INFORMATION & COMMUNICATION TECHNOLOGY

DRAFT ICT POLICY GUIDELINES

2014

Table of Contents

Abbreviations and Acronyms

(1) ATM Automatic Teller Machine
(2) BOQs Bill of Quantities
(3) BOU Basic Operation Unit
(4) BYOD Bring Your Own Device
(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) FTP File Transfer Protocol
(12) GFS Grandfather-Father-Son
(13) ICT Information and communication Technology
(14) ICTC Information and communication Technology Centre
(15) IEEE Institute of Electrical and Electronics Engineers
(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) OIC Officer in Charge of Campus
(27) PDAs Personal Digital Assistant
(28) PSTN Packet Switched Telephone Network
(29) POC Point of Contact
(30) SSH Secure Shell
(31) SANs Storage Area Networks
(32) SLA Service Level agreement
(33) SQL Structured Query Language
(34) Telnet A terminal emulation program for TCP/IP networks such as the Internet
(35) TCP Transmission Control Protocol
(36) UPS Uninterrupted Power Supply
(37) UMIS University Management Information System
(38) VPN Virtual Private Networks
(39) WAN Wide Area Network
(40) Wi-Fi Wireless Fidelity
(41) WWW World wide web
(42) ZIP "Zip" is the generic file format of a compressed archive

1. Introduction to the Policy

1.1 Preamble

The University has invested in a strong ICT base, which supports teaching, learning, research and management. Pwani University has developed its strategic plan for 2010-2020 taking cognizance of the changes in the operating environment. In this strategic plan, the University recognizes ICT as a prime mover and driver in stimulating creativity and innovation in the current highly technologically driven environment. The strategic role of ICT can therefore not be gainsaid. The performance and visibility of the University is determined to a great extent by its ICT function.

It is against this background that the University has taken the initiative of developing and regularly reviewing a blueprint that will guide in the design, development, implementation, and effective use of the ICT services and resources. 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

The purpose of this ICT Policy is to outline the acceptable use guidelines for ICT equipment and services at the University. This policy intends to promote a 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 ensure efficient and effective use of University ICT resources; protect ICT resources from injurious actions, including virus attacks, data loss, unauthorized access, network and system failures, and legal problems.

This policy seeks to guide designers, 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, reliability, enhanced performance, security, and reduce the cost of running the ICT infrastructure;
- establish information requirements and implement *security* across the University's ICT infrastructure;
- provide a framework, including guidelines, principles and procedures for the development and implementation of *Management Information Systems* 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;

- 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. This includes 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. This Policy applies to all ICT equipment, software or other facilities that is owned or leased by the University.

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

1.4 Approval of Policy Document

This draft policy document is yet to be discussed and approved for productive use by the University Management Board (UMB).

2. Network Development and Management Policy

2.1 Introduction

(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
- Wireless networks
- Virtual Private Networks (VPN)
- Connection to, access 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

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

(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 adequate, reliable and resilient to support continuous high levels of activity.

2.3 Scope

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 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 business 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, learning or administration functions take place should be connected. And every member of the University should have capability to access the University ICT infrastructure.

(c) The 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.

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 rolled out situation, major network developments shall be 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 cabling 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; wireless networks (Hotspots); Virtual Private Networks (VPN), data centers and campus Network Operation Centers (NOC)."

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, ICT.

(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 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 established.

(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 the University network security and management requirements.

2.9 Wireless Networks

2.9.1 Definition

Wireless LAN also known as Hotspot or Wi-Fi are networks rolled out using radio waves to provide mobile network access as defined under IEEE 802.11 protocol.

2.9.2 Structure of Wireless Networks

(a) Installation, configuration, maintenance, and operation of wireless networks serving on any property owned or rented by the University, are the sole responsibility of ICTC. Any independently installed wireless communications equipment is prohibited.

(b) Any request for installation of wireless device must be approved by Director, ICT.

(c) Wireless access points shall terminate at a point of connection to the University Network Backbone. In cases where it is not feasible to establish a single connection, multiple wireless gateways may be installed limited to a maximum of three hops.

(d) Wireless networks connecting to the University network shall meet overall University network security and management requirements including approved network identifiers.

2.10 Virtual Private Networks (VPN)

2.10.1 Definition

Virtual Private Network (**VPN**) extends university network across the Internet enabling users to send and receive data across shared or public networks as if they are directly connected to the University network, while ensuring security and applicable policies are observed.

2.10.2 Structure of Virtual Private Networks

(a) Authorized users of University ICT services shall be granted rights to use VPN connections if they intend to gain access to the University ICT intranet services through public networks.

(b) By using the VPN technology users are subject to the same rules and policies that apply while on campus.

(c) Users of this service are responsible for procurement and cost associated with acquiring basic Internet connectivity, and any related products or service.

(d) It is the responsibility of the user with VPN privileges to ensure that unauthorized users are not allowed access to the University networks through their credentials.

(e) All VPN services are to be used solely for the approved University business or academic purpose.

(f) All VPN service usage shall be logged and subject to auditing.

(g) Network protocols used on VPNs and communicating through the gateway must use approved configuration parameters including approved network credentials.

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, ICT.

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 rooms used for other purposes, the arrangements for access by the other user of the room shall require prior written consent of the Director, ICT. This

consent shall specifically exclude access by the other user to any communications cabinets or ICT network equipment located in the shared room.

2.11.3 Contractors

(a) Contractors providing ICT network services must obtain the prior approval of the Director, ICT and shall obtain the appropriate authorization 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, ICT.

2.11.6 Network Equipment

(a) Only designated members of the staff of ICT 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 ICT agrees that academic staff or the ICT Centre'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 ICTC 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 ICT, may make 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 ICT 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 ICT shall ensure that this access is strictly controlled and limited to specific external locations or persons.

(c) The Director ICT 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 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

(a) A user's access to the University's ICT networks will be revoked automatically:
   i. at the end of studies, employment or research contract;
   ii. at the request of the Director/Dean of Faculty/Head of Resource Centre/Head of Department or Head of Unit;
   iii. where there is a breach of these regulations

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

(c) The Registrar Administration/Academic Registrar will establish mechanisms to ensure that changes in student/employment status are communicated immediately to the Director of ICT so that their network access and e-mail accounts can be suspended or deleted as appropriate immediately.

- **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 policy 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 high 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 Vice Chancellor for appropriate action. The possible penalties may be any one or a combination of the following:

i. Suspension of the account which will be communicated to the relevant Director/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 Director/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 Director/Dean and/or the Head of Department or Head of Section requests the account be reinstated for employment/course related work only (e.g. completion of an assignment). In this case the user is required to sign an undertaking to abide by the Rules of use.
v. A system administrator can make a recommendation to disable an account to the Director, ICT. The director, ICT shall review the request and if it is considered to be, on the balance of probability, a transgression of the ICT Policy, 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.

2.12.6 Additional or Changed Equipment

(a) The Director ICT 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 ICT shall assess the likely impact on the University's ICT networks of the proposed change. The Director ICT 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.

2.12.7 External Data Communications

(a) All external data communications shall be channeled through University approved links.
(b) No external network connections shall be made without the prior written consent of the Director, ICT.
(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 University ICT network infrastructure, is prohibited, unless a proposal and justification for such connection has been authorized in writing by the Director, ICT.

2.12.8 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.

2.12.9 Web Filtering

The Director, ICT 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 promote efficient and high availability of Internet services to the majority of users.

2.13 New or Changed Use of ICT Equipment

(a) The Director, ICT shall be informed 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, ICT 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, ICT.

2.14 Monitoring of Network Performance

The Network Manager, ICTC, shall monitor and document University 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) *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.

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

d) *Spoofing* -The deliberate inducement of a user or a computer device to take an incorrect action by
e) 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 General use and ownership policy

3.2.1 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.

3.2.2 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. shared accounts are prohibited. 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 six (6) 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.

3.3 Conditions of Use of Computing and Network Facilities

3.3.1 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 ICTC 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 remote connection facilities, to offer services to others within or outside the University premises on free or commercial terms.

3.3.2 Wireless Network Users Responsibilities

(a) Any person attaching a wireless device to the University network shall be responsible for the security of the computer device and for any intentional or unintentional activities arising through the network pathway allocated to the device

(b) The University accepts no responsibility for any loss or damage to the user computing device as a result of connection to the wireless network

(c) Users shall ensure that they run up to date antivirus, host firewall and anti-malware software, and that their devices are installed with the latest operating system patches and hot fixes

(d) Users shall authenticate on the wireless network for every session

(e) Wireless network users shall ensure that their computer systems are properly configured and operated so that they do not cause inconveniences to other University network users

(f) Wireless network is provided to support teaching, research or related academic activities at the University. Use of the University wireless network services for other purposes is prohibited

(g) Wireless network users shall get their network addresses automatically; a valid network address shall be granted when connected. Use of other network addresses is prohibited.

3.3.3 Appropriate Use of Electronic Mail

Electronic mail and communications facilities provided by the University are intended for teaching, learning, research, outreach and administrative purposes. Electronic mail may be used for personal communications within appropriate limits.

3.3.3.1 Appropriate Use and Responsibility of Users

Users shall explicitly recognize their responsibility for the content, dissemination and management of the messages they send. This responsibility means ensuring that messages:

i) Are courteous and polite;

ii) Are consistent with University policies;

iii) Protect others' right to privacy and confidentiality;

iv) Do not contain obscene, offensive or slanderous material;

v) Are not used for purposes that conflict with the University's interests;

vi) Do not unnecessarily or frivolously overload the email system (e.g. spam and junk mail);

vii) Do not carry harmful content, such as Viruses viii)

Are not for commercial purposes

3.3.3.2 Confidentiality and Security

a) Electronic mail is inherently NOT SECURE.

b) As the University networks and computers are the property of the University, the University retains the right to allow authorized ICTC officers to monitor and examine the information stored within.

c) It is recommended that personal confidential material are not stored on or sent through University ICT infrastructure.

d) Users must ensure integrity of their password and abide by University guidelines on passwords. e) Sensitive confidential material shall NOT be sent through electronic mail unless it is encrypted.

f) Confidential information shall be redirected only where there is a need and with the permission of the originator, where possible.

g) Users shall be aware that a message is not deleted from the system until all recipients of the message and of any forwarded or attached copies have deleted their copies.

h) Electronic mail messages can be forged in the same way as faxes and memoranda. If a message is suspect, users shall verify authenticity with the ICTC.

3.3.3.3 User Indemnity

Users agree to indemnify the University for any loss or damage arising from use of University's email.

3.3.3.4 Limited Warranty

The University takes no responsibility and provides no warranty against the non-delivery or loss of any files, messages or data nor does it accept any liability for consequential loss in the event of improper use or any other circumstances.

3.4 Bring Your Own Device (BYOD)

a) Employees who prefer to use their personally-owned IT equipment for work purposes must secure corporate data to the same extent as on corporate ICT equipment, and must not introduce unacceptable risks (such as malware) onto the Corporate networks by failing to secure their own equipment

b) BYOD users must use appropriate forms of user authentication approved by Information Security, such as user IDs, passwords and authentication devices.

c) The following classes or types of corporate data are not suitable for BYOD and are not permitted on PODs:

   i) Anything classified SECRET or CONFIDENTIAL;

   ii) Other currently unclassified but highly valuable or sensitive corporate information which is likely to be classified as SECRET or above;

   iii) Large quantities of corporate data (i.e. greater than 1 Gb in aggregate on any one POD or storage device).

d) The University has the right to control its information. This includes the right to backup, retrieve, modify, determine access and/or delete corporate data without reference to the owner or user of the device.

e) The University has the right to seize and forensically examine any device within the University premises believed to contain, or to have contained, corporate data where necessary for investigatory or control purposes.

f) Suitable antivirus software must be properly installed and running on all devices.

g) Device users must ensure that valuable corporate data created or modified on the devices are backed up regularly, preferably by connecting to the corporate network and synchronizing the data between the device and a network drive or on removable media stored securely.

h) Any device used to access, store or process sensitive information must encrypt data transferred over the network (e.g. using SSL or a VPN)

i) Since ICT User support does not have the resources or expertise to support all possible devices and software, devices used for BYOD will receive limited support on a 'best endeavors' basis for academic purposes only.

j) While employees have a reasonable expectation of privacy over their personal information on their own equipment, the University's right to control its data and manage devices may occasionally result in support personnel unintentionally gaining access to their personal information. To reduce the possibility of such disclosure, device users are advised to keep their personal data separate from University data on the device in separate directories, clearly named (e.g. "Private" and "BYOD").

k) Take care not to infringe other people's privacy rights, for example do not use devices to make audio-visual recordings at work.

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 six (6) 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", "Pwani", " 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 Director, ICT.

(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 the Director, ICT. 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) 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.

(g) 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.

(h) 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. not run any applications that could transfer a virus such as email or file sharing in a computer where the anti-virus software is disabled. 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 VPN Policy

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

(b) All VPN access shall be strictly controlled, using either a one-time password authentication or a strong passphrase.

(c) When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel; all other traffic shall be dropped.

(d) All computers connected to the University's internal networks via VPN shall use the most up to date antivirus and anti-malware software that is the corporate standard,

(e) By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of the University's network; these machines must be configured and used in compliance with this ICT policy.

(f) VPN users shall automatically be disconnected from the University's network after thirty minutes of inactivity and the user required to logon again to reconnect back to the network. Pings or other artificial network processes to keep the connection open indefinitely are prohibited.

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 site 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, ICT, 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. 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 and 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 Backup Media

(a) Th : 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 Discs (CDs), CDRW (Read/Write CD), Digital Video Discs (DVDs)* or a *ZIP drives*. Are for medium capacity backups or archives.
   iii. *Tape cartridges (4mm tape, 8mm tape*). Are 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 Backup 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 cost effectively.

(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 the system of persons, data record and information in an organisation used in collecting, filtering, processing, creating, and distributing data. 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 existing 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* – is a diagram that shows the structure of an organization and the relationships and relative ranks of its parts and positions/jobs.

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

4.2 Introduction

Information Systems have become a vital part in many organizations as they are used to support core functions within organizations. This means that reliability is 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 replicated in future projects.

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 and standards that will ensure that the end product can stand the test of time.

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 policy.

4.3 Policy 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 development and support guidelines within University. 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

The Management Information System (MIS) section within ICTC is responsible for developing, and maintaining university wide administrative and academic systems. In order to provide a standard and reliable support to university community, ICTC has come up with a flexible policy which will govern system development & support in the University.

4.5.1 Outside ICTC (External):

MIS section shall provide systems development and support for university enterprise wide applications. However:

a) Departments & faculties may be allowed to buy software or customize software limited to internal usage.
b) Departments & faculties planning to buy software will need to acquire pre-approval for purchase from ICTC. ICTC will need to verify if the University already has licenses for the software requested or not. In addition, ICTC will verify if proposed software is compatible and conforms to university standard development software/operating systems.

c) MIS shall not provide any support to any systems built outside of ICTC department. MIS will not accept to inherit any systems developed outside of ICTC or purchased without approval from ICTC.

4.5.2 Project Planning & Organization

(a) Prior to the computerization or acquisition of any University information system, the Director, ICT 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.
(g) The Project Leader shall:
    i. identify a development methodology to be used and 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 are documented, ensure continuity of service and delivery are in conformance to the set policies;
    iv. ensure that risk assessment and management procedures have been put in place;
    v. ensure that the project has a software versioning mechanism and release plan

4.5.3 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 Leader shall review the efficiency of the business processes to be computerized through re-engineering. Any recommendations that come out of the re-engineering process shall be communicated to the main stakeholder and Director, ICT who shall be responsible in for channeling them to the relevant University organs for adoption in the University.
(c) At the end of the requirements phase, the Project 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 system users shall have reasonable time to review requirements and sign the user requirement specification document to indicate concurrence with the recorded specifications. Consequently, the requirements shall remain frozen until the system is implemented and deployed to the user department. In the event that certain unforeseen specifications or due to an adverse effect the specifications require to be revised, the entire process of system development will be restarted.

4.5.4 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.

(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 and a logical data model of the envisaged system. The deliverable in this phase shall be a Design or Functional Specification document and the User Interface Design.

(c) **Review or Validation Phase –** In this phase the Project 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.

4.5.5 Implementation

The Project Leader shall ensure that:

(a) Computer programs are written in accordance to defined coding standards.
(b) Systems Analysis is planned 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 with minimum negative impact on the user operations.

4.5.6 Monitoring and Evaluation

(a) The Project Leader shall 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.

4.6 MIS Support and Use

4.6.1 Technical Support

The Director, ICT 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 user requests for data or service by the users or stakeholders of any MIS system shall be channeled through the Director, ICT or such other approved communication channel.

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. In exceptional cases of emergency or data migration ICTC staff may be called upon to offer support, in such cases the system data owner shall validate the migrated data within a reasonable time and in any event not exceeding three months.

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 ICT Project Team whose composition shall be determined by the Deputy Director (MIS).

(b) There shall be functional meetings for each MIS regularly at least one every quarter.

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 Systems

This shall be done as per the ICTC service charter.

5. User Support Services Policy

5.1 Definition of Terms

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

(b) *Basic Operation Unit (BOU): A laboratory* with or more computers used by academic, non-teaching staff or students for general use, research, in a classroom setting 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.

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

(e) *ICT user support services*: ICT services directed at ICT users to enable them 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 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 Information Systems used by the University.

5.2 Introduction

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

5.3 Policy Objectives

(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 Policy Scope

This guideline shall steer the activities of producers and consumers of ICT technology, 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 are available to assist University ICT Users with technical and logistical support in the implementation (or roll-out) and operationalization of ICT technology, projects, products; and services.

5.5.2 Advocacy

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

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 as defined in section on ICT Equipment Maintenance 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 User 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) Software acquisitions shall meet the minimum specifications as outlined in the ICT procurement and ICT MIS development policies 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) Services acquisitions shall meet the minimum specifications as outlined in the ICT Procurement Policy in order to guarantee support by ICT.

5.5.9 Departmental Support

(a) The ICT support function shall act as the second level support to the existing Computer Laboratory Administrator for University Basic Operation Units (BOU). ICTC staff 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 ICTC.

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, environment 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

The University may 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.

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 College/Campus/Department shall provide office and workshop space; furniture; and basic office amenities to ICT Support function..

5.7.1 Tools and Equipment

Every campus shall have a stock of support tools consisting of items as determined by the support work within. In addition, a stock of shared tools shall be maintained centrally at ICT Centre.

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 other items as the management of ICT Centre may determine from time to time.

5.7.3 Logistical Resources

(a) Towards realizing the set support standards such as turn-around time and low down time, ICT Centre shall ensure availability of logistical resources for transport to ensure rapid movement between support sites and communications to ensure contact between support personnel.
(b) 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 Director, ICT. This shall be ensured through strict adherence to the ICT standards.

(b) Violations will be addressed through established University and national legal mechanisms.

(c) Where required and applicable, the Vice Chancellor shall provide oversights, insights and guidance in case of any violation.

6. ICT Equipment Maintenance Policy

6.1 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.

6.2 Introduction

The University recognizes the important role of the Maintenance unit 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 Central Facility as well as those at the various campuses.

6.3 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.

6.4 Scope

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

(b) 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 ICT central facility to work in liaison with vendors, suppliers and hardware manufacturers to repair and/or replace faulty equipment.

(e) The ICT 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 [1] 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 in order to guarantee support by ICT Centre.

6.5.3 Privately Owned Computer Equipment/Peripherals

The ICT Centre 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 such systems with prior approval shall be responsible for the following with the assistance of ICT Centre:

(a) Adequate operating environment (floor space, environment 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 Procurement and Disposal 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.

[1] The supportable hardware categories are Desktop Computers, Laptop Computers, Printers, Scanners, Digital Cameras, LCD Projectors, UPSes, IPads 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 ICT Centre.

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 preventive 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[2] 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 and the relevant University policy and regulations. 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.

[2] 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 products and services are developed or procured by the ICTC in response to the business requirements of the University. Upon production, these products and services are distributed (or made available) to users. Thereafter, continuous and tailored training is necessary in order for the users to fully exploit them. The policy shall clarify guidelines for such training.

7.2 Policy Objective

The objective of this policy is to outline the guidelines applicable when planning for, organizing and conducting ICT training at the University.

7.3 Scope

(a) This policy specifies the general approach to the training of all University staff and students; and any other stakeholders accessing University ICT services, as the primary users of ICT services.

(b) It addresses the training content and methodology for ICT users.

7.4 Policy Statements

7.4.1 ICT Literacy

It is desirable that all University staff 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 ICT resources, products and services.

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) Officer in Charge of Campus (OIC) in response to assessed needs shall jointly with the user departments in their campus nominate users and forward the names to the Deputy Director (USS&M). The operating unit shall make the necessary arrangements to facilitate trainees drawn from such units.

7.4.4 Training Resources

The ICTC in liaison with the user department shall identify the appropriate trainers for the training 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 Leaders 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 requirements of the training.

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

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 Policy Objectives

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

(a) provide the best possible database service to 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 used

8.4 Scope

(a) This 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 and Internet Policy, while training will be in accordance with the ICT Training Policy.

(c) The MIS application process will be carried out in accordance with the Software Development, Support and Use 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 MIS applications, projects or for enhancing their database skills.
iv) Developers shall have a special role for functional development and integration databases that they support.

b) Storage of Data Base User Names and Passwords

i) Database user names and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable.
ii) Database credentials may reside on the database server. In this case, a hash number identifying the credentials may be stored in the executing body of the program's code. iii)
Database credentials may not reside in the documents tree of a web server.
iv) Passwords or pass phrases used to access a database must adhere to the *Password Policy*.

c) Retrieval of Database User Names and Passwords

i) If stored in a file that is not source code, then database user names and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the user name and password must be released or cleared.
ii) The scope to which database credentials are stored must be physically separated from the other areas of code, for example the credentials must be stored in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the user name and password) and any functions, routines, or methods that shall be used to access the credentials.
iii) For languages that execute from source code, the credentials' source file must not reside in the same browseable or executable file directory tree in which the executing body of code resides.

d) Access to Database User Names and Passwords

i) Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.
ii) Database passwords used by programs are system-level passwords as defined by the Password Policy.
iii) Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the Password Policy. This process must include a method for restricting knowledge of database passwords to a need-to-know basis

e) 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.

f) 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.

g) Monitoring and Tuning

i) Once the data and applications have been moved to production, the DBA shall utilize various tools to monitor their operation.
ii) The DBA shall make modifications to the data size allocations, reorganization frequency, and copy and frequency only liaison with the relevant Project Leader.
iii) 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. Systems Administration Policy

9.1 Policy Scope

This policy applies to all University students, faculty and staff and to others charged with the support of university information technology resources. This policy refers to all University information resources whether individually controlled or shared, stand-alone or networked. It applies to all information technology resources owned, leased, operated, or contracted by the University.

9.2 Policy Statements

9.2.1 Responsibilities to the University

The System Administrator shall ensure the following:

(i) take precautions against theft of or damage to the system components;

(ii) take precautions that protect the security of a system or network and the information contained therein;

(iii) promulgate information about specific policies and procedures that govern access to and use of the system, and services provided to the users or explicitly not provided;

(iv) cooperate with the system administrators of other information technology resources, whether within or outside the University, to find and correct problems caused on another system by the use of the system under his/her control;

(v) comply with the technical direction and standards established by the ICT Centre and other guidelines or standards defined by the unit

9.2.2 Copyrights and Licenses

(i) Systems Administrators shall respect copyrights and licenses to software and other online information.

(ii) All software protected by copyright shall not be copied except as specifically stipulated by the owner of the copyright or otherwise permitted by copyright law.

(iii) Protected software may not be copied into, from, or by any University system, except pursuant to a valid license or as otherwise permitted by copyright law.

(iv) The number and distribution of copies must be handled in such a way that the number of simultaneous users in a department shall not exceed the number of original copies purchased by that department, unless otherwise stipulated in the purchase contract.

(v) In addition to software, all other copyrighted information (text, images, icons, programs, etc.) retrieved from computer or network resources shall be used in conformance with applicable copyright and other law.

9.2.3 Modification or Removal of Equipment

(i) System administrators shall not attempt to modify or remove computer equipment, software, or peripherals that are owned by others without proper authorization. Notwithstanding, such authorization may be granted for any University owned equipment through written permission of the Director, ICT.

(ii) Information technology resources that are retired or transferred to another location must have all data and licenses removed prior to release of the equipment.

9.2.4 Data Backup Services

System Administrators must perform regular and comprehensive backups for the systems under their custody according to established backup policy. System Administrators shall describe the data restore services, if any, offered to the users. A written document given to users or messages posted on the computer system itself shall be considered adequate notice.

9.2.5 Investigate Possible Misuses

(i) A System Administrator may be the first person to witness possible misuse or security breaches as described in this policy, hence the administrator must comply with the guidelines for handling misuse as set forth

(ii) Systems Administrators shall report in writing critical security breaches to the ICT Security officer immediately upon discovering the breach.

(iii) Systems Administrators shall immediately investigate any possible breach reported to them by the ICT Security officer.

(iv) System Administrators shall maintain appropriate system logs useful in tracing and identification of individual user's systems activity for a minimum of 30 days. System administrators shall beware that any log is subject to subpoena or other legal process.

9.2.6 System Integrity

(i) Systems Administrators shall be responsible for maintaining all aspects of system integrity, including obtaining releases and fixes that assure the currency of operating system upgrades, installation of patches, managing releases, installation of anti-virus software, updates of virus definitions, and the closure of services and ports that are not needed for the effective operation of the system.

(ii) System Administrators shall be responsible for prompt renewals of stipulated vendor hardware and software agreements, or as may be described in the vendor support contracts

(iii) Systems Administrators shall remain familiar with the changing security technology that relates to their system and continually analyze technical vulnerabilities and their resulting security implications

9.2.7 Account Integrity

(i) Systems Administrators shall manage accounts on a timely basis, providing new accounts and deleting old accounts in a prompt manner.

(ii) Systems Administrators shall ensure user accounts will be disabled and deleted based on the access rules for the environment and in compliance with all licensing.

(iii) Systems Administrators shall ensure that good passwords are used and that passwords are changed frequently, within the limits of the system environment.

(iv) System Administrators shall ensure that accounts can be traced to an individual person (or a group of people in the case of group accounts) and that the accounts have system access that match the authorization of the user.

(v) System Administrators shall ensure that stored authentication data (e.g., password files, encryption keys, certificates, personal identification numbers, access codes) are appropriately protected with access controls, encryption, shadowing, etc. - e.g., password files must not be world-readable.

10. Telecommunications Policy

10.1 Definition of Terms

(a) VOIP (Voice over Internet Protocol): methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. Other terms commonly associated with VoIP are IP telephony, Internet telephony, Voice over Broadband (VoBB) and IP communications, and broadband phone service.

(b) Teleconference: is the live exchange and mass articulation of information among several persons and machines remote from one another but linked by a telecommunications system.

(c) Videoconference: conducting a conference between two or more participants at different sites by using computer networks to transmit audio and video data.

(d) Underground Cable: the underground copper cable that links to the telephone exchange.

(e) Private Branch Exchange (PABX): automatic telephone switching system within a private enterprise.

(f) Internet Protocol(IP) phones: a VoIP phone or IP Phone that uses VOIP technologies for placing and transmitting telephone calls over an IP network.

10.2 Introduction

Telecommunications services and associated infrastructures are intended to support the objectives and operations of the University. These services include telephone, teleconference, video-conference, facsimile, and VOIP services. ICTC implements and supports the telecommunications infrastructure.

10.3 Policy Objective

Act as a guideline for the ICT Communication service for enabling ICT users to effectively and productively exploit provided services which include Telephone and VOIP services and Operationalization of ICT projects.

10.4 Policy Scope

This policy will apply to all users and external service providers of telecommunications services within the University.

10.5 Policy Statements

a) University ICT projects and services

The Director, ICT shall ensure that ICT Communication services will be available to facilitate users with technical and logistical support in the administration and management of University functions.

b) Advocacy

The ICT Centre through ICT Communications function 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 ICT Communications information to users, and provide them with liaison interface or escalation point to the main ICTC office.

c) Support Coverage

The ICT Communications function shall provide qualified support personnel at each University campus. ICT Communications 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 telecommunications infrastructure and number of users there off.

d) Procurement Support

The ICT Communications function shall assist users in deriving the technical requirements and specifications of all Telecommunications related 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 Communications function shall verify all Telecommunications acquisitions and purchases.

e) Infrastructure support

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

(ii) The ICT Communications function shall also be responsible for the day to day monitoring and repairs of the various telecommunication links for the University. These will include the Underground cable and the UTP cable that integrates the legacy PABX's to the routers.

f) Hardware (Telephones and IP phone) support

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

(ii) On a second level, the ICT Communications function shall support the aforementioned hardware for the users. In the event that the hardware develops a fault, the ICT Communications function shall diagnose, troubleshoot and configure hardware for users.

(iii) On a third level, where the equipment has failed to work due to configuration issues or firmware (in case of an IP phone), if it is on warranty the supplier will be contacted and the phone returned to them for further action.

g) ICT Communications services support

(i) The ICTC shall support ICT Communication services that are commonly required by users in their offices to adequately perform their tasks.

(ii) Acquisitions shall meet the minimum specifications as outlined in the ICT procurement policy for hardware in order to guarantee support by ICT. The respective department should seek further consent on the Telephone models or IP phone models to procure from ICT Communications services. This is to ensure compatibility with the existing telecommunications infrastructure.

h) Telecommunications infrastructure devices

The ICTC shall own telecommunications infrastructure active devices such as PABX's, switches, routers, Call Managers and related equipment including enclosures, and shall be responsible for the following:

(i) creating and maintaining adequate operating environment (floor space, ventilation, backup power supply) for the equipment;
(ii) routine maintenance and upgrade of the equipment;
(iii) advising on all expenses incurred during repair, maintenance, and upgrade

i) Escalation of support requests

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

j) Support resources

(i) Tools and equipment

Every campus shall have a stock of tools consisting of items dedicated for the support work.

(ii) 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 safety boots, gumboots, overalls, dustcoats, dust masks, safety gloves and other items as management may determine from time to time.

(iii) Logistical Resources

- To ensure realization of the set support standards, ICT shall provide logistical resources to ensure movement between support sites.
- Communication: Support personnel shall be equipped with appropriate communication equipment to maintain effective contact with one another in the course of duty.

k) Software and other systems running the telecommunications infrastructure

(i) ICT Communications function shall ensure that all systems supporting telecommunications infrastructure especially VOIP, including Operations Manager, Communications Manager, Attendant Console and Billing are checked for compliance in licensing.
(ii) ICT Communications function shall ensure that all software and systems aforementioned have maintenance support contract, as recommended by the manufacturer.

l) Telecommunications infrastructure routine maintenance

A schedule for maintenance shall be drawn, for the telecommunications infrastructure 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.

m) Guidelines on the use of telephones

(i) Any move, changes, or rearrangements of telecommunications services must be coordinated with the ICT Communications section. Departments are responsible for telephones that are lost, damaged or stolen.

(ii) All University departments must acquire their telecommunications services through the ICTC.

(iii) Departments that plan to procure new telephone sets shall get approval from the Manager, Communications to ensure that they are compatible with the existing telephone infrastructure.

n) Guidelines on the use of IP Phones

(i) Colleges/Faculties/Schools/Units/Departments and Divisions should seek the approval of Director, ICT when purchasing new VOIP phones to compatibility with existing systems.

(ii) All employees are prohibited from modifying the network configuration of any IP phone on campus.

(iii) All unauthorized Employees or Contractors are prohibited from updating the software that runs the IP phone. ICT Center staff shall update the software as is necessary.

(iv) All configuration changes will be made by an authorized ICT Center staff.

(v) ICT Center reserves the right to replace or remove your telephone at any time if a violation of any of this policy occurs. When a violation occurs, the employee's supervisor will be notified immediately.

(vi) ICT Center shall also provide communication within reasonable time to all employees and students of the University when maintenance will occur. ICT Center shall not schedule any kind of outage unless absolutely necessary and preferably after regular business hours.

o) Quotas for calling and level 9 access

(i) The authorization for granting of monthly quotas to specific employees is to be given by the respective Heads of Units. The Unit will be responsible for paying for the bills for all the authorized employees in the Unit.

(ii) Some cadre of staff are entitled to a quota for making calls per given month. This is currently available on the desktop wireless phones.

(iii) Level 9 Access is available to a select number of employees. The authorization for the level 9 service is to be given by the respective Heads of Units. Level 9 is currently available on analogue telephone and on VOIP.

(iv) Calls made whether local, trunk or mobile should be for University business. Calls of a personal nature are discouraged.

p) Radio communications equipment

ICTC shall play an advisory role on the design of and roll-out of any new Radio communications solution within the University, including necessary assistance with procurement and licensing of frequencies from Communications Commission of Kenya (CCK). All operational matters of the installed Radio communications equipment and related infrastructure, including enforcing observance of all legal and regulatory obligations, shall be the responsibility of the user department.

11. ICT Procurement Policy

11.1 Definition of Terms

(a) *Department*: The University is made up of numerous units. 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 qualified and 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 for use in procurement, which clearly and accurately describes the essential and technical requirements for items, materials, information systems or services, including 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 in accordance with the Procurement and Disposal Act.

(e) *Proposal:* 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) *Project:* This is a series of activities geared toward achieving a defined objective within a specified period of time.

(g) *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.

11.2 Introduction

Procurement of goods and services shall be done in accordance to the rules and policy governing the procurement of goods and services in the Republic of Kenya.

The ICT centre shall provide the following services:

(a) Assist the departments in preparation of technical specifications for the purpose of procuring goods and services related to ICT whenever need arises.

(b) Assist the Procurement office in cases of emergencies to identify reputable companies or registered providers to reduce any delay in procurement.

(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.

11.3 Policy Objectives

The objective of this policy is to inform and guide procurement of ICT related goods and services in the University.

11.4 Policy Scope

The ICTC shall assist the departments with preparation of technical specifications whenever need arises. The principles of efficiency and effectiveness in the procurement of the goods and services involved shall guide the process. Transparency in the procurement process is essential.

11.5 Policy Statements

The following policy statements shall govern the units or entities of the University in the procurement of ICT goods and services in:

(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 are aligned with the latest technology.
(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 wherever it may be headquartered from time to time or to such other place as may be agreed between the procuring department and ICT centre.
(f) All ICT goods and services shall be inspected by ICT representative(s) to ensure compliance to the technical specification prior to being commissioned for use.
(g) Inventory of all the ICT goods and services procured by the various departments must be forwarded to the Director, ICT for record keeping purposes.

ICTC shall:

i. Check the delivered of goods and services against the LPO
ii. Examine and test the compliance of the goods to technical specifications in accordance with the contract awarded to the supplier.
iii. Install software and configure delivered equipment and software.

11.6 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, ICT hardware shall be replaced after every five years in accordance with user needs and change in technology. 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 Public Procurement and Disposal Act.

12. Statement of Enforcement of Policy

(a) The Director, ICT, in liaison with the University Management, shall be responsible for enforcing these policies and where necessary shall take appropriate remedial measures.
(b) The Director of ICT shall monitor the implementation of this policy.

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