UNIVERSITY OF NAIROBI

Information and Communication Technology

Policy Guidelines

January 2010

Table of Contents

Abbreviations and Acronyms

(1) ATM Automatic Teller Machine
(2) BOQs Bill of Quantities
(3) BOU Basic Operation Unit
(4) CBPS College of Biological and Physical Sciences
(5) CDs Compact Discs
(6) CD-ROMS Read only memory compact discs
(7) CDRW Read/Write CD
(8) DBA Database administrator
(9) DAS Direct Attached Storage
(10) DVDs Digital Video Discs
(11) Director ICT Unless otherwise stated shall also be referred to as Director and shall also mean his/her nominee
(12) FTP File Tranfer Protocol
(13) GFS Grandfather-Father-Son
(14) ICT Information and communication Technology
(15) ICTC Information and communication Technology Centre
(16) IS Information System
(17) ISO International Organization for Standardization
(18) IP Internet Protocol
(19) IP Intellectual Property
(20) IPSec Internet Protocol Security
(21) LCD Liquid Crystal Display
(22) MIS Management Information System
(23) LAN Local Area Network
(24) NAS Network Attached Storage
(25) NFS Network File System
(26) NUS Network User Support
(27) OIC Officer in Charge of Campus
(28) OS Operating system
(29) PDAs Personal Digital Assistant
(30) PSTN Packet Switched Telephone Network
(31) POC Point of Contact
(32) SSH Secure Shell
(33) SANs Storage Area Networks
(34) SDLC Software Development Life Cycle
(35) SLA Service Level agreement
(36) SQL Structured Query Language
(37) Telnet A terminal emulation program for TCP/IP networks such as the Internet
(38) TCP Transmission Control Protocol
(39) UoN University of Nairobi
(40) UPS Uninterrupted Power Supply
(41) UMB University Management Board
(42) UMIS University Management Information System
(43) WAN Wide Area Network
(44) WWW World wide web
(45) ZIP “Zip" is the generic file format of a compressed archive

Information and Communication Technology Policy, 2008

1. Introduction

1.1 Preamble

Among the nine key strategic objectives identified by the University of Nairobi [1]in its vision towards world-class excellence, is the support and development of the ICT function within the University. In this connection, one of the objectives of the Strategic Plan for 2008-2013 is to: maximize student and staff productivity and service delivery, enhance teaching and learning and improve quality of research through ICT. Clearly, this is a challenge that must be taken on board with vigour and gusto; with a clear vision and plan and with a commitment from all concerned including students, staff and management. Against this background, the ICTC, acting on behalf of the University has taken its mandate of developing a blueprint that will guide in the development, implementation, and effective use of the ICT services at the University.

Where there is no separate ICT standards document for the University, this policy will serve, alongside other related published documents, as the reference document on ICT standards.

1.2 Statement of purpose

This policy seeks to guide developers and users of information and ICT resources on appropriate standards to be adopted at the University. Its objectives include to:

- provide guidance in developing a pervasive, reliable and secure *communications infrastructure* conforming to recognized International standards supporting all services in line with the priorities of the University;

- provide a framework for development and management of ICT *network services* that shall ensure the availability, enhanced performance, security, and reduce the cost of running the ICT infrastructure;

- establish information and implement *security* requirements across the University's ICT infrastructure;

- provide a framework, including guidelines, principles and procedures for the development and implementation of *Software Information System* projects in the University;

- guide the handling of *organizational information* within the ICTC and the University as a whole by ensuring compliance with applicable statutes, regulations, and mandates for the management of information resources; and thereby establish prudent practices on *Internet* and the *University Intranet* use;

- uphold the integrity and image of the University through defined standards and guidelines for ensuring that the content of the University's *websites* is accurate, consistent and up-to-date;

[1] Herein referred to as the University

- serve as the direction pointer for the ICTC's mandate in *supporting users*, empowering them towards making maximum use of ICT services and resources and specifying the necessary approaches;

- to guide the process of enhancing user utilization of ICT resources through *training***;**

- outline the rules and guidelines that ensure users' PCs and other *hardware* are in serviceable order, specifying best practices and approaches for preventing failure;

- to provide a paradigm for establishing the University's *database service* that will support groups working on systems development, production and any other groups; and,

- inform departments carrying out projects financed in whole or in part by the University, of the arrangements to be made in *procuring* the goods and services for the projects.

1.3 Scope of the University ICT Policy

This policy applies to any person accessing/developing/implementing and/or using ICT-based information and ICT resources owned, managed, supported or operated by, or on behalf of, the University. The addresses include all University staff and students; any other organizations accessing services over University ICT resources; persons contracted to develop, repair or maintain University's ICT resources; and suppliers of outsourced ICT services.

Adherence to this policy applies to all these and other relevant parties.

1.4 Approval of Policy Document

This policy document was discussed and approved for productive use by the University Management Board (UMB) and The Senate in April 15 2009 and May 15 2009 respectively. This version, dated 5 January 2010 is a revised edition which has taken into consideration recommendations arising from the two meetings s well as advice from the University Legal Officer.

2. Network Development and Management Policy

2.1 Introduction to network policy

(a) The information and communications infrastructure at the University has evolved into a large, complex network over which the education, research and business of the University is conducted. It is envisaged that the network will integrate voice, data and video, to form a unified information technology resource for the university community. Such a network shall demand adherence to a centralized, coordinated strategy for planning, implementation, operation and support. Decentralization shall be implemented through appropriate University structures.

(b) The University network functions shall be broken down into the following areas:
- University ICT Infrastructure Development
- University backbone
- Campus Local Area Networks (LANs)
- Inter-campus connections
- Dial-up access
- Private networks
- Access to ICT facilities
- Connection to and usage of ICT facilities
- New or changed use of ICT equipment
- Monitoring of network performance.

(c) This therefore shall require a policy that will secure the future reliability, maintainability and viability of this valuable asset.

2.2 Objectives of network policy

(a) The objective of this policy is to establish a comprehensive and uniform Network Development and Management policy for the management of ICT infrastructure for the University.

(b) This policy defines the arrangements and responsibilities for the development, installation, maintenance, and use and monitoring of the University's ICT networks to ensure that, these networks are sufficiently adequate, reliable and resilient to support continuous high levels of activity.

2.3 Scope of network policy

This policy applies to any person accessing or using the ICT infrastructure owned, managed, supported or operated by, or on behalf of the University. These include all University staff and students; any other organization accessing services over University ICT networks; persons contracted to repair or maintain the University's ICT networks; and suppliers of network services.

2.4 General network policy

2.4.1 The Network

The University will develop and support a University-wide ICT network as a basic infrastructure service for the facilitation of sharing electronic information and resources by all members of the University. This includes all staff and students of the University, and other persons engaged in legitimate University functions as may be determined from time to time.

2.4.2 Universal availability

(a) The University network will be designed and implemented in such a way as to serve those located at the University campuses and, to a lesser extent, those located elsewhere.

(b) The ultimate goal is that every room in the University in which research, teaching or support activities take place should be connected. And every member of the University should have capability to access the University ICT infrastructure.

(c) The University network will form part of the general fabric or infrastructure of the University.

(d) There will be one coherent network supporting access to all general information services provided to the University members. There may be separate private networks where they are warranted.

2.4.3 Reliability

(a) High levels of availability, reliability and maintenance will be major objectives in the construction and operation of the University ICT network.
(b) The design and construction of the University network will take into account emerging technologies and standards wherever possible.

2.5 University ICT Infrastructure Development

2.5.1 Development plan

The ICTC will prepare a rolling five (5) year network development plan, advising on appropriate developments aimed at ensuring the adequacy of the University's ICT infrastructure in future. This plan will take account of the University's strategic plan; usage and demand patterns; technological change; security; management and cost implications.

2.5.2 Implementation of new developments

(a) Prior to installation of the "live" situation, major network developments shall be "soak-tested" in off-line simulation.

(b) For up to two months after the live installation of the new development, the network provision that it is to be replaced shall, wherever possible, remain in place as a "fall-back" in the event of any subsequent failure of the new development when it is subject to actual user demand.

2.5.3 ICT network provision in new and refurbished buildings

(a) Network provision for new and refurbished buildings shall be made in accordance with the specification published from time-to-time by the ICTC.

(b) Where the Network requirements are of specialized nature the Officer in Charge of Campus (OIC) concerned shall seek further guidance from the network manager.

(c) All new buildings to be erected in the University shall incorporate an appropriate structured data wiring system to allow connection to the University network.

2.6 University Backbone

2.6.1 Definition

The University network will consist of several parts: "Backbone" systems, a collection of inter-building connections; “Campus LANs,” a collection of “inter-campus” connections; University “Dial-up” service; and a number of “Server Farms.”

The University Network Backbone will comprise an inter-building cabling system, together with one or more "Gateway" interfaces at each building or in the path to each building which will connect the Backbone to the network(s) within each building.

2.6.2 Structure of University backbone

(a) The University Network Backbone shall connect, singly or severally, to buildings, not to individual departments or units.

(b) The planning, installation, maintenance and support of the University Network Backbone shall be under the control of the ICTC.

(c) Connection to the University Network Backbone shall be approved by the Director ICTC.

(d) The ICTC shall adhere to and maintain copies of all relevant networking standards, and keep abreast of national and international developments in these standards.

(e) The University Network Backbone at any particular point of time will be aimed at facilitating the traffic flow between connected buildings or networks.

2.7 Campus LANs

2.7.1 Definition

The respective OICs will take responsibility for the Campus LANs, namely, the necessary wiring and related equipment within existing buildings to allow connection to the LAN gateways.

2.7.2 Structure of Campus LANs

(a) Wherever feasible, the network(s) within each building shall be arranged so that there is a point of connection to the University Network Backbone. In cases where it is not possible to establish a single connection, multiple building gateways may be installed.

(b) Network protocols used on building networks and communicating through the gateway must use approved configuration parameters including approved network identifiers.

(c) Building networks connecting to the University network shall meet overall University network security and management requirements.

(d) In cases where there are constraints to connecting any building to the University Network Backbone, consultations and subsequent approvals by the Director ICT shall be made to allow for alternative configurations.

2.8 Inter-campus connections

2.8.1 Definition

The Inter-campus connections shall consist of the necessary services and related equipment that allow a remote campus or remote university office to access the central University backbone.

2.8.2 Structure of inter-campus connection

(a) Wherever feasible, the network(s) within each remote site will be so arranged so that there will be one point of connection to the University Network Backbone. In cases where it is not possible to establish a single connection, multiple Inter-campus connections may be installed.

(b) Network protocols used on Inter-campus connections must use approved configuration parameters including approved network identifiers.

(c) Inter-campus links connecting to the University network shall meet overall the University network security and management requirements.

2.9 Dial-up Access

2.9.1 Definition

Authenticated access through telephone dial-up access via designated Packet Switched Telephone Network (PSTN) telephone numbers to network services provided for staff and students.

2.9.2 Structure of dial-up access

(a) Network protocols used on the service shall use approved configuration parameters including approved network identifiers.

(b) Dial-up links connecting to the University network shall meet overall the University network security and management requirements.

(c) The dial-up links shall provide authenticated off-campus access to designated information systems and services available on the network using normal individual usernames and passwords.

2.10 Private networks

2.10.1 Definition

Departments or units may install, at their own expense, networks independent of the University Network Backbone. Provided that the installation shall not interfere with the University network. And provided the installation shall adhere to the University policies and standards for installing and implementing such networks.

2.10.2 Structure of private networks

(a) Private departmental networks may extend between buildings.

(b) The ICTC may provide links for these networks but any extra expense incurred above the University Network Backbone requirements shall be charged to the Department.

(c) The ICTC shall provide Campus Gateways for private departmental networks where the private network caters for all the building occupants.

2.11 Access to ICT facilities

2.11.1 Communications rooms, cabinets and ICT network equipment

(a) All communications rooms and cabinets shall be locked at all times.

(b) Entry to communications rooms and cabinets, and interference with ICT network equipment is strictly prohibited.

(c) Other than in an emergency, access to communications rooms, cabinets and ICT network equipment shall be restricted to designated members of staff of the ICTC. Any necessary access must have prior written consent of the Director of ICTC

2.11.2 Access in an emergency

(a) In the event of a fire or other emergency, security staff and/or staff of the Estates Department and/or the emergency services may enter these areas, without permission, to deal with the incident.

(b) Where ICT network equipment is housed in accommodation used for another purpose, the arrangements for access by another user of that accommodation shall require the prior written consent of the Director of ICTC. This consent shall specifically exclude access by the other user to any communications cabinets or ICT network equipment located in the shared accommodation.

2.11.3 Contractors

(a) Contractors providing ICT network services must obtain the prior approval of the Director of ICTC and shall obtain the appropriate authorization and the necessary Contractors' badge in compliance with procedures and regulations of the University Security System.

(b) Contractors shall observe any specific access conditions which apply within the areas in which they will be working. These access conditions include, in all cases, that contractors working in main server rooms shall be accompanied by appropriate University ICT personnel.

2.11.4 Installation of cabling

All installations and changes of electrical power cabling in facilities housing ICT equipment shall be approved and managed by the Estates Department in consultation with the Director ICT in writing.

2.11.5 Installation of equipment

The specification of any equipment to be installed in communications rooms and cabinets and the installation of such equipment, shall require the prior written consent of the Director of ICTC.

2.11.6 Network equipment

(a) Only designated members of the staff of ICTC are authorized to install and maintain active network equipment including hubs, switches and routers connected to the University's ICT networks.

(b) Where the Director of the ICTC agrees that academic staff or the ICTC's technical staff may install and maintain hubs and switches within local staff or student networks, such permission will in every case specifically exclude the point at which these hubs and switches connect to the University's network infrastructure.

2.12 Connection to and Usage of ICT facilities

2.12.1 Connecting to the ICT network

(a) All connections to the University's ICT networks must conform to the protocols defined by the UICTC and with the requirements that apply to Internet Protocol (IP) addresses.

(b) Only designated members of staff of the ICTC, or other staff authorized specifically by the Director of the ICTC, may make initial connections of desktop services equipment to the ICT network.

(c) Computer workstations connected to the ICT network will not be set up to offer services to other users, for example, to act as servers, unless the prior written consent of the Director of the ICTC has been obtained. Such consent will normally exclude all external access (stated under paragraph 2.12.2 below)

2.12.2 External access to servers on the backbone network

(a) External access means access by persons external to the University; access to the backbone network from external locations.

(b) Where specific external access is required to servers on the backbone network, the Director of the-ICTC shall ensure that this access is strictly controlled and limited to specific external locations or persons.

(c) The Director ICTC will monitor compliance with access arrangements as stipulated in this ICT Policy and the relevant ICT Security Policy on Server Security issued by the University from time to time.

(d) Abuses of or failure to comply with these arrangements shall result in immediate restriction to or disconnection from the network.

2.12.3 Domain name services

All Domain Name Services (DNS) activities hosted within the University shall be managed and monitored centrally, for the whole University, by the ICTC.

2.12.4 Electronic mail

Electronic mail or email shall be received and stored on central servers managed by the ICTC from where it can be accessed or downloaded by individual account holders.

2.12.5 Suspension and/or termination of access to ICT networks

- **University Employees**

(a) A staff's access to the University's ICT networks will be revoked automatically:
   i. at the end of his or her employment or research contract;
   ii. at the request of his or her Dean of Faculty/Head of Resource Centre/Head of Department or School or Head of Unit;
   iii. where he or she has breached these regulations.

(b) The University reserves the right to revoke staff's access to the University's ICT networks where the user is suspended pursuant to a disciplinary investigation.

(c) The Administration Registrar will establish mechanisms whereby changes in employment status are communicated immediately to the Director of ICTC so that these employees' computing and e-mail accounts can be suspended or deleted as appropriate.

- **Students leaving the University**

The Academic Registrar will notify the UICTC, by means of the regular student data transfer, of the names of students leaving the University so that such students' computing, e-mail, printing and lending accounts can be deleted.

- **Procedures on Restriction of Use**

(a) Appropriate procedures shall apply in restricting usage after a formal complaint has been lodged or a breach of policy or rule has been reported or detected.

(b) Any breach of ICT policies shall be reported or communicated in writing to the Director, ICT.

(c) Upon receipt of any such complaint, the Director, ICT shall classify the complaint as “serious” or “non-serious.” A “non-serious” complaint shall be defined as a breach of policy which does not subject the University to a cost nor any risk.

(d) When a complaint is classified as “non-serious,” the Director, ICT is authorized to impose any one of the following penalties:

   i. Suspension of the account for a minimum period of four weeks
   ii. Permanent disabling of the account

(e) When a complaint is classified as “serious,” the Director, ICT shall refer the complaint to the ICT Committee for appropriate action. The possible penalties may be any one or a combination of the following:

i. Notification of the suspension will be communicated to the relevant Dean and/or Head of Department or Section;
ii. Suspension of the account shall be for a minimum period of four weeks. Formal approval of the relevant Dean and/or Head of Department or Head of Section and a signed undertaking to abide by the Rules of Use shall be required before reinstatement of the account.
iii. Permanent disabling of the account shall be taken, where the severity of the offence warrants such action.
iv. Accounts may be reinstated before the end of the suspension period where either the student or staff presents information to the Director, ICT, which indicates that he or she was not involved in the transgression of the Rules of Use, or the Dean and/or the Head of Department or Head of Section requests the account be reinstated for course related work only (e.g. completion of an assignment). In this case the student or staff is required to sign an undertaking to abide by the Rules of use.
v. A system administrator within NUS can make a recommendation to disable an account to the Director, ICT. The director, ICT shall review the request and if there is considered to be, on the balance of probability, a transgression of the NUS ICT Rules of Use, the account shall be suspended.
vi. An account may also be suspended, if a request has been made to the Director, ICT from a systems administrator of another system, with a reasonable and accepted case for suspension.
vii. Users should note that suspension of access to ICT facilities also includes access to the terminal server password access, and as such dial-up modem access will be disabled where a user account is suspended.

Appeals

Students or staffs whose access has been suspended shall have the right to appeal in writing to the ICT Committee.

2.12.6 Internet Protocol (IP) addresses

(a) All equipment connected to the ICTC networks shall be assigned unique IP addresses.

(b) The IP addresses assigned to equipment shall be recorded visibly on the casing of the equipment.

(c) The Communications and Networks Manager, ICTC shall plan and allocate Blocks of IP addresses to different network segments and notify the relevant OIC.

(d) The OIC, after distribution of the allocated IP Block shall notify the Communications and Networks Manager who shall in turn update the IP address master record.

(e) The Communications and Networks Manager shall maintain a central record of IP addresses and may remove inactive IP addresses after six months.

2.12.7 Inventory control

As part of their audit responsibilities, OICs shall be required to record in their local equipment inventory records the IP address assigned to each item of equipment for which they are responsible, together with the location of such equipment.

2.12.8 Connection of privately owned computers to the University Network

Although members of staff and students may apply for an IP address, using the procedures in this Policy, to enable them to connect such computers or workstations to the University network, permission shall be given only where the Communications and Networks Manager, ICTC, is satisfied that the computer workstation meets the specification determined by the Director of ICTC and that it poses no risk to the University network.

2.12.9 Additional or changed equipment

(a) The Director ICTC shall be advised in advance and at the earliest opportunity, of any plan to add items of desktop services equipment to or to replace or to relocate desktop equipment that are connected or that may require connection to the University's ICT network.

(b) The Director ICTC shall assess the likely impact on the University's ICT networks of the proposed change. The Director ICTC shall give approval for the proposed change only where appropriate adjustments can be made to accommodate any effects on network traffic that this change may cause.

2.12.10 External data communications

(a) All external data communications shall be channeled through the University's approved links.

(b) No external network connections shall be made without the prior written consent of the Director ICTC.

(c) The installation and use of leased or private links on premises owned, managed or occupied by the University shall require the prior written consent of the Estates Manager.

(d) The use of modems, leased or other means of access to other networks on equipment located on premises owned, managed or occupied by the University that are linked to the ICT network infrastructure, is prohibited, unless a proposal and justification for such connection has been authorized in writing by the Director, ICT.

2.12.11 Web cache provision

(a) The ICTC shall be responsible for provision and management of University web cache facilities for incoming web traffic.

(b) All web access shall be set up to ensure use of the University's web cache facility for incoming web traffic under the ICT Internet Usage Policy.

2.12.12 Web filtering

The Director ICTC shall be responsible for the implementation of appropriate filtering facilities for web-based and non-web Internet traffic, including MP3 traffic and other high bandwidth intensive services that may not have direct educational or research value, where and when necessary in conformity with the ICT

Policy and relevant ICT Guidelines that promise efficient and high availability of Internet services to the majority of users.

2.13 New or changed use of ICT equipment

(a) The Director ICTC shall be advised in advance of any plan that involves a new use, a change of use or addition to the University's ICT networks that might impact on the performance or security of the network.

(b) The Director ICTC shall assess the likely impact of the proposed use and will advise on the consequential impact upon the performance of the University's ICT network. Such changes shall be effected after approval by the Director ICTC.

2.14 Monitoring of network performance

The Network Manager, ICTC, shall monitor and document ICT network performance and usage and shall maintain regular monthly reports.

3 ICT Security and Internet Policy

3.1 Definitions of terms

(a) *Spam* - Unauthorized and/or unsolicited electronic mass mailings

(b) *"Chain letters," "Ponzi," "pyramid" schemes*- Messages that purport to tell the addressee how, for a relatively small investment, the addressee can make huge amounts of money. There are several variations, but they are all based on a common fraudulent concept — that the addressee pays a relatively small amount of money to a few people above the addressee in a chain, with the expectation that later a very large numbers of people will be making similar payments to the addressee.

(c) *Port scanning*- Attempting to learn about the weaknesses of a computer or a network device by repeatedly probing it with a series of requests for information.

(d) *Network sniffing* -Attaching a device or a program to a network to monitor and record data traveling between computers on the network.

(e) *Spoofing* -The deliberate inducement of a user or a computer device to take an incorrect action by Impersonating, mimicking, or masquerading as a legitimate source.

(f) *Denial of service* -Procedures or actions that can prevent a system from servicing normal and legitimate requests as expected.

(g) *Ping attack* - A form of a denial of service attack, where a system on a network gets "pinged," that is, receives a echo-request, by another system at a fast repeating rate thus tying up the computer so no one else can contact it.

3.2 Purpose

The purpose of this ICT Policy is to outline the acceptable use guidelines for ICT equipment and services at the University. The intention of this policy to promote the University's established culture of openness, trust and integrity. These are general guidelines on what can be done, and what should not be done, on the University ICT Infrastructure in order to protect ICT resources from injurious actions, including virus attacks, data loss, unauthorized access, network and system failures, and legal problems.

3.3 Scope

This policy applies to permanent, temporary and casual staff, students, contractors, consultants, and other users of the University ICT services, including all personnel affiliated with third parties. This Policy applies to all ICT equipment, software or other facilities that is owned or leased by the University.

3.4 General use and ownership policy

3.4.1 Roles

(a) While the ICTC is committed to the provision of a reasonable level of privacy, the ICTC shall not guarantee confidentiality of personal information stored or transmitted on any network or device belonging to the University. The data created and transmitted by users on the ICT systems shall always be treated as the property of the University.

(b) The ICTC shall protect the University's network and the mission-critical University data and systems. The ICTC shall not guarantee protection of personal data residing on University ICT infrastructure.

(c) Users shall exercise good judgment regarding the reasonableness of personal use of ICT services. They shall be guided by ICT policies concerning personal use of ICT Internet, Intranet or Extranet systems. In the absence of or uncertainty in such policies or uncertainty, they shall consult the relevant ICT staff.

(d) For security and network maintenance purposes, authorized staff within the ICTC shall monitor equipment, systems and network traffic at any time as provided for in the network and development policy.

(e) The ICTC shall reserve the right to audit networks and systems on a periodic basis to ensure compliance with this ICT Policy.

3.4.2 Securing confidential and proprietary information

(a) University data contained in ICT systems shall be classified as either confidential or non-confidential. Examples of confidential information include but are not limited to: payroll data, human resource data, and research data. Employees shall take all necessary steps to prevent unauthorized access to confidential information

(b) Users shall keep passwords secure and shall not share accounts. *Harambee* or shared accounts are strongly discouraged. Authorized users are responsible for the security of their passwords and accounts. System level passwords shall be changed on a monthly basis; user level passwords shall be changed at least once every 3 months.

(c) All PCs, laptops and workstations shall be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host is unattended.

(d) Postings by users from the University email address to newsgroups shall contain a disclaimer stating that the opinions expressed are strictly the user’s and not necessarily those of the University, unless posting is in the course and within the scope of official duties.

(e) All hosts connected to the University Internet, intranet or extranet, whether owned by the user or the University shall at all times be required to execute approved virus-scanning software with a current virus database.

(f) The user shall exercise caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

3.4.3 Unacceptable use

(a) Under no circumstances shall an employee, student, contractor or any staff be authorized to engage in any activity that is illegal under Kenyan or international law while utilizing the University ICT resources.

(b) The following activities shall be prohibited. The list is by no means exhaustive, but is an attempt to provide a framework of activities that fall in the category of unacceptable use.

3.4.3.1 Unacceptable System and Network Activities

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

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

(b) Introduction of malicious programs into the network or server, for instance viruses, worms, Trojan horses or e-mail bombs.

(c) Sharing of the University user accounts and passwords– users shall take full responsibility for any abuse of shared accounts

(d) Using the University computing resources to actively engage in procuring or transmitting material that could amount to sexual harassment or constitute creation of a hostile work environment.

(e) Making fraudulent offers of products, items, or services originating from any the University account.

(f) Causing a security breach or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which one is not an intended recipient or logging onto a server that one is not expressly authorized to access, unless this is within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged attacks, packet spoofing, denial of service, and forged routing information for malicious purposes.

(g) Port scanning or security scanning unless prior notification to ICT management is made.

(h) Executing any form of network monitoring which will intercept data not intended for the originator's host computer, unless this activity is a part of an employee's normal job or duty.

(i) Circumventing user authentication or security of any host, network or account.

(j) Interfering with or denying service to other network users, also known as denial of service attack.

(k) Using any program, script or command, or sending messages of any kind, with the intent to interfere with, or disable, another user's terminal session, via any means, locally or via the Internet, intranet or extranet.

(l) Using the University network or infrastructure services, including dial-up Internet connection, to offer services to others within or outside the University premises on free or commercial terms.

Unacceptable email and communications activities

(a) Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material, also known as email Spam.

(b) Any form of harassment via email, telephone, or chat sessions, whether through language, frequency, or size of messages.

(c) Unauthorized use, or forging, of email header information.

(d) Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

(e) Creating or forwarding "chain letters," "Ponzi" or other "pyramid" schemes of any type.

(f) Use of unsolicited email originating from within the University networks of other Internet, intranet and extranet service providers on behalf of, or to advertise, any service hosted by the University or connected via the University network.

3.5 Password Policy

3.5.1 Rules

(a) All system-level passwords such as root, enable, Windows server administration, application administration accounts, shall be changed at least once every month.
(b) All user-level passwords such as email, web, and desktop computer shall be changed at least once every three months.
(c) User accounts that have system-level privileges granted through group memberships or programs such as "sudo" shall have passwords distinct from all other accounts held by such users.
(d) Passwords shall not be inserted into email messages or other forms of electronic communication.
(e) Passwords for the University accounts shall not be used for other non University access such as personal ISP account, Yahoo Mail, and Bank ATM.
(f) All passwords shall be treated as sensitive, confidential University information. Users shall not share the University passwords with anyone, including administrative assistants or secretaries.
(g) Users shall not use the "Remember Password" feature of applications like Eudora, Outlook, and Netscape Messenger.
(h) Users shall not write passwords down and store them anywhere in their offices.
(i) Where an account or password is suspected to be compromised the affected passwords shall be changed immediately. The ICTC shall be alerted immediately to investigate the incident, if it affects critical University information systems or processes.
(j) As a proactive defense procedure, password cracking or guessing tools may be performed on a periodic or random basis by the relevant staff of the ICTC or its delegates. If a password is guessed or cracked during one of these scans, the affected user shall be required to change the password immediately.

(k) All user-level and system-level passwords shall conform to the guidelines described below.

3.5.2 General password construction guidelines

Computer passwords are used for various purposes at the University. Since very few systems have support for one-time tokens, that is, dynamic passwords that are only used once, all users shall familiarize themselves with the following information on how to select strong passwords.

Poor, weak passwords have the following characteristics:

(a) The password contains less than eight characters
(b) The password is a word found in an English, Swahili or other dictionary
(c) The password is a common usage word such as:
    i. Names of family, pets, friends, co-workers, or fantasy characters.
    ii. Computer terms and names, commands, site, company, hardware, software.
    iii. The words "university", "nairobi", " kenya" or any such derivation.
    iv. Birthdays and other personal information such as addresses and phone numbers.
    v. Word or number patterns like aaabbb, qwerty, zyxwvuts, or 123321.
    vi. Any of the above spelled backwards.
    vii. Any of the above preceded or followed by a digit such as ecret1, 1secret.

Strong passwords have the following characteristics:

(a) Contain both upper and lower case characters like a-z, A-Z.
(b) Have digits and punctuation characters as well as letters such as 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?, or /.
(c) Are at least eight alphanumeric characters long.
(d) Are not words in any language, slang, dialect, or jargon, among others.
(e) Are not based on personal information, or names of family, among others.

3.5.3 Application development standards

Application developers shall ensure that their programs contain the following security precautions.
(a) Shall support authentication of individual users, not groups.
(b) Shall not store passwords in clear text or in any easily reversible form.
(c) Shall provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
(d) Shall support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

3.6 Server Security Policy

3.6.1 Ownership and Responsibilities

Any server deployed on the University ICT network shall have an operational group that shall be responsible for its system administration. Operational groups shall monitor configuration compliance and shall implement an exception policy tailored to their environment. Each operational group shall establish a process for changing the configuration guides; if the server is executing critical University systems this shall involve a final review and approval by the ICTC's management.

(a) All servers shall be registered with the ICTC. At a minimum, the following information shall be forwarded:
   i. Contacts of the System administrator
   ii. Physical location of the server
   iii. Hardware and Operating System version in use
   iv. Description of functions and applications of the server

(b) Configuration changes for servers shall follow the appropriate change management procedures.

3.6.2 General configuration guidelines

(a) Server Operating Systems shall be configured in line with approved ICT guidelines.
(b) Services and applications that are not used shall be disabled at all times, for instance NFS, Telnet, and FTP.
(c) Access to services shall be logged and protected through access-control methods such as TCP Wrappers where possible.
(d) The most recent security patches shall be installed on the systems as soon as practical, the only exception being when immediate application would interfere with business requirements.
(e) Antivirus software shall be installed and configured to update regularly.
(f) Trust relationships, such as through NFS, between systems are a security risk, and these use shall be avoided. No trust relationship shall be used where alternative secure methods of communication are available.
(g) User access privileges on a server shall be allocated on "least possible required privilege" terms, just sufficient privilege for one to access or perform the desired function.
(h) Super-user accounts such as "root" shall not be used when a non-privileged account can do.
(i) If a methodology for *secure channel connection* is available, that is technically feasible, privileged access shall be performed over secure channels, for instance, encrypted network connections using SSH or IPSec.
(j) Servers shall be physically located in an access-controlled environment.
(k) It shall be prohibited to operate servers from uncontrolled or easily accessible areas.

3.6.3 Monitoring

(a) All security-related events on critical or sensitive systems shall be logged and audit trails backed-up in all scheduled system backups.

(b) Security-related events shall be reported to the ICT information security officer, who shall review logs and report incidents to ICT management. Corrective measures shall be prescribed as needed. Security-related events include, but are not limited to:
   i. port-scan attacks
   ii. evidence of unauthorized access to privileged accounts
   iii. anomalous occurrences that are not related to specific applications on the host.

3.7 Audit policy

For the purpose of performing an audit, any access needed shall be provided to members of the University ICT audit team when requested. This access shall include:

(a) user level and/or system level access to any computing or communications device.
(b) access to information (such as electronic or hardcopy) that may be produced, transmitted or stored on the University ICT infrastructure.
(c) access to work areas such as computer laboratories, offices, cubicles, or storage areas.
(d) admission to interactively monitor and log traffic on the University ICT networks.

3.8 Internal Computer Laboratory security policy

3.8.1 Ownership responsibilities

(a) All the University units that own or operate computer laboratories shall appoint officers, designated as Computer Laboratory administrators, who shall take charge of their computer laboratories. A Computer Laboratory administrator shall be responsible for the day to day running of a Computer Laboratory, and shall be the point of contact (POC) for the ICTC on all operational issues regarding the Laboratory. Heads of units shall formally inform the ICTC of the names and contacts of their computer Laboratory administrators.

(b) Computer Laboratory administrators shall be responsible for the security of their laboratories and their impact on the University network, or any other network. They shall be responsible for overseeing adherence to this policy and associated processes.

(c) Computer Laboratory administrators shall be responsible for the Laboratory's compliance with all the University ICT policies.

(d) Computer Laboratory administrators shall be responsible for controlling access to their computer laboratories; they shall ensure that only legitimate users can gain access to laboratory resources.

(e) The ICTC reserves the right to interrupt laboratory connections if such connections are viewed to impact negatively on the ICT infrastructure, or pose a security risk. For this purpose, Computer

Laboratory administrators shall be available round-the-clock for emergencies, otherwise actions shall be taken without their involvement.

(f) The ICTC shall be furnished with records of all IP addresses and related configurations assigned to hosts in any computer laboratory. The Computer laboratory administrator or any other person shall, at no time, change these configurations without first notifying the ICTC network management.

(g) Any University unit that wishes to add an external connection to their Computer Laboratory whilst the laboratory is connected to the University network shall provide a diagram and documentation of the proposed connection to the ICTC with adequate justification. The ICTC shall study such proposals for relevance, review it for any security concerns, and must approve before implementation is allowed to proceed.

(h) No computer laboratory shall replicate the core production services offered by the ICTC. Production services shall be defined as all shared critical services running over the University ICT infrastructure that generate revenue streams or provide customer capabilities. These services shall include, but shall not be limited to, World wide web (WWW) proxy services, E-mail services, Web hosting and FTP services. The ICTC shall, alone, manage these services.

(i) The ICTC shall address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

3.8.2 General configuration requirements

(a) All traffic between the production networks (networks connecting servers that run critical University systems) and computer laboratories shall go through screening firewalls. Computer laboratory network devices (including wireless) shall not cross-connect a laboratory to a production network, circumventing screening firewalls.

(b) Computer laboratories shall be prohibited from engaging in port scanning, network auto-discovery, traffic spamming or flooding, and similar activities that may negatively impact on the overall health of the University network and/or any other network. The general use and ownership policy shall apply.

(c) In computer laboratories where non-University users are allowed access (such as computer training laboratories), direct connectivity to the University production network from such laboratories shall be prohibited. In addition, no University confidential information shall reside on any computing equipment located in such laboratories.

3.9 Anti-virus policy

(a) All Computers connected to the University ICT network shall run the University standard supported anti-virus software, and shall be configured to perform daily full-system and on-access scans.

(b) Anti-virus software and the virus pattern files shall be kept up-to-date always through scheduled daily automatic updates.

(c) Computer laboratory administrators and owners of computers, in consultation with the relevant ICTC personnel, shall be responsible for executing required procedures that ensure virus protection on their computers. Computers shall first be verified as virus-free before being allowed to connect to the University network.

(d) Once discovered, any virus-infected computer shall be removed from the University network until it is verified as virus-free.

(e) The following precautions shall be observed by all users to reduce virus problems. Users shall:

i. never open any files or macros attached to emails from an unknown, suspicious or untrustworthy source. All such emails shall be deleted immediately and emptied from trash folders
ii. delete spam, chain, and other junk email without forwarding, in compliance with the General Use and ownership Policy.
iii. never download files from unknown or suspicious sources.
iv. avoid direct disk sharing with read/write access unless this is absolutely necessary.
v. always scan removable media, including diskettes and memory sticks, from unknown sources for viruses before using.
vi. back-up critical data and system configurations on a regular basis and store the data in a safe place.
vii. in a computer where the anti-virus software is disabled, not run any applications that could transfer a virus such as email or file sharing. Such a computer shall be disconnected from the network.
viii. periodically check for anti-virus updates and virus alerts because new viruses are discovered almost every day.

3.10 Dial-in access policy

(a) Authorized users of University ICT services shall be granted rights to use dial-in connections if they intend to gain access to the University ICT network services while outside the University premises.

(b) All dial-in access shall be strictly controlled, and all account activity shall be continuously monitored to prevent abuse or breach of security.

(c) Users who are granted dial-in access privileges shall remain constantly aware that dial-in connections between their location and the University are literal extensions of the University network, which can provide a potential path to the University's most sensitive information.

(d) Dial-in access users shall observe all other ICT security policies; in particular, they shall adhere to the General Use and Ownership policy, Password policy, and Anti-Virus policy.

(e) Dial-in users shall take every reasonable measure to protect University assets or information that they are allowed to access by this facility.

(f) The ICTC shall reserve the right to disable any dial-in account, with or without prior notice to affected user, if abuse is suspected.

3.11 Physical Security policy

3.11.1 Required physical security

(a) *Security marking:* All University computer hardware shall be prominently marked, either by branding or etching, with the name of the University unit and name of office or computer laboratory where the equipment is normally located.

(b) *Locking of personal computer (PC) cases:* PCs fitted with locking cases shall be kept locked at all times.

(c) *Sitting of computers:* Wherever possible, computer equipment shall be kept at least 1.5 metres away from external windows in high-risk situations.

(d) *Opening windows:* All opening windows on external elevations in high-risk situations shall be fitted with permanent grills.

(e) *Blinds:* All external windows to rooms containing computer equipment at ground floor level or otherwise visible to the public shall be fitted with window blinds or obscure filming.

(f) *Door specification:* All doors giving access to the room or area with computer equipment both from within and outside the building, shall be, as a minimum, be fitted with supplementary metal grills.

(g) *Intruder alarm:* Rooms and buildings incorporating high-density computer equipment shall have intruder alarm detection equipment installed.

(h) *Location of intruder alarms:* Detection devices shall be located within the room or area and elsewhere in the premises to ensure that unauthorized access to the room or area is not possible without detection. This shall include an assessment as to whether access is possible via external elevations, doors, windows and roof.

(i) *Detection device test:* A walk test of movement detectors shall be undertaken on a regular basis in order to ensure that all PCs are located within the alarm-protected area. This is necessary due to the possible ongoing changes in the position of furniture, screens and partitions, which may seriously impede the field of cover provided by existing detection devices.

(j) *Alarm confirmation:* Visual or audio alarm confirmation shall be provided for all conventional detection within the premise.

3.11.2 Computer server rooms

(a) Computer servers shall be housed in a room built and secured for the purpose.

(b) The computer server rooms shall contain an adequate air conditioning system in order to provide a stable operating environment and to reduce the risk of system crashes due to component failure.

(c) No water, rainwater or drainage pipes shall run within or above computer server rooms to reduce the risk of flooding.

(d) Where possible the floor within the computer suite shall be a raised false floor to allow computer cables to run beneath the floor and reduce the risk of damage to computer equipment in the case of flooding.

(e) Power feeds to the servers shall be connected through uninterrupted power supply (UPS) and surge protector equipment to allow the smooth shutdown and protection of computer systems in case of power failure.

(f) Where possible generator power shall be provided to the computer suite to help protect the computer systems in the case of a mains power failure.

(g) Access to the computer server rooms shall be restricted the authorized University staff only.

(h) All non-ICTC staff working within the computer server room shall be supervised at all times and the ICT management shall be notified of their presence and provided with details of all work to be carried out, at least 24 hours in advance of its commencement.

3.11.3 Access control

(a) The system Administrator in charge of a particular system shall be the only authorized person to assign system, network or server passwords for relevant access to the system.

(b) The system administrator shall be responsible for maintaining the integrity of the system and data, and for determining end-user access rights.

(c) All supervisor passwords of vital network equipment and of those critical ICTC servers shall be recorded in confidence with the Director of ICTC, and the record safely stored under lock and key for emergencies.

(d) System audit facilities shall be enabled on all systems to record all log-in attempts and failures, and to track changes made to systems.

3.11.4 Physical LAN/WAN security

(a) Switches

i. LAN and WAN equipment such as switches, hubs, routers, and firewall shall be kept in secured rooms. In addition, the equipment shall be stored in lockable air-conditioned communication cabinets.

ii. All communication cabinets shall be kept locked at all times and access restricted to relevant ICT staff only.

iii. Whenever legitimate access to communication cabinets is necessary, it shall be done with physical supervision of the responsible ICT personnel.

(b) Workstations

i. Users shall log out of their workstations when they leave their workstation for any length of time.
ii. All unused workstations shall be switched off outside working hours.

(c) Wiring

i. All internal or external network wiring shall be fully documented.
ii. All unused network points shall be de-activated when not in use.
iii. All network cables shall be periodically scanned and readings recorded for future reference.
iv. Users shall not place or store any item on top of network cabling.
v. Where ducting is involved, fumigation and inspection shall be carried out regularly to curb damage to the cables by rodents.
vi. Redundant cabling schemes shall be used where possible.

(d) Monitoring Software

i. The use of monitoring tools, such as network analyzers or similar software shall be restricted to ICTC staff who are responsible for network management and security only. Network monitoring tools shall be securely locked up when not in use.

(e) Servers

i. All servers shall be kept securely under lock and key.
ii. Access to the system console and server disk or tape drives of the production servers shall be restricted to authorized ICTC staff only.

(f) Electrical security

i. All servers and workstations shall be fitted with UPS to condition power supply.
ii. All switches, routers, firewalls and critical network equipment shall be fitted with UPS.
iii. Critical servers shall be configured to implement orderly shutdown in the event of a total power failure.
iv. All UPS equipment shall be tested periodically.

(g) Inventory management

i. ICTC shall keep a full inventory of all computer equipment and software in use throughout the University.
ii. Computer hardware and software audits shall be carried out periodically to track unauthorized copies of software and changes to hardware and software configurations.

3.12 Systems Backup Policy

3.12.1 Responsibility

All ICTC sections that operate key University systems shall formulate and implement systematic schedules for performing regular backups on the systems in their custody.

The following cadre of staff shall carry full responsibility with regard to data backup implementation: The system administrators, application managers, MIS project leaders and database administrators. The responsible staff shall arrange to perform backups as scheduled at all times.

The ICT Security Officer shall be the principal back-up custodian. Back-ups of critical systems shall be documented with the ICT security office and handed over for safekeeping.

All responsible shall take necessary measures to ensure integrity, confidentiality and reliability of the back-ups.

3.12.2 Backup window

Backups for online systems shall be carefully scheduled so as to diminish any perceived degradation on system performance. Hence, back-up windows shall be scheduled at specific times of the day where the most minimal interruption on system services is likely. As a rule of thumb, all major backups shall be scheduled to run at night or during weekends, times when demand for system services is expected to be generally low.

3.12.3 Back-up inventory file

The ICTC shall maintain *a back-up inventory file*, which shall document all backups carried out on critical University systems. This shall provide mechanisms for quick monitoring and tracking of implementation of scheduled back-ups.

All relevant backups, whether stored in removable back-up media and/or on fixed media (hard-disks), shall be recorded in a *back-up inventory file*. See *documenting data back-ups* below for details.

The *back-up inventory file* shall be kept in a safe storage area, under custody of the ICT Security Officer.

3.12.4 Documenting data back-ups

The following information shall to be documented for all generated data backups:

(a) Date and time the data backup was carried out (dd/mm/yyyy: hh:mm).
(b) The name of the system or short description of the nature of the data
(c) Extent and type of data backup (files/directories, incremental/full).
(d) Backup hardware and software used (computer name, operating system (OS), version number).
(e) Sequence number if any (where multiple removable backup media are used).
(f) Physical location of the server and the logical path on file-system to the back-up area, when fixed media (hard-disks) are used.
(g) Data restoration procedures. This may be a separate booklet or set of guidelines

The above information shall be filed in the back-up inventory file. Removable media, in addition, must carry proper labels documenting items (a) to (e).

3.12.5 Verification

There shall be a regular audit of all backup media. It is recommended that this exercise be carried out at least once every three months. A complete set of back-up media shall be restored, on a temporary location, and then inspected for accurate data reconstruction.

A report on the outcome of the audit shall be generated and recorded in the back-up inventory file.

3.12.6 Storage

(a) Removable backup media shall be stored in a locked fireproof safe within an access-controlled room.

(b) A complete copy of the current removable backup set shall be moved to secure offsite storage once every month.

3.12.7 Data restoration procedures

All step-by-step procedures needed in order to achieve complete data reconstruction and resumption of system operations from backups shall be documented. A hard copy of this document shall be filed in the back-up inventory file.

3.12.8 Back-up retention period and media rotation schedule

The retention period for back-up media shall be set in such a manner as to minimize the risk of catastrophic loss of data at reasonable media cost.

The following guide, commonly known as the Grandfather-Father-Son (GFS) method, shall be adopted:

(a) Daily backups, known as the Son, shall be carried out on all, or selected days of the week;
(b) The last full daily backup in a week, known as the Father, shall be the weekly backup;
(c) Daily backups age only for the length of the week, hence the media shall be reused in the coming week;
(d) The weekly backups shall be retained for a month and shall be reused during the next month;
(e) The last full backup of the month is known as the monthly backup, or the Grandfather;
(f) The Grandfather backups become the oldest, and shall be retained for a year before the media can be reused.

Back-up media must first be tested to guarantee their integrity before re-use. Media re-use must always begin with the oldest set.

3.12.9 Data Archiving

(a) ICTC is obliged to maintain archives of data of critical University systems for a time frame that is beyond the normal backup retention period, in case of future need to refer to the data by the University or authorized Government agencies.

(b) For this purpose, in addition to normal backups, responsible staff shall arrange for a special backup scheduled at close of each financial year for all sensitive data on respective systems. Tapes used for this purpose shall be clearly documented and safely retained, with no intention of re-use, in a long-term storage facility.

3.12.10 Back-up media

(a) The following back-up media are recommended.
   i. *Fixed computer hard drives*. These can be located over the network on a separate computer or, most preferably, on equipment using specialized storage technology such as Direct Attached Storage (DAS), Network Attached Storage (NAS) and Storage Area Networks (SANs). Use of these media is recommended where fast, very frequent and high capacity backups are required.
   ii. *Compact Disc s(CDs), CDRW (Read/Write CD), Digital Video Discs (DVDs)* or a *ZIP drives*. Are recommended removable media for medium capacity backups or archives.
   iii. *Tape cartridges (4mm tape, 8mm tape*). Recommended removable media for use where high capacity backups and archives are required.

(b) For storage or transfer of small backups, *flash memory sticks* are recommended. *Floppy disks* are discouraged. Floppies have too low capacity and often develop errors over time, sometimes rendering backup data unrecoverable.

(c) Where backups are made on fixed media, redundant copies of the backup file shall be periodically made on removable media such as 4mm tapes, DVDs, or Read/Write CDs and stored at off-site storage area.

3.12.11 Back-up plans

Back-up plans, with the schedule of the general regular backup pattern for the key University systems, shall be documented. The ICT security officer shall prepare this plan in conjunction with the persons responsible for back-ups. The ratified plan shall be authorized by the Director ICT and filed in the *back-up inventory file*. Persons responsible for back-ups shall carryout all back-ups as scheduled on the back-up plan, but may also stipulate additional event-dependent intervals where necessary.

3.13 Internet Usage Policy

(a) All software used to access the Internet shall be part of the University standard software suite or approved under the ISO standard.
(b) All users shall ensure that Internet access software shall incorporate the latest security updates provided by the vendors.
(c) All files downloaded from the Internet shall be scanned for viruses using the University's corporate anti-virus software suite with the latest virus detection updates.
(d) All Internet access software shall be configured to use stipulated gateways, firewalls, or proxy servers. Bypassing any of these servers shall be strictly prohibited.
(e) Accessed Internet sites shall comply with the University General Use and Ownership Policy.
(f) Internet access traffic through the University ICT infrastructure shall be subject to logging and review.

(g) The University Internet access infrastructure shall not be used for personal solicitations, or personal commercial ventures.
(h) All sensitive University materials transmitted over the Internet shall be encrypted.
(i) Official electronic files shall be subject to the same rules regarding the retention of records that apply to other documents and information or records shall be retained in accordance with University records retention schedules.

4 Software Development, Support and Use Policy

4.1 Definition of terms

(h) *Documentalist* – This is the person who prepares and edits all the documents needed during the Information System development process**.**

(i) *Feasibility study* - The purpose of a feasibility study shall be to define a business problem and to decide whether or not a new system is feasible or viable and can be secured by spending minimum amount of time and money in the effort.

(j) *Information System* (IS) - A system can be defined as a set or arrangement of things or components so related or connected as to form a whole. An Information System is a system that manages data needed by a business. It keeps records and maintains the various facts and figures needed to run the business. More specifically, an information system should support the day-to-day operations, management and decision-making information needs of business workers.

(k) *Programmer* – This is the person who writes computer programs or applications aimed at solving a business problem as specified by the Systems Analyst. Programmers convert the systems specifications given to them by the analyst into instructions the computer can understand. This is sometimes called *coding.*

(l) *Requirement specification document* – This is a document prepared during the Analysis phase of IS development. It outlines the problems identified with the old system and states precisely what is expected of the new or envisaged system.

(m) *Systems analyst* - A systems analyst is a system-oriented problem solver. *System problem solving* is the act of studying a problem environment in order to implement corrective solutions that take the form of new or improved systems.

(n) *System changeover* – This is the process of converting from an existing system to a new Information System, including the migration of data and putting in place all necessary resources to manage the migration

(o) *User Interface* – The method by which an operator or user interacts with a software program.

(p) *Organization chart* – This is hierarchy showing all the establishment of a University department and personnel reporting structures within the same department.

(q) *Stakeholder* – Any person, department or organization that has an interest in an Information System.

4.2 Introduction

(a) Information Systems are becoming a vital part in many organizations as they are used to support core functions within organizations. This means that reliability shall be a key component of these

Information Systems. Reliability does not come by coincidence; it shall be planned for and incorporated in the entire development process. This means that the entire software development process shall be planned for and executed in the best way possible using techniques that can be repeated in future projects.

(b) A good software product should meet the functional, quality and resource requirements of the user to acceptable levels without compromise. In order to achieve this, the University and the users shall employ sound software development techniques, policies and standards that will ensure that the end product can stand the test of time.

(c) Once software has been developed and is operational, there is need to ensure that all necessary support and use procedures are adhered to. This will ensure that the information from the system remains relevant, is accurate and will only be available to authorized persons. This will also ensure that the integrity of the system is not compromised at all times. Users shall be supported at all times as stipulated in this ICT policy.

4.3 Objectives

(a) The purpose of this policy is to ensure that the process of software development at the ICTC follows the due process right from the planning phase through to the implementation stage and that all deliverables at every milestone meet the required standards.

(b) This policy also seeks to continually improve on the process of software development at the ICTC and ensure that the software products produced meet the requirements of the user and are of good quality.

(c) This policy also addresses the need for software support and use of the available information to ensure that the integrity of the system is not compromised at any time. The need for ownership of software by users is also addressed to apportion responsibility and improve access to this information.

4.4 Scope

The policy covers the Software Development Lifecycle (SDL). Moreover, the policy also covers the support required for any operational Information Systems, integrity of data, request for service, and accessibility of Information.

4.5 Software Development Policy Statements

4.5.1 Project Planning & Organization

(a) Prior to the computerization or acquisition of any University information system, the Director of ICTC in consultation with the relevant authority shall constitute an *IS* project team comprising all the relevant stakeholders.
(b) The Director ICT shall appoint a Project Leader for every project.
(c) In case the project leader finds that there are some stakeholders that have been excluded from the project team then he or she shall make a request to the Director for them to be included.

(d) The DBA shall be part of the project team and shall be responsible for advising the team and implementing issues relating to the database management and administration.
(e) The Director ICT shall ensure that each IS Project has an organization chart.
(f) The roles and responsibilities of the different persons involved in the project development and implementation shall be clearly defined in the project job description document and everyone in the project trained on them. The Director of ICT shall facilitate the drafting of this document.
(g) The Project Leader shall:
    i. identify a development methodology to be used. The methodology shall address the following: Requirements, design, implementation, and monitoring and evaluation (maintenance) phases.
    ii. identify all the important milestones in the development cycle and indicate the expected deliverables that would include: feasibility study report, development plan, requirements document, design document, testing, implementation and change control procedures.
    iii. ensure that all changes made to the system follow the change control procedures.
    iv. ensure that the project has a project plan and implementation methodology.
    v. ensure that risk assessment and management procedures have been put in place.
    vi. be charged with the responsibility of ensuring that the project has a software versioning mechanism and release plan, indicating the number of versions and releases expected and when they are to be out.

4.5.2 Requirements Phase

(a) In this phase of software development, the Systems Analyst shall identify all business, functional, constraint and quality (including performance, compatibility, usability and security) requirements of the envisaged system in consultation with the Stakeholders of the system.
(b) In this phase, the Project Team Leader shall review the efficiency of the business processes to be computerized through re-engineering. Any recommendations that come out of the reengineering process shall be communicated to the main stakeholder (or champion) who shall be responsible for channeling them to the relevant University organs for adoption in the University.
(c) At the end of the requirements phase, the Project Team Leader will present to the stakeholders a requirement specification document. The stakeholders will then validate the document to verify that their requirements have been captured correctly in accordance with the documentation standards.
(d) The stakeholders shall have reasonable time to review requirements and the Project Leader shall verify that the stakeholders agree to the requirements that come out of the requirements phase. Consequently, the requirements shall remain frozen (unless in exceptional situations) until the system is implemented and deployed to the user department.

4.5.3 Design phase

The design phase shall have the following sub-phases:

(a) **Preliminary design phase** – In this phase, the Systems Analyst in conjunction with the Project Leader and the Documentalist shall produce a design document showing the overall design of the new system. The deliverables in this phase shall be: a design document and a user interface design document.

(b) **Main design phase** – In this phase, the Systems Analyst in conjunction with the Project Leader and the Documentalist shall perform detailed design of the functionality of the new system with the aim of establishing complete details of all the possible actions and results in the requirements. This

phase shall cover: input/output design, file design and a logical data model of the envisaged system. The deliverable in this phase shall be a Design or Functional Specification document.

(c) **Review or validation phase –** In this phase the Project Team Leader in consultation with the Stakeholders shall review and validate the design documents and make any changes as recommended or appropriate. The result of this phase shall be validated design documents.

4.5.4 Implementation

The Project Leader shall ensure that:

(a) Programs are written in accordance to the University coding standards.
(b) Systems Analysis is planed for and user training executed in the best way possible with appropriate schedules for the different categories of system users.
(c) Prior to the deployment of any system (developed or procured), the system is thoroughly subjected to tests including but not limited to, unit, integration, system, volume, usability, acceptance and performance testing
(d) The project has ready and up to standard documentation before handover to the stakeholders.
(e) System changeover is planned for and executed using the best technique that will have minimum negative impact on the user operations.

4.5.5 Monitoring and evaluation

(a) The Project Team Leader will have to put in place modalities for ensuring that the system developed is reviewed after every six months or such a time deemed fit to find out if the System is still fulfilling the user requirements, and if not, appropriate actions taken to ensure that the System meets the ever-changing user needs.
(b) A system that is too costly to maintain, does not meet user requirements or is deemed to be obsolete shall be retired after consultation with all stakeholders.
(c) Any changes in any system shall be done through the change control procedure (refer to ISO documentation).

4.6 MIS Support and Use policy

4.6.1 Technical support

The Director ICTC shall ensure that every project has alternatives for staff that provide essential support service to guarantee that services are provided even in the absence these staff members. This is important for the continuity of systems and the avoidance of over-dependence on one staff member whose absence can disrupt user services.

4.6.2 User requests

All Requests for data or service by the users or stakeholders of any MIS system shall be channeled through the Director ICTC.

4.6.3 Response to requests

This shall be done as per the ICTC service charter

4.6.4 Data collection and updates

All users shall be responsible for collecting, updating, validating and verifying all data required by all Information Systems in their custody except in cases of emergency or data migration where the ICTC staff may be called upon to offer support.

4.6.5 Tracing data update

Transactions shall be made traceable through the system by use of audit trails.

4.6.6 Project team for each system

(a) For each MIS project, there shall be an ICTC project team whose composition shall be determined by the MIS Manager.
(b) There shall be functional meetings for each MIS once a month or such a time that may be deemed fit.

4.7 System ownership

The user department shall take ownership of the system and shall be responsible for the daily operation of the system.

4.8 Accessibility to information system

This shall be done as per the ICTC service charter

4.9 Software License/Maintenance Contracts

ICT Centre shall ensure that all software and equipment critical to the University operations are put on maintenance contract.

5 User Support Policy

5.1 Definition of terms

(a) *ICT project***:** Any ICT work or undertaking that happens only once, and has a clear beginning and end, and is intended to create or deploy a unique ICT technology, product, knowledge or service.]

(b) *Basic Operation Unit (BOU) Laboratory***:** 3 or more computers used by academic, non-teaching staff, or students for general use, research, in a classroom setting, or as a component of a class and operated by an autonomous department, school, faculty, institute, centre or other unit of the University.

(c) *Hardware***:** All University-owned computer and peripheral equipment (such as printers, scanners, CD-ROMS (Read only memory compact discs), network cards and multimedia equipment). Excluded from such equipment would be equipment that is already under an existing service contract, warranty, nonstandard ICT equipment for which only advisory information shall be provided.

(d) *Tools and equipment***:** The stock of shared tools maintained both centrally at ICT and within individual campuses for use by the support personnel.

(e) *ICT user support services*: ICT services directed at ICT users to enable users to effectively exploit ICT technologies, products and services available at the University. These shall mean all activities, carried out by the support personnel involving setup, creation, procurement and acquisition, installation and deployment, repair and training on ICT technologies, and products and services, with the aim of assisting users to maximize expected utility and benefit

(f) *Support coverage*: Support Site and deployment of support personnel in accordance with the assessed support load per site.

(g) *Hardware support***:** Attending to problems associated with hardware categories as listed under the support policy.

(h) *Software support***:** Attending to problems associated with software categories as listed under the support policy.

(i) *MIS support***:** support for corporate systems used by the University.

5.2 Introduction

The ICTC acquires, develops and produces a variety of ICT technologies, products and services in response to the academic business and related requirements of the University. Upon production, these require are distributed (or made available) to users. Thereafter, continuous and carefully tailored support is necessary in order for the users to fully exploit them. A policy guideline is necessary for this support.

5.3 Policy objective

(a) A guideline for the ICT User Support Service for enabling *bona fide* University ICT users to productively exploit provided University ICT resources.

(b) Specific Services include: General User Support Service; PC and User Peripheral Service; Hardware Maintenance Service; Network Support Service; ICT Staff Professional Training Service; ICT User Training Service; Operationalization of ICT Projects.

5.4 Scope

This guideline shall steer the activities of producers and consumers of ICT technologies, products and services across the University.

5.5 Policy Statements

5.5.1 University ICT projects and services

The Director, ICT shall ensure that ICT Support services to assist University ICT Users with technical and logistical support in the implementation (or roll-out) and operationalization of ICT Technologies, Projects, Products; and Services.

5.5.2 Advocacy

The ICT Centre through User Support services shall provide users with consultancy services on any ICT matter; it shall provide technical representation in all ICT related meetings and committees; it shall communicate relevant User Support information to users, and provide them with liaison interface (or escalation point) to the greater ICTC.

5.5.3 Support Coverage

(a) Support sites shall be designated by campus and to some extent by function. These shall be as detailed in the schedule of support coverage in the standards document.

(b) The ICT Support function shall provide qualified support personnel at each University campus. ICT Support personnel shall be deployed in accordance with the assessed support load per support site (or campus). The load shall be proportional to the extent to which ICTs are in use, determined mainly by the expansion of the University network and number of users there off.

5.5.4 Procurement Support

The ICT User Support function shall assist users in deriving the technical requirements and specifications of all ICT acquisitions and purchases. Other acquisitions and purchases must meet the minimum specifications as outlined in the ICT procurement policy for all hardware, software, services and

consumables in order to guarantee support by ICT under the categories outlined above. The ICT User Support function shall verify all ICT acquisitions and purchases.

5.5.5 Infrastructure support

The ICT User Support function shall assist users in carrying out surveys, design, requirements, specifications, and preparation of BOQs, material acquisition and supervision of implementation of all ICT infrastructures at the University.

5.5.6 Hardware Support

(a) The User shall be responsible for daily care and basic routine maintenance of ICT hardware under their care. ***(Refer to ICT Maintenance equipment Policy)***

(b) On a second level, the ICT Support Function shall support the hardware categories that are commonly required by users in their offices, computer rooms, laboratories and lecture theatres to perform their job responsibilities. These shall include servers, desktop computers, laptop computers, printers, scanners, digital cameras, liquid crystal display (LCD) projectors, *PDAs* (palm or pocket PC), UPSes, network access hardware, among others.

5.5.7 Software and MIS Support

(a) ICT Support shall support software categories that are commonly required by users for use in their offices, computer rooms, laboratories and lecture theatres to perform their job responsibilities.

(b) Acquisitions shall meet the minimum specifications as outlined in the ICT procurement and ICT MIS development policies for software and MIS in order to guarantee support by ICT ***(Refer to Software Development, Support and Use Policy)***. The supported categories shall include PC Operating Systems, PC Applications and Client Software, Security and Antivirus, PC backup support, among others.

5.5.8 ICT services support

(a) The ICTC shall support ICT services that are commonly required by users in their offices, computer rooms, laboratories and lecture theatres to adequately perform their job responsibilities.

(b) Acquisitions shall meet the minimum specifications as outlined in the ICT procurement policy for software in order to guarantee support by ICT.

5.5.9 Departmental Support

(a) The ICTC shall act as the second level support to the existing Computer Laboratory Attendant or Administrator for University Basic Operation Units (BOU) with ICT personnel. The ICTC shall be available to consult or to help with significant problems.

(b) The ICT centre shall not be available to provide basic and routine cleaning and simple troubleshooting for machines except where such computer laboratories are directly owned by the ICT.

5.5.10 Network devices

The ICTC shall own core network active devices such as switches, routers, bridges, gateways and related equipment including enclosures, and shall be responsible for the following:

(a) Creating and maintaining adequate operating environment (floor space, climate control, ventilation, backup power supply) for the equipment.
(b) Routine maintenance and upgrade of the equipment.
(c) Advising on all expenses incurred during repair, maintenance, and upgrade.

5.5.11 Printing facilities

A Basic Operation Unit in the University shall implement a centralized printing facility at which most print jobs shall be processed. This shall be equipped with at least one print device of appropriate specification that shall be administered from a print server. The facility shall also be equipped with at least one photocopier.

5.6 Escalation of support requests

Where necessary the ICT Support Function shall escalate user support requests to appropriate ICTC sections and to other University functional units.

5.7 Support resources

(a) The BOU shall provide Office and workshop space, furniture, and basic office amenities.

5.7.1 Tools and equipment

Every campus shall have a stock of support tools consisting of items as listed on the schedule dedicated for the support work within. In addition, a stock of shared tools shall be maintained centrally at ICT.

5.7.2 Dress and gear

Support personnel shall be supplied with protective and safety clothing and gear suitable for the tasks involved in the support activities. These shall include items such as overalls, dustcoats, dust masks, safety gloves and the management of the ICTC from time to time may determine other items.

5.7.3 Logistical Resources

(a) Towards realizing the set support standards such as turn-around time and low down time, ICT shall ensure availability of logistical resources for transport to ensure rapid movement between support sites, and, communications to ensure contact between support personnel.
(b) Transportation*:* There shall be sufficient transport services available for the support function.

(c) Communication*:* Support personnel shall be equipped with appropriate communication equipment to maintain effective contact with one another in the course of duty.

5.7.4 Enforcement

(a) The enforcement of this policy shall be the responsibility of the ICTC. This shall be ensured through strict adherence to the ICT standards.

(b) Violations will be addressed by established University and National Legal Mechanisms.

(c) Where required and applicable, an ICTC Committee shall provide oversights, insights and guidance in case of any violation.

6 ICT Equipment Maintenance Policy

6.10 Definition of Terms

(a) *Hardware*: This shall mean all University owned computer and peripheral equipment (such as printers, scanners, CD-ROMS, network cards and multimedia equipment). Excluded from such equipment shall be equipment that is already under an existing service contract, warranty, and non-standard ICT equipment and for which only advisory information shall be provided.

(b) *Tools and equipment*: The stock of shared tools maintained both centrally at ICTC and within individual campuses for use by the support personnel.

(c) *Brand name system*: A brand name computer (both hardware and software) is based on a particular company's architecture aimed at providing a unique service to its customers.

(d) *Clone or semi brand system***:** A clone is a computer system (both hardware and software) based on another company's system and designed to be compatible with it.

(e) *Central Facility:* The main hardware maintenance workshop at the ICT Centre building in Chiromo Campus.

6.11 Introduction

The University recognizes the important role of the Maintenance Section in providing quality services to its users, by ensuring that their equipment are well maintained and repaired in good time. This policy will guide the maintenance personnel at the University Central Facility as well as those at the various campuses.

6.12 Policy objective

This policy document outlines the rules and guidelines that ensure that users' PCs and related hardware are in serviceable order. It specifies best practices and approaches in ICT equipment maintenance.

6.13 Scope

(a) This policy applies to any person accessing or using the ICT infrastructure owned, managed, supported or operated by, or on behalf of, the University, including all University staff and students; and any other organization accessing University ICT services including persons contracted to repair or maintain the University's ICT equipment and suppliers of such equipment.

(b) This policy specifies the general approach that the maintenance centre shall use in providing users with the facilities; services and skills to enable them to utilize the maintenance centres productively.

(c) It describes the steps that are to be followed by the maintenance personnel in the process of providing repair support.

6.5 Policies

6.5.1 Operational logistics

(a) Operationally, users shall resolve basic problems as the first level of maintenance and support.

(b) At the second level, the OIC in each campus shall offer support to the users on issues they cannot resolve.

(c) At the third level specialist Maintenance Engineers at the Central Facility shall handle issues escalated from various campuses.

(d) The fourth and final level should enable the Central Facility to work in liaison with vendors, suppliers and hardware manufacturers to repair and/or replace faulty equipment.

(e) The Central Facility shall be charged with the responsibility of enforcing any maintenance contracts, agreements and warranties.

6.5.2 Hardware Maintenance

The ICTC shall maintain and support the supportable hardware[2]categories that are commonly required by users for use in their offices, computer rooms, laboratories and lecture theatres to perform their daily responsibilities. Users shall follow the ICT procurement policy for hardware in order to guarantee support by ICT.

6.5.3 Privately owned computer equipment/peripherals

The ICTC shall not take responsibility for the replacement, repair or upgrade of privately owned equipment/peripherals.

6.5.4 Computer Systems and Peripherals

In the case of computer systems, departments that purchase the equipment shall be responsible for the following with the aid of ICT Centre:

(a) Adequate operating environment (floor space, climate control, ventilation, and backup power supply) for the system.
(b) Installation and administration of the system.
(c) Routine maintenance and upgrade of the system.
(d) All expenses incurred during repair, maintenance, and upgrade.
(e) Full compliance with the University's Procurement and Disposal Policy/Act.
(f) Full compliance with the University's security policy, including installation and regular update of the anti-virus software.

Supplies for spares to support such systems and peripherals shall be the responsibility of the department.

[2] The supportable hardware categories are Desktop Computers, Laptop Computers, Printers, Scanners, Digital Cameras, LCD Projectors, UPSes and network equipment.

6.5.5 Tools and equipment

Every campus shall have a stock of support tools that is continually being stocked. In addition, a stock of shared tools shall be maintained centrally at the ICTC.

6.5.6 Campus workshops

Every campus shall have a designated repair facility. This facility shall take the form of a room reserved for the purpose of conducting all hardware repair and maintenance activities. The ICTC personnel in the campus shall have custody of such facility.

6.5.7 Preventive maintenance

A schedule for maintenance shall be drawn, recognizing every piece of hardware. Preventive maintenance shall be carried out according to the recommendations of the manufacturer of the hardware, in terms of frequency and method of maintenance. However, where justified by the case, service shall be provided on the basis of request.

6.5.8 Outsourced Service Agreement for Critical Equipment

Equipment not supportable[3]by ICTC shall as far as possible be placed on maintenance contracts.

6.5.9 Obsolescence of hardware

ICT hardware shall be declared obsolete according to the recommendations of the manufacturer. The hardware maintenance team shall periodically conduct maintenance to identify, retire and replace the hardware categorized as at “end-of-life.”

6.5.10 Warranty guidelines

Maintenance staff at the ICTC shall facilitate the repair and maintenance of equipment under warranty. They shall keep accurate records of the warranty of the individual items of equipment and use such information when needed to operationalize the warranty and/or guarantee for the equipment.

[3] Equipment not supportable by ICTC include Generators, Digital Line Printers, Air Conditioners and high end UPSes

7 ICT Training Policy

7.1 Introduction

A variety of services are developed and produced by the ICTC in response to the business requirements of the University. Upon production, these services are distributed (or made available) to users. Thereafter, continuous and carefully tailored training support is necessary in order for the users to fully exploit them. Policy guidelines shall be clarified for such training.

7.2 Objective

The objective of this policy is to outline the guidelines that serve as the guiding reference when planning for, organizing and conducting ICT training at the University.

7.3 Scope

(a) This policy applies to any person accessing or using the ICT infrastructure owned, managed, supported or operated by, or on behalf of, the University, including all University staff and students; and any other organization accessing University ICT services including persons contracted to repair or maintain the University's ICT equipment and suppliers of such equipment.
(b) This policy specifies the general approach to the training of all University staff and students; and any other organization accessing University ICT services, as the primary users of ICT services.
(c) It addresses the training content and methodology for ICT users.

7.4 Policy Statements

7.4.1 ICT Literacy

It shall be mandatory for all University staff to be literate users of ICT services, the level of literacy being in line with the demands of their job functions. Training shall therefore focus on building skills in users making them effective in exploiting provided ICT resources.

7.4.2 Mode of Training

(a) External ICT training shall be organised by the ICTC in response to need as may be assessed from time to time when training is not possible within the University.

(b) Internal ICT user training targeting the university community shall be scheduled on a continuous basis and shall be conducted both in the campuses and at the corporate training computer laboratory at the ICTC.

7.4.3 Trainees

(a) The ICTC shall jointly with user departments nominate trainees for external ICT training when the need for such training arises.

(b) Every Officer in Charge of Campus (OIC) shall jointly with the user departments in their campus and in response to assessed needs nominate trainees early in every quarter and forward the list to the user support manager. The number of trainees shall be as targeted in the Strategic Plan for the campus or unit. The operating unit shall make the necessary arrangements to facilitate trainees drawn from such units.

7.4.4 Training Resources

The ICTC shall in liaison with either the Project Manager or the producer of the relevant services identify the appropriate trainers for the training. These shall be as demanded by the needs of the scheduled training.

The ICT Centre jointly with the user departments shall provide necessary resources to facilitate the training

7.4.5 Training needs and Curriculum Development

OICs, Project Managers and service developers shall establish ICT training needs in liaison with user departments and service consumers. In cases where the ICTC is not well placed to train in a given area, the ICTC shall identify and recommend appropriate training and work out the cost for competent trainers.

(a) The ICTC shall develop curricula for all training including development of source material. To this end, the ICTC shall:-
   i. recommend curriculum for all external training
   ii. where possible provide training materials on-line via the University website.
   iii. where possible conduct on-line assessment tests and examinations.

(b) Where external training is sourced, the ICTC shall jointly with the external training agent, customize the content to meet the training needs of the users.

7.4.6 Acknowledgement of training

The ICTC shall issue certificates on successful completion of training and examination.

8 Database Administration Policy

8.1 Terms and definitions

a) *database* - software used for management of data objects.

b) database administrator (DBA) – The person in charge of administration and management of a database

c) *production database* – database for applications that have gone through the system life cycle as defined in the Software Development Policy.

d) *replication database* – database used for maintaining a complete copy of the production database.

e) *development database* – database used for development of applications before deployment to the integration database.

f) *integration database* – database used for testing and integrating applications before deployment into the production environment

g) *education database* - database used for use by students and staff of the university.

8.2 Introduction

Contemporary Information Systems (IS) rely on the use of emerging database technologies for storage and manipulation of data. Several challenges arise in the utilization of these database technologies, including:

(a) availability of the database service to the intended customers
(b) flexibility in terms of access through the use different interfaces
(c) administration and management of the same service

8.3 Objectives

These policies have been developed in order to achieve the following goals:

(a) provide the best possible database service to the University Management Information Systems application development and administration groups as well as the University academic and student community in general.
(b) allow the flexibility required to rapidly develop information and communication technology solutions unhindered, while at the same time providing access to expert consultation when desired.
(c) ensure that the University's data resources are firmly controlled based upon known requirements and that data changes can be audited.
(d) enhance the efficiency with which database applications are developed, deployed and executed.

8.4 Scope

(a) This ICT Policy document shall be a point of reference between the Database Administrators (DBAs), on the one hand, and application developers, Project Leaders, database users and students, on the other hand, in usage, administration and management of the database service within the University.

(b) The University database services, maintenance of user accounts; backup, and recovery shall be carried out in accordance to the ICT security policy, while training will be in accordance with the User Support and Training policy.

(c) The MIS application process will be carried out in accordance with the MIS Software Development Policy.

8.5 Policy Statements

8.5.1 Services

An appropriate channel of communication that allows the DBA to receive and respond to requests for database services shall be available e.g. email and memo.

The DBA shall provide the following services:

a) Authorization and Access Control

(i) Authorization and data control: Access to the production (and replication) databases shall be restricted to production applications and through authorized reporting tools.

(ii) Authorization outside of these applications shall be approved by the client controlling the data and will be maintained and controlled by DBA.

(iii) Access to the development and integration, as well as education databases shall be given to developers, students or members of staff working on current UMIS (or otherwise) projects or for developing their database skills.

(iv) Developers shall have a special role for functional development and integration databases that they support.

b) Development Support

(i) DBA shall provide support to the development group.

(ii) Support activities shall include, but shall not be limited to the following areas: database design or re-design; application design; application (SQL) performance analysis; disk space analysis; data recovery analysis; and data and process modeling.

c) Operational Support

Operational support shall include: production application analysis; data monitoring and reorganization; recovery management; space management; performance monitoring; exception reporting; application system move to production. These ongoing activities must occur in order for data and applications to quickly move through the Development Life Cycle process and perform efficiently in the production environment.

d) Monitoring and tuning

(a) Once the data and applications have been moved to production, the DBA shall utilize various tools to monitor their operation.

(b) The DBA shall make modifications to the data size allocations, reorganization frequency, and copy and frequency only liaison with the relevant Project Leader.

(c) The DBA shall bring application inefficiencies to the attention of the relevant Project Leader and make recommendations, if desired, on ways to tune them and make them more efficient.

8.5.2 Service Level Agreements (SLAs)

The DBA shall respond to service request in accordance to the ICTC Service Charter

9 Procurement Policy

9.1 Definitions

(a) *Department*: The University is made up of numerous units that have their own procurement needs. These units control their own resources and can therefore procure goods and services. These include Colleges, Institutes, Schools, Faculties, Academic Departments, Service Departments, Centres and administrative offices. In this policy, the term Department means the procuring entity within the University.

(b) *ICT Goods and services***:** The ICT goods and services to be provided by the selected Bidder under the Contract (such as the supply of any major hardware, software, or other components of the required Information Technologies specified, or the performance of any related Services, including software development, transportation, installation, customization, integration, commissioning, training, technical support, maintenance or repair).

(c) *Technical specifications*: A document intended primarily for use in procurement, which clearly and accurately describes the essential and technical requirements for items, materials, information systems or services, including the procedures by which it will be determined that the requirements have been met.

(d) *Emergency*: This is a sudden unforeseen crisis usually involving possible negative consequences, requiring immediate action, in this case undertaking a sudden procurement. This will be done through obtaining quotations upon the approval by the Tender Board Committee.

(e) *Project*: This is the activity of establishing and assembling all the specifications and cost elements with a view to initiating an acquisition within an agreed scope.

(f) *Quotation*: This will mean a statement of the present going market price for goods or services including the accompanying terms as provided by the intending supplier.

9.2 Introduction

The rules and regulations governing procurement of goods and services for the Republic of Kenya and which are applied by the University shall form the basis of these policy statements on procurement of goods and services.

(a) The ICTC shall assist the departments with preparation of technical specifications for the purpose of procuring goods and services related to ICT whenever need arises.

(b) The ICTC shall also assist the Procurement office in cases of emergencies to identify reputable companies or registered providers to reduce any delay in procurement.

(c) The rights and obligations of the department and the suppliers of goods and services for the project are governed by the procurement regulations, the procurement policy, the bidding documents, and by the contracts signed by the University with the suppliers of goods and services, and shall prevail in the event they are inconsistent with this policy.

9.3 Objectives

The objective of this policy is to inform and guide departments procuring ICT related goods and services at the University.

9.4 Scope

(a) The responsibility for the implementation of the project, and therefore for the award and administration of contracts under the project, rests with the University. The ICTC, shall endeavour to ensure that various departments have followed the correct procedure for procurement of ICT related goods and services.

(b) The ICTC shall assist the departments with preparation of technical specifications whenever need arises. The principles of economy and efficiency in the procurement of the goods and services involved shall guide the process. The importance of transparency in the procurement process is essential.

(c) The procedures shall conform to the University's rules, regulations and obligations and ensure that projects for various departments are pursued diligently and efficiently. The procedures shall also ensure that the goods and services to be procured meet the following criteria::
   i. are of satisfactory quality and are compatible with the balance of the project;
   ii. will be delivered or completed in timely fashion; and,
   iii. are priced so as not to adversely affect the economic and financial viability of the project.

9.5 Policy Statements

It is important for various departments to follow the procurement policy set by the University for the Procurement of goods and services. The following policy statements shall govern the units or entities of the University in the procurement of ICT goods and services:

(a) Identification of the needs and the justification for procurement of goods and services.
(b) Development of the technical specification with the help of the ICTC and ensure the specification used by the user department is up-to-date and uses state of art technology and not older than three months.
(c) Adhere to the procurement policy of the University.
(d) Comply with the financial regulations of the University.
(e) All ICT goods and services shall be delivered to the ICTC located in College of Biological and Physical Sciences (CBPS), Chiromo Campus or wherever it may be headquartered from time to time.
(f) Inventory of all the ICT goods and services procured by the various departments must be forwarded to the Director of the ICTC for record keeping purposes.

(g) ICTC shall:

i. Check the delivery schedule.
ii. Examine and test the compliance of the goods to technical specifications in accordance with the contract awarded to the supplier.
iii. Install necessary software and configure the PCs, printers and laptops and assign IP addresses for unique identification of delivered equipment.

9.6 Replacement of Goods and Services

The life cycle of the goods and services is dependent on the type of the goods and services procured by the University. On average, hardware shall be replaced after every five years if funds are available. While for software the life cycle is dependent on the release of the new versions in accordance with the software maintenance agreement. The disposal of obsolete equipment shall be governed by the University Procurement Policy.

10. Statement of Enforcement of Policy

(a) The Director, ICTC, in liaison with the University Management, ICT Centre Section Heads and the ICT Project Leaders shall be responsible for enforcing these policies and standards and where necessary shall take appropriate remedial measures.The Director of ICTC shall monitor the implementation of this policy. This policy shall be enforced and practised in the entire University.

(b) Failure to comply with these policies shall result in immediate withdrawal of services.

(c) Violation of this policy shall be addressed by appropriate University and national legal mechanisms.