virus, it must be reported to the ICT Directorate immediately at icthelpdesk@kibu.ac.ke or University's main telephone through extension 2351. Report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material;
- v. No employee should attempt to destroy or remove a virus, or any evidence of that virus, without direction from the ICT Department; and
- vi. Any virus-infected computer will be removed from the network until it is verified as virus-free.

2.6.4 Rules for Virus Prevention

- i. Always run the standard anti-virus software provided by KIBU;
- ii. Never open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source;
- iii. Never open any files or macros attached to an e-mail from a known source (even a coworker) if you were not expecting a specific attachment from that source;



- iv. Be suspicious of e-mail messages containing links to unknown Web sites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link;
- v. Files with the following filename extensions are blocked by the e-mail system: [list extensions]. [Describe any workaround procedures for sending/receiving business-critical files with banned extensions, such as use of a file compression utility;
- vi. Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media;
- vii. Avoid direct disk sharing with read/write access. Always scan a floppy diskette/flash disk for viruses before using it;
- viii. If instructed to delete e-mail messages believed to contain a virus, be sure to also delete the message from your Deleted Items or Trash folder;
- ix. Back up critical data and systems configurations on a regular basis and store backups in a safe place; and
- x. Regularly update virus protection on personally-owned home computers that are used for business purposes. This includes installing recommended security patches for the operating system and other applications that are in use.

2.6.5 ICT Directorate Responsibilities

The following activities are the responsibility of the KIBU ICT Directorate:

- i. The ICT Directorate is responsible for maintaining and updating this Anti-Virus Policy. Copies of this Policy will be posted at University's Intranet or shared folder in known network location. Check one of these locations regularly for updated information;
- ii. The ICT Directorate will keep the anti-virus products it provides up-to-date in terms of both virus definitions and software version in use. The ICT Directorate shall configure automatic up-dates of anti-virus definitions on a daily basis (9 pm) with definitions automatically pushed to client PCs on start-up each day;
- iii. The ICT Directorate will apply any updates to the services it provides that are required to defend against threats from viruses;
- iv. The ICT Directorate will install anti-virus software on all KIBU owned and installed desktop workstations, laptops, and servers;
- v. The ICT Directorate will assist employees in installing anti-virus software according to standards on personally-owned computers including laptops that will be used for business purposes. The ICT Directorate [will] provide anti-virus software in these cases;
- vi. The ICT Directorate will take appropriate action to contain, remove, and assist in recovery from virus infections. In order to do so, the ICT Directorate may be required to disconnect a suspect computer from the network or disconnect an entire segment of the network;
- vii. The ICT Directorate will perform regular anti-virus sweeps of [system(s) name] files; and
- viii. The ICT Directorate will attempt to notify users of KIBU systems of any credible virus threats via e-mail or telephone messages. Virus reports will not be acted upon until

validated. Employees should not forward these or any virus warning messages in order to keep network traffic to a minimum.

2.6.6 Department and Individual Responsibilities

The following activities are the responsibility of KIBU Departments and employees:

- i. Departments must ensure that all Departmentally-managed computers have virus protection that is in keeping with the standards set out in this Policy;
- ii. Departments that allow employees to use personally-owned computers for business purposes must implement virus protection processes and procedures that are in keeping with the standards set out in this Policy;
- iii. All employees are responsible for taking reasonable measures to protect against virus infection; and
- iv. Employees must not attempt to either alter or disable anti-virus software installed on any computer attached to the KIBU network without the express consent of the ICT Department.

2.6.7 Enforcement

Any employee who is found to have violated this Policy may be subject to disciplinary action as may be determined by University's disciplinary committee or code of regulation.

2.7: BACKUP POLICY

2.7.1 Introduction

Data is one of KIBU University most important assets. In order to protect this asset from loss or destruction, it is imperative that it be safely and securely captured, copied, and stored.

2.7.2 Purpose

The purpose of this Policy is to protect University Data from loss or destruction by specifying reliable backups that are based upon the availability needs of each unit and its data.

2.7.3 Data Back-Up

This Policy refers to the backing up of data that resides on KIBU servers. Servers and the files and/or data types on these servers that are covered by this Policy include:

- i. KIBU-Application server Hosts the main University database;
- ii. KIBU-Email server Hosts the University email system;
- iii. KIBU-web and proxy server Hosts the University's Intranet); and
- iv. KIBU-authentication server Controls accessibility to the intranet.

This Policy does not refer to backing up of data that resides on individual PC or notebook hard drives. Responsibility for backing up data on local desktop systems or laptops rests solely with the individual user. It is strongly encouraged that end users save their data to the appropriate server listed above in order that their data is backed up regularly in accordance with this Policy.

In addition, files that are left open at the time the backup procedure is initiated may not be backed up. End users are reminded to save and close all files, as well as all related applications, prior to the backup procedure window.

It is the responsibility of server administrators to ensure that all new servers be added to this Policy, and that this Policy be applied to each new server's maintenance routine. Prior to deploying a new server, a full backup must be performed and the ability to perform a full restoration from that backup confirmed. Prior to retiring a server, a full backup must be performed and placed in permanent storage.

2.7.4 Backup Schedule

Backups are conducted both Manually/automatically. The University shall acquire a backup utility, with features for both Manual and automatic backup of selected files or resources.

The servers listed above must be backed up according to the following procedure. This method ensures that no more than one day's working data will be missing in the event of a data loss incident:

- i. All backup tapes (annual backup – permanent) are to be labeled using the following labeling conventions: KIBU-YRx (where x = year);



- ii. All backup tapes stored on site are to be stored in the ICT Designated Backup Safe;
- iii. All backup media stored off site are to be stored in a designated off-site location known to the ICT Department's staff and managed by system administrators;
- iv. All backups will take place between the hours of 9 pm and 1 am. This timeframe has been selected to minimize the impact of server downtime on end users that may be caused by the need to take servers offline in order to perform the backup itself. If this backup schedule in some way interferes with a critical work process, then the affected user(s) is to notify the ICT Department so that exceptions or alternative arrangements can be made;
- v. Incremental backups (only files changed since the last backup) will be performed daily, Monday through Friday. These tapes will be stored onsite during the following backup cycle. At the end of the latter cycle, the daily hot-swap disks will be removed to a predetermined offsite location for storage for 5 weeks. When this 5 week period has elapsed, the hot-swap disk will be brought back on site for reuse for a period not to exceed one year;
- vi. A full backup will be performed each Friday. This Hot-Swap Disk will be stored on site during the following backup cycle. At the end of the latter cycle, the weekly disk will be removed to a predetermined offsite location for storage for 5 weeks. When this 5 week period has elapsed, the disk will be brought back on site for reuse for a period not to exceed one year;
- vii. A full backup will be performed at the end of each month. This disk will be immediately removed to a predetermined offsite location for permanent storage. These disks will never be reused;
- viii. All server backups performed must be noted in the server backup log immediately upon completion. All server backup log sheets must be kept in an appropriately labeled three-ring binder in an agreed-upon, centralized location. The log must include:
 - a. Server name;
 - b. Date and time of backup;
 - c. Name of administrator performing the backup;
 - d. Files backed up and/or skipped;
 - e. Software used to perform the backup;
 - f. Backup medium used and its label/name; and
 - g. Whether the backup was successful or not.
- ix. If, for some reason, the backup cannot be completed, is missed, or crashes, then it must be completed by 9:00 a.m. the following morning. The reason for non-completion of the originally scheduled backup must be noted in the server backup log. In addition, if a backup fails more than one day in a row, end users in the organization must be notified; and
- x. If a disk is discovered to be damaged or corrupt, then the disk must be destroyed to prevent further use and replaced with a new one.

2.7.5 Managing Restores

The ultimate goal of any backup process is to ensure that a restorable copy of data exists according to Recovery Time Objectives and Recovery Point Objectives. If the data cannot be restored, then the process is useless. As a result, it's essential to regularly test one's ability to restore data from its storage media. Consequently:

- i. All daily disks must be tested at least once every 3 months to ensure that the data they contain can be completely restored;
- ii. All weekly disks must be tested at least once every 3 months to ensure that the data they contain can be completely restored; and
- iii. All monthly disks must be tested at least once every 2 years to ensure that the data they contain can be completely restored.

Data will be restored from a backup if:

- i. There is an intrusion or attack;
- i. Files have been corrupted, deleted, or modified;
- ii. Information must be accessed that is located on an archived backup; and
- iii. Verification of work done by officers is in dispute.

In the event a data restore is desired or required, the following Policy will be adhered to: The individual responsible for overseeing backup and restore procedures is an ICT officer designated by Head of ICT Department. If a user has a restore request, they can contact Head of ICT Department by calling extension 2351, sending an e-mail to icthelpdesk@kibu.ac.ke, or filling out and submitting a request form located at [\[www.kibu.ac.ke\]](http://www.kibu.ac.ke).

In the event of unplanned downtime, attack, or disaster, consult KIBU's Disaster Recovery Plan for full restoration procedures.

In the event of a local data loss due to human error, the end user affected must contact the ICT Department and request a data restore. The end user must provide the following information:

- i. Name;
- ii. Contact information;
- iii. Name of file(s) and/or folder(s) affected;
- iv. Last known location of files(s) and/or folder(s) affected;
- v. Extent and nature of data loss;
- vi. Events leading to data loss, including last modified date and time (if known); and
- vii. Urgency of restore.

Depending on the extent of data loss, a daily disk, weekly disks, or combination of both will need to be used. The timing in the cycle will dictate whether or not these disks are onsite or offsite. Hot-Swap Disks must be retrieved by the server administrator or pre-determined replacement. If disks are offsite and the restore is not urgent, then the end user affected may be required to wait up to 2 days for a time- and cost-effective opportunity for the disk(s) to be retrieved. If the data loss was due to user error or a lack of adherence to procedure, then the end user responsible may be required to participate in a tutorial on effective data backup practices.

2.8: E-MAIL ACCEPTABLE USE POLICY

2.8.1 Introduction

E-mail is a critical mechanism for business communications at KIBU University. However, use of KIBU's electronic mail systems and services are a privilege, not a right, and therefore must be used with respect and in accordance with the goals of KIBU.

2.8.2 Purpose

The objectives of this Policy are to outline appropriate and inappropriate use of KIBU's e-mail systems and services in order to minimize disruptions to services and activities, as well as comply with applicable policies and laws.

2.8.3 Account Activation/Termination

E-mail access at KIBU is controlled through individual accounts and passwords. Each user of KIBU's e-mail system is required to read and sign a copy of this E-Mail Acceptable Use Policy prior to receiving an e-mail access account and password. It is the responsibility of the employee to protect the confidentiality of their account and password information.

All employees of KIBU are entitled to an e-mail account. E-mail accounts will be granted to third party non-employees on a case-by-case basis. Possible non-employees that may be eligible for access include:

- i. Contractors/ Consultants; and
- ii. Part-time staff (such as Interns).

Applications for these temporary accounts must be submitted in writing to Head of ICT Department. All terms, conditions, and restrictions governing e-mail use must be in a written and signed agreement.

E-mail access will be terminated when the employee or third party terminates their association with KIBU, unless other arrangements are made. KIBU is under no obligation to store or forward the contents of an individual's e-mail inbox/outbox after the term of their employment has ceased.

2.8.4 General Expectations of End Users

Important official communications are often delivered via e-mail. As a result, employees of KIBU with e-mail accounts are expected to check their e-mail in a consistent and timely manner so that they are aware of important University announcements and updates, as well as for fulfilling business- and role-oriented tasks.

E-mail users are responsible for mailbox management, including organization and cleaning. If a user subscribes to a mailing list, he or she must be aware of how to remove himself or herself from the list, and is responsible for doing so in the event that their current e-mail address changes.

E-mail users are also expected to comply with normal standards of professional and personal courtesy and conduct.



2.8.5 Appropriate Use

Individuals at KIBU are encouraged to use e-mail to further the goals and objectives of KIBU. The types of activities that are encouraged include:

- i. Communicating with fellow employees, partners of KIBU, and clients within the context of an individual's assigned responsibilities;
- ii. Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities; and
- iii. Participating in educational or professional development activities.

2.8.6 Inappropriate Use

KIBU's e-mail systems and services are not to be used for purposes that could be reasonably expected to cause excessive strain on systems. Individual e-mail use will not interfere with others' use and enjoyment of KIBU's e-mail system and services. E-mail use at KIBU will comply with all applicable laws, all KIBU policies, and all KIBU contracts.

The following activities are deemed inappropriate uses of KIBU systems and services and are prohibited:

- i. Use of e-mail for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses);
- ii. Use of e-mail in any way that violates KIBU's policies, rules, or administrative orders, including, but not limited to, discrimination, gender-bias;
- iii. Viewing, copying, altering, or deletion of e-mail accounts or files belonging to KIBU or another individual without authorized permission;
- iv. Sending of unreasonably large e-mail attachments. The total size of an individual e-mail message sent (including attachment) should be 10 MB or less;
- v. Opening e-mail attachments from unknown or unsigned sources. Attachments are the primary source of computer viruses and should be treated with utmost caution.
- vi. Sharing e-mail account passwords with another person, or attempting to obtain another person's e-mail account password. E-mail accounts are only to be used by the registered user; and
- vii. Excessive personal uses of KIBU e-mail resources. KIBU allows limited personal use for communication with family and friends, independent learning, and public service so long as it does not interfere with staff productivity, pre-empt any business activity, or consume more than a trivial amount of resources. KIBU prohibits personal use of its e-mail systems and services for unsolicited mass mailings, non-KIBU commercial activity, political campaigning, dissemination of chain letters, and use by non-employees.

2.8.7 Monitoring and Privacy

The e-mail systems and services used at KIBU are owned by the University, and are therefore its property. This gives KIBU the right to monitor any and all e-mail traffic passing through its e-mail system. While the University does not actively read end-user e-mail, e-mail messages may be inadvertently read by IT staff during the normal course of managing the e-mail system.

In addition, backup copies of e-mail messages may exist, despite end-user deletion, in compliance with KIBU's records retention Policy. The goals of these backup and archiving procedures are to ensure system reliability and prevent KIBU record loss.

In case the University discovers or has good reason to suspect activities that do not comply with applicable laws or this Policy, e-mail records may be retrieved and used to document the activity in accordance with due process. All reasonable efforts will be made to notify an employee if his or her e-mail records are to be reviewed. Notification may not be possible, however, if the employee cannot be contacted, as in the case of employee absence due to vacation.

Use extreme caution when communicating confidential or sensitive information via e-mail. Keep in mind that all e-mail messages sent outside of KIBU become the property of the receiver. A good rule is to not communicate anything that you wouldn't feel comfortable being made public. Demonstrate particular care when using the "Reply" command during e-mail correspondence.

2.8.8 Reporting Misuse

Any allegations of misuse should be promptly reported to Registrar Administration. If you receive an offensive e-mail, do not forward, delete, or reply to the message. Instead, report it directly to the individual named above.

2.8.9 Disclaimer

KIBU assumes no liability for direct and/or indirect damages arising from the user's use of KIBU's e-mail system and services. Users are solely responsible for the content they disseminate. KIBU is not responsible for any third-party claim, demand, or damage arising out of use the KIBU's e-mail systems or services.

The following disclaimer shall be applied to all outgoing email:

"This email is confidential and intended for the sole use of the individual or entity to which it was addressed. If you have received this email in error please notify the sender immediately and delete this email without disclosing, copying, using, distributing or storing its contents. Kindly note that unless expressly stated, any views or opinions presented in this email are solely those of the author and do not necessarily represent those of KIBABII UNIVERSITY. The recipient should check this email and any attachments for the presence of viruses. The University does not accept liability for any damage caused by this email."



2.8.10 Failure to Comply

Violations of this Policy will be treated like other allegations of wrongdoing at KIBU. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for inappropriate use on KIBU's e-mail systems and services may include, but are not limited to, one or more of the following:

- i. Temporary or permanent revocation of e-mail access;
- ii. Disciplinary action according to applicable KIBU policies; and
- iii. Legal action according to applicable laws and contractual agreements.

2.9: HELP DESK TRIAGE POLICY

2.9.1 Introduction

The primary role of the ICT Directorate is to support end users in completing business tasks. In order to ensure this role is carried out in a timely and high quality manner, a Policy has been established to help assign priority levels to problems or issues reported by end users to the ICT Directorate.

2.9.2 Purpose

The goal of this Policy is to establish service expectations and inform employees at KIBU of the method by which help desk requests will be prioritized and what resolution times can be expected.. The primary role of the IT Department is to support end users in completing business tasks. To ensure this role is carried out in a timely and quality manner, this Policy helps assign priority levels to problems or issues reported by end users to IT.

2.9.3 General Guidelines

2.9.3.1 Before contacting the help desk, try the following:

- a) If data loss isn't a concern, reboot your system if possible; and
- b) Try to find a resolution to the problem yourself by reviewing available documentation, help sheets, and posted FAQs for the system that is presenting problems. This information can be found at KIBU help desk system.

2.9.3.2 Problems and requests designated as Level 1 Severity will take priority. Level 4 Severity issues hold the lowest priority;

2.9.3.3. Problems and requests within a specific priority category will be handled on a first come, first served basis;

2.9.3.4 In some cases, special consideration will be given to mobile and remote employees whose access to University resources is more constrained; and

2.9.3.5 In the event of a natural disaster, failure of a third-party utility (such as electrical power), or some other catastrophic event, stated response and resolution times may be longer.

2.9.4 Priority Categories

The following table shows different priority levels for requests, a brief description of what constitutes each priority category, and timelines for problem response and resolution by the ICT Directorate.

Table 1: Problems and Requests

Severity	Description	Response Time	Resolution Time
Level 1	Critical system is down. Functions not usable. No workaround or alternative is available. Data is corrupted. Many end users are affected. Regulatory/legal deadlines will be missed.	15 Minutes	1 Hour
Level 2	Some functions are usable with severe restrictions. No workaround or alternative is available. Several end users affected.	1 Hour	4 Hours
Level 3	Basic functions are usable with minor restrictions. Workaround or alternative is available. One or more users affected.	4 Hours	Next Business Day
Level 4	Minor problem. Functions are usable. Defect is cosmetic or simply a nuisance.	Next Business Day	3 Days

2.9.6 Contact Information

To report a problem or submit a request, use one of the mechanisms listed below. Kindly state your name, section/faculty/Directorate/Department, e-mail address, telephone number, the nature of the problem you are experiencing, the number of affected users, and the severity of the problem as it relates to your (or your colleagues') ability to complete necessary work.

- Send an e-mail to icthelpdesk@kibu.ac.ke;
- Fill out the job-card / online form located on the intranet at [www.kibu.ac.ke]; and
- Call ICT Directorate main office (2351).

The following ICT Helpdesk procedures/guidelines are recommended:

- Helpdesk receive the requests or inquiry from the end user through a phone call, request memo, physical request and e-mail;
- Helpdesk officer records down the request and assign it a particular code/reference

- iii. Helpdesk officer then inform the user/client his/her code/reference assigned to the request forwarded for future reference and follow up;
- iv. Helpdesk then forward the coded request to Administrator/Director ICT Directorate for scheduling to respective section for action;
- v. Administrator/Director of ICT Directorate then forward the coded request to the relevant section (Repair and Maintenance section, Systems Administration or to procurement or as deem required) for action;
- vi. The necessary action is taken by the relevant section and report is generated based on action; and
- vii. The helpdesk update the inventory of the requests through administration management Section.

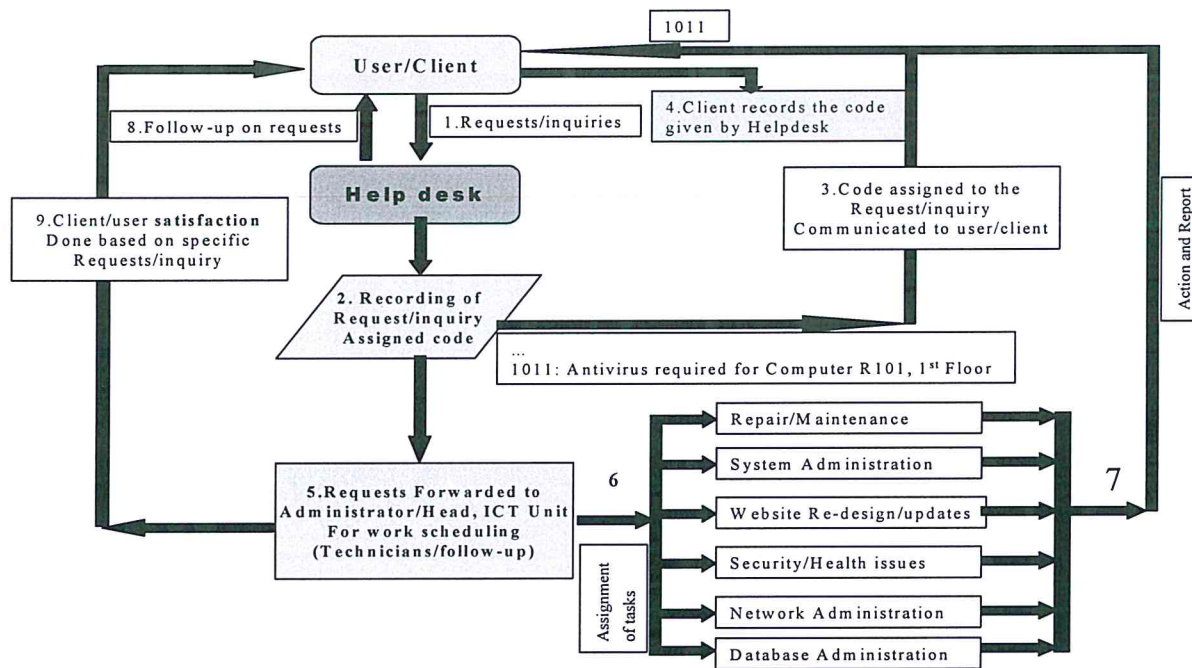


Figure 3: Helpdesk ICT Procedures

2.10: SYSTEM CONTROLS AND SECURITY POLICY

2.10.1 Introduction

The University has invested substantially in ICT resources. These resources are vital in realizing the University's business objectives and are integral to the ability of the University to operate effectively. This Policy establishes general guidelines, rules and regulations for the use and protection of the University's information and ICT systems. The implementation of this Policy will thus promote the availability, integrity and confidentiality of the University's ICT systems.

2.10.2 Purpose

This Policy establishes regulations to ensure comprehensive protections are in place to safeguard all information technology resources. KIBU managers must ensure that protections are in place to protect against accidental or deliberate, unauthorized alteration, destruction, delay, theft, access, use or damage to systems, data, applications, equipment, and telecommunications. This regulation also defines KIBU's ICT security missions, goals, scope, and responsibilities.

2.10.3 Objectives

The objectives of system controls and security Policy are to: -

- i. Create general awareness on appropriate security measures that must be implemented to safeguard the effective operation of the University;
- ii. Communicate the responsibilities for the protection of ICT systems;
- iii. Facilitate the preservation of the integrity and privacy (confidentiality) of the University's information and
- iv. Protect and promote the University's reputation.

2.10.4 Systems Security Control Policy

The University's ICT systems, and the service they provide, will be protected by effective control of security risks at all levels of the organization, providing, managing and operating to ensure that the requirements regarding availability, confidentiality and integrity are preserved;

i. Configurations

For security purpose and business continuity, DICT shall maintain a confidential file of all systems configurations. Accessibility to the file will be restricted to: chief system administrator, the network administrator and the senior most systems developer at the University.

ii. Access

Access to the systems will be restricted to authorized users as determined by the head of a service area.

iii. Breaches

Any breach of this Policy shall be dealt with under the University's Disciplinary Policy and Procedures. In addition, the University may advise law enforcement agencies of the breach where it considers that a criminal offence may have been committed.



iv. Review

The University will establish the ICT Security Committee whose responsibilities will include the review of this aspect of the ICT Policy at intervals of six (6) months and amended as need arises. Any changes shall be communicated to all users of the University's ICT systems.

2.10.5 Physical Security

ICT resources are generally exposed to the risk of unauthorized access, manipulation, disruption and natural disasters. In an effort to protect the ICT equipment and systems and ensure their availability the University will institute appropriate control measures to ensure that its ICT resources are safeguarded. Appropriate controls will be established to limit access to ICT infrastructure, computer equipment and data, commensurate with the acceptable level of risk. The access to the University ICT systems shall be reviewed every six (6) months.

2.10.6 Passwords

The ICT Department shall prevent unauthorized access to the University's corporate computer systems. Such controls shall take the form of passwords in the user identification process.

2.10.7 Data Security

The head of ICT shall develop rules, regulations and guidelines that ensure confidentiality, integrity, availability and safety of all University information.

2.10.8 Copyright and License Agreements

Only licensed software shall be used in the University. Copying and distribution should not be done without the necessary licenses. The head of ICT Department will ensure that all software applications used by the University complies with the relevant licensing agreements, compile all relevant licensing agreements and maintain a record.

Copyright for all software developed in-house for internal use shall remain with KIBU. Code for such software shall remain the property of KIBU and shall not be distributed.

2.10.9 Internet

- a) To ensure productive, appropriate use and to minimize risks, access to the Internet should be available to staff and students for both teaching, learning and administrative work. Users should use the Internet in an effective, ethical and in a lawful manner.
- b) Users should not use the Internet access to view, print, distribute, display, send or receive images, text or graphics of offensive or obscene material or material that violates any Kenyan law.

- c) The University shall maintain a log of sites visited as a means of determining appropriate usage.
- d) The University shall install and maintain firewalls to filter content coming in or going out via the internet and protecting external attacks.

2.10.10 Email

- a) The University encourages the use of email and respects the privacy of users. The University will not routinely inspect, monitor or disclose the contents of email without the consent of the user. However, subject to the requirements for authorization, notification, and other conditions specified in this Policy, the University may inspect, monitor, or disclose email when the University believes that it has a business need to do so. The use of email must be related to the University's business activities.
- b) Use of email is permitted as long as it does not:
 - i) Violate this Policy
 - ii) Degrade the performance of the network and
 - iii) Divert attention from work
- c) The following disclaimer shall be applied to all outgoing email:

“This email is confidential and intended for the sole use of the individual or entity to which it was addressed. If you have received this email in error please notify the sender immediately and delete this email without disclosing, copying, using, distributing or storing its contents. Kindly note that unless expressly stated, any views or opinions presented in this email are solely those of the author and do not necessarily represent those of University. The recipient should check this email and any attachments for the presence of viruses. The University does not accept liability for any damage caused by this email.”

2.10.11 Monitoring and Evaluation

All ICT systems, as with all other assets, are the property of the University. The University therefore reserves the right to monitor these systems to ensure compliance with this Policy. The monitoring of the ICT system activities will be carried out in a manner that respects the rights and legitimate interests of those concerned.

- i) Users of the University's ICT systems should be aware that their activities can be monitored and they should not have any expectation of privacy. In order to maintain their privacy, users of the University's ICT resources should avoid storing information on these systems that they consider private. By using the University's ICT systems, users expressly consent to the monitoring of all their activities within the University's ICT systems.
- ii) During the implementation of this Policy, the University will ensure that there is continuous monitoring and evaluation for efficiency, accountability and transparency. The



Monitoring and Evaluation will be carried out by the ICT internal M&E team in consultation with the ICT Committee.



2.11: WEBSITE POLICY

2.11.1 Introduction

The KIBU website is the electronic representation of the University and its most visible recruiting tool and, as such, should reflect the University's purpose and standards with a consistent look, user-friendly navigation and factual information that work together to present a positive, uniform image. Content will be presented in tone, style and manner specifically for delivery on the web.

2.11.2 Purpose

This Policy establishes conditions for use of, and requirements for KIBU websites. The University encourages faculty and staff to communicate information freely and openly on the World Wide Web within the constraints of existing laws and policies. The publication criteria stipulated in this document include stylistic consistency standards and guidance on the legal and procedural nuances of communicating on the World Wide Web. These guidelines augment existing KIBU computer accounts agreements, KIBU ICT Security Policy, and the KIBU Network Acceptable Use Policy. These requirements are necessary to help ensure the University maintains a professional, up-to-date web presence.

2.11.3 University Website Information Standards

The information referenced through the web must adhere to all University policies and any other governing laws. In addition, it must be directly related to the University's mission and the information should reflect the high quality standards for official publications of the University. Any web pages or sections of those web pages that are largely unusable (for example, due to incorrectly written code or nonfunctioning links), contain incorrect or outdated information may be removed from the web until they are corrected. The University webmaster will attempt to provide reasonable notice of the link or file removal, but reserves the right to act without notice if the situation warrants or if the situation is not corrected within a reasonable amount of time.

2.11.4 Restrictions

Pages related in any way to the programs of the University its faculties and Departments shall be considered official pages. Official University-related and Departmental websites should reside on web servers within the University's network infrastructure. Departments that require outside websites MUST consult ICT Director to obtain written authority.

Websites owned by official vendors of the University under contractual relationship with the University may reside on servers of those vendors provided they abide by the policies specified in this document.

For security reasons, use of downloaded or unit written CGI scripts is prohibited unless approved by Information Technology Services. To request implementation of a script, contact the Help Desk at 2351 or email icthelpdesk@kibu.ac.ke



Use of KIBU web servers for personal monetary gain is strictly prohibited. Links to specifically for-profit sites with the express purpose of conducting business transactions are likewise prohibited. Web pages in the KIBU domain may link to other official pages on this site, other educational or nonprofit organizations, pages created or maintained by KIBU faculty or staff, and online materials for research or educational purposes.

Although student workers may be hired to create and maintain Departmental web pages, students are not allowed to publish (upload) material to the official KIBU website. Web pages created or altered by students should be approved and published by a KIBU faculty or staff member. Passwords that allow an individual to publish material to the web server may not be shared with students.

No official KIBU web page may link to an individual student's web page. Student organizations do not have reserved space on the KIBU web server; however, student organizations with established sites on non-campus servers may link to the KIBU website.

2.11.5 Copyright and Trademark—All Pages

The preferred names for the University are KIBABII UNIVERSITY(KIBU). Use of other names is discouraged.

Misuse of the University name photos or logo on the web in a prejudicial manner is prohibited and liable to prosecution

Authors or originators using trademarks should have express permission of the person(s) or organization(s) owning the trademarks prior to their use.

Use of the KIBU logo or trademark should be sanctioned by the University top management. Authors or originators using photos and images may need the permission of not only the person or organization that owns the photo or image, but also from any persons included within the images.

Any use of other copyrighted material must have the express written permission of the person or organization that owns the copyright. The administration of KIBU reserves the right to require proof of the written permission and to remove the material if that proof cannot be produced.

All portions of these materials are copyright of 2014 KIBU.



2.11.6 Web Oversight

2.11.6.1 Role of University Webmaster

The administration of the core KIBU site and its links are assigned to the University webmaster who is the custodian of the main home page and keeper of its links to other pages. The webmaster can provide guidance and should be used as a point of reference if necessary with developing new sites or pages. The responsibilities of the webmaster are to the University and not to the community-at-large. The webmaster, reporting to the ICT director will:

- i. Monitor and maintain homepage and other pages of the core site
- ii. Maintain a list of current sites located within the kibabiiUniversity.ac.ke domain and the associated unit content owners for those sites.
- iii. Work with the System administrator, Directorate of ICT, ICT committee of academic board and officer in charge of publicity to enforce policies and guidelines related to web publishing.
- iv. Maintain regular communications with unit content managers and supply updates and new guidelines to those individuals.
- v. Report on a regular basis to the director of ICT on the status of the University website as well as new technologies and developments.
- vi. Serve as a constant point of contact and guide on web-related issues.

2.11.6.2 Role of the Director of ICT

The role of the director is to determine Policy for images, organization, and institutional standards relating to the structure of content and design of the homepage and core site pages, as well as implementing rules for other pages hosted on the KIBU server. The director is responsible for:

- i. Planning for the orderly development of the overall institutional site
- ii. Determining the organization of the display of links and the site index
- iii. Making Policy recommendations that support a consistent image and set standards for identification and information on pages at unit levels
- iv. Advising and assisting the webmaster in promoting compliance with policies and procedures

2.11.6.3 Role of Content Manager

Each unit with page linked to the core site or a Department site will designate a content manager with the following responsibilities:

- i. Monitor and maintain pages within their Section;
- ii. Make sure that pages related to the Unit are monitored for accuracy and currency of content, links to other pages or sites, contacts for visitor information and inquiries;



Kibabii ISO 9001: 2015 Certified
Knowledge for Development

Page 39

- iii. Ensure that data is consistent with the Fact Book and other official sources maintained by the Office of Institutional Research;
- iv. Make certain that the unit pages are meeting the approved guidelines for Web publishing; and
- v. Serve as a liaison and communicate with the University webmaster on a regular basis to assure the sites are meeting the necessary requirements; report any new, major developments; and coordinate requests for new pages or sections.

2.11.7 Enforcement and Notification

These policies will be enforced by the University webmaster or through the webmaster by way of Directorate of ICT. Notification will be given for violations and appropriate action will be taken in accordance with these and other mentioned policies.

2.11.8 Social Media

We are happy to engage in social networking conversations through our multiple social media mediums, but comments or posts that are slanderous are liable for prosecution and will be immediately removed.



2.12: ICT DISASTER MANAGEMENT POLICY

2.12.1 Introduction

The Directorate of Information and Communication Technology (ICT) will develop and maintain an ICT infrastructure and information management platform, which is “best in class” in guaranteeing network access to students, staff and other stakeholders while remaining aligned with the University’s requirements. This will provide a robust, reliable and technologically rich, yet focused environment that supports teaching, research, learning and administration across a dispersed campus. ICT will support existing and anticipated business requirements, while also influencing and shaping future developments and innovation across all of the University’s functions, supporting change and organizational transformation as appropriate. This ICT Strategy is fully aligned with the institutional Strategic Plan. ICT Disaster Management Policy is fully aligned with the institutional Disaster Management Recovery Plan. The University considers ICT as a flagship project.

At the center of all these applications and services is the data processed and stored by the systems. This data is very crucial and must be kept safe in such a way that any possible scenario may not lead to loss and subsequent repercussions to the business processes in place. Currently, there is no central storage facility and Disaster Management Policy and Plan. Computer system users individually store their data and information with very minimal safeguard controls in place.

It should be noted that despite KIBU’s advancements in Information and Communications Technology, there still exists several risk factors, that could result into the worst catastrophic disasters of permanent loss of any data or information stored over a period of reliance on the use of Computer and Network based Systems.

The primary aim of this ICT Disaster Management Policy is to provide an action plan in response to a disaster that destroys the University’s central computer systems run by the Computing Services Unit/Department located in the Main Data Centre in the Academic Block.

It is however important to note that, this Policy does not guarantee zero data loss in the event of a computer system related disaster at Kibabii University.

2.12.2 Objectives of the Disaster Management Policy

- i. To develop orderly course of action for restoring critical computing capability within the shortest possible time after the occurrence of a disaster;
- ii. Outline criteria for making decisions to recover and repair data and equipment hosted in the University’s data Centre;
- iii. Provide information about personnel and technical expertise required;
- iv. Identify equipment and facilities necessary for recovery; and
- v. Ensure full restoration of the facility.

2.12.3 Disaster Planning

The Disaster planning process at Kibabii University should start by evaluating the risks currently existing at the University's Data Centre which could spark off a disaster, as highlighted below:

2.12.3.1 Electricity related damages to Equipment and Data

The greatest risk at Kibabii University is the inconsistent and ever fluctuating electricity supply to the Data Centre, through the national electricity grid. This can have severe effects of shortening the lifespan of the equipment and completely destroying the data stored on the storage media attached.

Preventive Measures

- i. The danger posed by the erratic nature of the electricity supply shall be reduced by installing clean power systems (uninterrupted power supply) and power backup systems to run for at least 10 hours in all designated data centers and server rooms at the University;
- ii. The data centre shall be served from two KPLC power substations to guarantee commercial power supply to the data centre;
- iii. The Computing Services Unit/Department shall implement a centralized data storage solution for all University data and information;
- iv. The Computing Services Unit/Department shall implement both real time and regular back up procedures of data hosted at all designated data centers in the University; and
- v. The Computing Services Unit/Department shall implement offsite backup at the secondary location that is geographically separate from the primary site.

2.12.3.2 Fire

The amount of electricity supplied to the University's main data center comes with several electrical connections and fluctuating power supply could at any time result in short circuits. Short circuits are known to be very common causes of fire outbreaks, which could destroy the equipment and data stored in the Data Centre.

Preventive Measures

- i. Installation of fire and smoke detectors in the Data Centre;
- ii. Installation of fire suppression systems in the Data Centre;
- iii. Installation of hand-held fire extinguishers in visible locations, throughout the building;
- iv. Staff shall be required to undergo training on the proper firefighting procedures in the event of a fire; and
- v. Periodic inspection of the facility by University Electricians at least thrice a year, to eliminate any possible short circuits that may cause fires.

2.12.3.3 Flooding and Leakages

The current Data center faces the risk of water leakages emanating from the air-conditioning units installed there-in.

There is also the possibility of flooding resulting from rain water over flow, from the windows of the facility.

Preventive Measures

- i. Periodic service maintenance shall have to be done for the air-conditioning units in the facility, in order to avert the occurrence of water leakages;
- ii. Periodic inspection of the facility by the University Estates and Works Department, to eliminate any possible causes of flooding and leakages; and
- iii. Installation of water sensor systems that alerts techies in the event of water leakage.

2.12.3.4 Lightning

There is always the looming risk of a lightning bolt striking in this part of the world. If this struck it could result into the permanent damage of the equipment within the data center.

Preventive Measures

- i. Lightening Arresters shall be installed and maintained on the roof of the building housing the Data center; and
- ii. The Computing services unit shall ensure that the centralized data storage unit has provisioned proper earthing/grounding for data storage equipment.

2.12.3.5 Computer Crime

Computer related crimes are on the increase in the country and world over. The systems at Kibabii University would be an obvious target for hackers, crackers, Theft, Terrorism and Sabotage. This unauthorized access to the system could lead to the tampering or damage to the data hosted by the systems.

Preventive Measures

- i. The Computing Services Unit shall implement both software and hardware security controls to avert any hacking attempt into the University's computer and network systems e.g. Firewalls, Access Control lists;
- ii. The Computing Services Unit shall implement both real time and regular back up procedures of data hosted at all designated data centers in the University;
- iii. The University's security office shall increase the vigilance of patrols around the facility,

- especially during the nights;
- iv. The door to the datacenter should always be securely locked and access keys only issued to authorized personnel;
- v. All persons accessing the data centre facility shall get authorized by the Director, ICT and record the reasons for accessing the data centre. Biometric access shall be implemented for ease of tracking the access logs; and
- vi. Adequate lighting shall be provided around the facility during the nights.

2.12.4 Disaster Preparation

2.12.4.1 Replication facilities

The University shall set up a number of replication facilities (hot sites) to mirror all the data hosted in the main data center. Any of these sites will automatically be the temporal main hosting site in case a disaster befell the main data center, before the facilities in the main data center are restored.

The following options shall be considered in choosing the alternate replication facilities.

- i. Setting up a hot site data center within the University Campus; and
- ii. Set up a Warm site data center with a hosting company (private or public cloud) at a cost.

2.12.5 Replacement Equipment

In case of any disaster there shall be a sizeable amount of equipment damage/loss that will have to be replaced in order for the facility to be restored. The following shall therefore have to be in place:

- i. Preparation of a complete inventory of all the components of each computer and network system and their software that must be restored after a disaster by the Computing Services Unit;
- ii. Provisions within the University's Procurement procedure to allow for emergency procurement situations like disasters;
- iii. Prequalified supplier's/service providers to provide replacement equipment in case of disaster; and
- iv. Service Level Agreement with equipment vendors that allows equipment replacement in case of emergency e.g. SMARTNET with Cisco.

2.12.6 Backups

The greatest insurance to computer data loss is making regular backups of the original data. The Computing Services Unit shall therefore implement backup processes on external hard drive infrastructure for all University data and information in the following ways:



- i. Real-time data backup within the main Data Centre;
- ii. Real-time data off- site backup;
- iii. Periodic data backup; and
- iv. Periodic data backup of the site at the Hosting Company.

2.12.7 Backup Procedure

Every Application system running within the University shall define and implement both automatic and scheduled back up procedures, in line with the available facilities, hardware and software.

The Developers of the application systems shall clearly provide functionality for back up within the system and clearly indicate this in the documentation.

2.12.8 Initiation of Emergency Procedures

2.12.8.1 Disaster Notification List

In the event that a disaster actually occurs there is a need for a list of important stakeholders to be notified immediately. The list shall be compiled and clearly displayed in case of any eventuality.

- i. Computing Services Unit/Department Staff Contacts;
- ii. Deans/Directors of Faculties and Institutes;
- iii. Vice Chancellor;
- iv. University Security Office;
- v. Kenyan Police;
- vi. Fire Brigade; and
- vii. Ambulance/Hospital Services.

2.12.9 ICT Disaster Management Team

The ICT Disaster Management Team shall be tasked with the responsibility of ensuring that all University systems, applications, data and information are restored for user access in the shortest possible time following the occurrence of a disaster.

The team will suitably be headed by the Director ICT and composed of Systems, Web and Network Administrators and IT Officers.

2.12.10 ICT Disaster Management Recovery Plan

The greatest aim of the operation shall be to restore all systems functionality with no data loss.

The following describes a series of actions to be performed after a disaster has occurred;

- i. Recovery Manager shall appoint a Recovery Management Team, in consultation with all University stakeholders;
- ii. Recovery Manager convenes a meeting of the Recovery Management Team;
- iii. Each member's responsibility in the recovery shall be reviewed;
- iv. Recovery manager shall review the recovery plan with the recovery team;
- v. Each member shall perform their respective responsibility until all the data is restored; and
- vi. Next meeting of recovery team shall be scheduled.

2.12.11 Equipment Protection

2.12.11.1 Protection

During the recovery process any equipment, magnetic media and other items damaged at the site shall be protected from any elements to avoid further damage.

2.12.11.2 Inventory

As soon as practicable, a complete inventory of all salvageable equipment shall be taken along with estimates about when the equipment will be ready for use and the list of items to be freshly procured.

2.12.11.3 Damage Assessment

There shall be a preliminary damage assessment intended to establish the extent of damage to critical hardware and the facility that houses it to determine what should be procured immediately.

2.12.12.4 Emergency Procurement

Having fully established the equipment to be replaced, emergency procurement procedures shall be initiated for this equipment to be replaced as soon as practicable.

2.12.13 Initiation of Recovery Procedures

Once the occurrence of a disaster results into the non-functioning of any application system or retrieval/access of information at the main data center, then any one of the replication sites referred to in section 3.1 shall be temporarily lit up to act as the primary site for the entire recovery process.

The choice of which site to use shall depend on an evaluation by the Recovery team on which site is adequately prepared to take up the immediate role of hosting all data processes.

2.12.14 Site Preparation

Having fully re-directed the central data processing activity to one of the replication sites, the recovery team shall embark on recovering the primary computing and network facilities. This process shall highly dependent on how quickly replacement equipment can be procured.

2.12.15 System Platform Recovery Procedures

The Recovery Team shall thereafter recover and restore all University systems and run the restoration of the data backups of these systems

2.12.16 Critical Applications

Throughout the recovery and restoration process, the recovery team shall decide which systems are critical enough to take precedence of others.

2.12.17 Restoration of the Data Center

Once all the restoration procedures have been performed and reviewed, the main Data Center shall undergo rigorous tests before it is re-established as the primary site and the others act as replication sites.

2.12.18 Maintaining the ICT Disaster Recovery Plan

The ICT Disaster Recovery Plan shall be made available to all relevant stakeholders in order to be maintained. This plan shall also be reviewed at least once a year by the University's ICT Committee. It is important to note that since the University's computing infrastructure continues to change, the plan shall therefore have to change accordingly.

APPROVAL

Title: **ICT Policies and Procedures Manual**

Contact: Deputy Vice Chancellor, Administration, Finance & Development

Approval Authority: The University Council

Commencement Date:

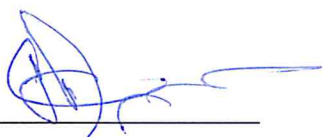
SIGNED



Chairman of Council



Date



Vice Chancellor/Secretary to the Council
Prof. Isaac Ipara Odeo



Date

APPENDIX 1: REFERENCES

- i. National Information and Communication technology ICT Policy;
- ii. Masinde Muliro University of Science and Technology ICT Policy 2012;
- iii. The University of Cape Coast ICT Policy, 2004;
- iv. University of New South Wales (UNSW) Website Policy 2004;
- v. Vision 2030, 2007; and
- vi. Millennium Development Goals (MIDGs).



APPENDIX 2: ICT EQUIPMENT USE AGREEMENT

I have read and understood the ICT Equipment Use Policy. I understand if I violate the rules explained herein, I may face legal or disciplinary action according to applicable laws or company Policy.

Name: _____

Signature: _____

Date: _____



APPENDIX 3: DECLARATION TO ADHERE TO KIBU ANTI-VIRUS POLICY

I have read, understood, and agree to adhere to KIBU Anti-Virus Policy.

Name (Printed): _____

Name (Signed): _____

Date : _____

APPENDIX 4: DECLARATION OF UNDERSTANDING KIBU SERVER BACKUP POLICY

I have read, understood, and agree to adhere to KIBU Server Backup Policy.

Name : _____

Sign : _____

Date : _____

APPENDIX 5: E-MAIL USER AGREEMENT

I have read and understand the E-Mail Acceptable Use Policy. I understand if I violate the rules explained herein, I may face legal or disciplinary action according to applicable laws or University Policy.

Name: _____

Signature: _____

Date: _____

