Pwani UNIVERSITY	OFFICE OF THE DEPUTY VICE CHANCELLOR (ACADEMIC AND STUDENTS AFFAIRS)	
ICT HANDBOOK	Reference	PU/DVCASA/MAN/01
	Issue/Rev.	01/00

ICT HANDBOOK

PU/DVCASA/MAN/01

Approval and Issue

Approved.. Date 06-03-2020

Dr. Musangi Jane Mutua, PhD

Chair of Council

Activity	Responsible	Signature	Date
Prepared by:	ICT Committee		15/2/2019
Reviewed by:	DVC ASA		18/2/2019
Reviewed by:	Management Board		20/2/2019

AMENDMENT RECORD SHEET

This record is revised regularly to ensure relevance to the systems and guidelines it defines. A record of contextual additions or omissions is given below:

Date	Page No.	Review/Modification Subject	Revised by:	Approved By:

FUNDAMENTAL STATEMENTS

Mandate

To provide quality education, training, research, outreach and opportunities for innovation for the advancement of the individual and society

Mission

To generate, disseminate and apply knowledge while sustaining excellence in teaching, learning and research

Vision

A world class university in socio-economic and technological advancement

Philosophy statement

Pwani University will strive to be dynamic, responsive and provide quality education, training, research, outreach and opportunities for innovation for the advancement of the individual and society. The institution is committed to invest its infrastructure and human resources so as to enhance discovery, transmission, preservation and enhancement of knowledge and to stimulate the intellectual growth and participation of students in the economic, social, cultural, scientific, and technological development of Kenya.

The University will offer disseminate knowledge in all disciplines relevant to the daily life of Kenyans for the purpose of enlightening and enabling students and others to improve their standards of living, provide for intellectual advancement and uplift their spiritual and moral status.

General statements should include the development of inclusionary practices, catering to diverse students

Motto

Shajiisho la maendeleo endelevu (Empowerment for sustainable development)

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

ATM	Automatic Teller Machine
BOQs	Bill of Quantities
BOU	Basic Operation Unit
BYOD	Bring Your Own Device
CDs	Compact Discs
CD-ROMS	Read only memory compact discs
CDRW	Read/Write CD
DBA	Database Administrator
DAS	Direct Attached Storage
DVDs	Digital Video Discs
FTP	File Transfer Protocol
GFS	Grandfather-Father-Son
ICT	Information and communication Technology
ICTC	Information and communication Technology Centre
IEEE	Institute of Electrical and Electronics Engineers
IS	Information System
ISO	International Organization for Standardization
IP	Internet Protocol
IPL	Intellectual Property
IPSec	Internet Protocol Security
LCD	Liquid Crystal Display
MIS	Management Information System
LAN	Local Area Network
NAS	Network Attached Storage
NFS	Network File System
OIC	Officer in Charge of Campus
PDAs	Personal Digital Assistant
PSTN	Packet Switched Telephone Network
POC	Point of Contact

SSH	Secure Shell
SANs	Storage Area Networks
SLA	Service Level agreement
SQL	Structured Query Language
Telnet	A terminal emulation program for TCP/IP networks such as the Internet
TCP	Transmission Control Protocol
UPS	Uninterrupted Power Supply
UMIS	University Management Information System
VPN	Virtual Private Networks
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
WWW	World wide web
ZIP	“Zip" is the generic file format of a compressed archive

1. INTRODUCTION TO THE ICT HANDBOOK

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 2014-2024 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 underestimated. 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 handbook will serve, alongside other related published documents, as the reference document on ICT standards.

1.2 Statement of Purpose

The purpose of this ICT Handbook is to outline the acceptable use guidelines for ICT equipment and services at the University. This handbook intends to promote a culture of responsibility, openness, trust and integrity. These are general guidelines on how to use computing facilities, 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 handbook seeks to guide designers, developers and users of information and ICT resources on appropriate standards to be adopted at the University. Its objectives include:

- Providing 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;
- Establishing information requirements and implement security across the University's ICT infrastructure;
- Providing a framework, including guidelines, principles and procedures for the development and implementation of Management Information Systems in the University;
- Guiding the handling of organizational information within the ICT 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;

- Upholding 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;
- Serving as the direction pointer for the ICT's mandate in supporting users, empowering them toward making maximum use of ICT services and resources and specifying the necessary approaches;
- Guiding the process of enhancing user utilization of ICT resources through training,
- Outlining the rules and guidelines that ensure users' PCs and other hardware are in serviceable order, specifying best practices and approaches for preventing failure;
- Providing a paradigm for establishing the University's database service that will support groups working on systems development, production and any other groups; and,
- Informing 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 Handbook

This handbook 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 organization accessing services over the University ICT resources; persons contracted to develop, repair or maintain the University's ICT resources; and suppliers of outsourced ICT services. This handbook applies to all ICT equipment, software or other facilities that is owned or leased by the University. Adherence to this handbook applies to all these and other relevant parties.

2. NETWORK DEVELOPMENT AND MANAGEMENT POLICY

2.1 Introduction

(a) The information and communication 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 various communication medium, 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 is implemented through appropriate University structures.

(b) The University network functions are broken down into the following areas:

- University ICT Infrastructure Development
- University Network 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 requires a policy that secures the future reliability, maintainability and viability of this valuable asset.

2.2 Objectives

a) To establish a comprehensive and uniform Network Development and Management structures for administration of the University ICT infrastructure.

b) To define the arrangements and responsibilities for the development, installation, maintenance, 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 University-wide network

2.3.1 The Network

The ICT department supports a University-wide network as a basic infrastructure service to facilitate the sharing of electronic information and resources among 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.

2.3.2 Universal Availability

a) The University network is 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 administrative functions take place should be connected. Every member of the University should have capability to access the University ICT infrastructure.

c) The network forms part of the general fabric or infrastructure of the University.

d) There is one coherent network supporting access to all general information services provided to the University members.

2.3.3 Reliability

a) High levels of availability, reliability and maintenance are major objectives in the construction and operation of the University ICT network.

b) The design and construction of the University network takes into account emerging technologies and standards wherever possible.

2.4 University ICT Infrastructure Development

2.4.1 Development Plan

The ICT Department has 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 takes into account of the University's strategic plan, usage and demand patterns, technological change, security, management and cost implications.

2.4.2 Implementation of New Developments

a) Prior to installation of the rolled out situation, major network developments are only tested in off-line simulation.

b) Two months after the live installation of the new development, the network provision that is to be replaced, wherever possible, remains in place as a "fallback" in the event of any subsequent failure of the new development when it is subject to actual user demand.

2.4.3 ICT Network Provision in New and Refurbished Buildings

a) Network provision for new/refurbished buildings is made in accordance with the specifications published from time-to-time by the ICT Department

b) Where the network requirements are of specialized nature the Officer in Charge of section/department concerned seeks further guidance from the Network Administrator.

c) c) All new buildings in the University shall incorporate an appropriate structured cabling system to allow connection to the University network.

2.5 University Network Backbone

2.5.1 Definition

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

2.5.2 Structure of University Backbone

a) The University Network Backbone connects, singly or severally, to buildings, not to individual departments or sections.

b) The planning, installation, maintenance and support of the University Network Backbone is under the control of the ICT Department.

c) The Manager, ICT, approves connection to the University Network Backbone.

d) The ICT Department adheres to and maintain copies of all relevant networking standards, and keeps abreast of national and international developments in these standards.

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

2.6 Campus LANs

2.6.1 Definition

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

2.6.2 Structure of Campus LANs

a) Wherever feasible, the network(s) within each building is 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 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 Manager, ICT are made to allow for alternative configurations.

2.7 Inter-Campus Connections

2.7.1 Definition

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

2.7.2 Structure of lnter-Campus Connection

a) Wherever feasible, the network(s) within each remote site are arranged so that there is 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 meet the University network security and management requirements.

2.8 Wireless Networks

2.8.1 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.

2.8.2 Wireless Networks Operations

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

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

c) Wireless access points terminate at a point of connection to the University Network Backbone.

d) 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.

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

2.9 Virtual Private Networks (VPN)

2.9.1 Definition

Virtual Private Network (VPN) extends the 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.

2.9.2 Virtual Private Networks Operations

Authorized users of the University ICT services are granted rights to use VPN connections if they intend to gain access to the University ICT intranet services through public networks.

a) By using the VPN technology users are subject to the same rules and policies that apply while on campus.
b) Users of this service are responsible for procurement and cost associated with acquiring basic Internet connectivity, and any related products or service.
c) It is the responsibility of the user with VPN privileges to ensure that unauthorized
d) 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.

2.10 Access to ICT Facilities

2.10.1 Communication Rooms, Cabinets and ICT Network Equipment

a) All communication rooms and cabinets are 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 communication rooms, cabinets and ICT network equipment are restricted to designated members of staff of the ICTC.
d) Any necessary access must have prior written consent of the Manager, ICT.

2.10.2 Access in an Emergency

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

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 Manager, ICT.

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

2.10.3 Contractors

a) Contractors providing ICT network services must obtain the prior approval of the Manager, 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 appropriate University ICT personnel shall accompany contractors working in main server rooms.

2.10.4 Installation of Cabling

All installations and changes of electrical power cabling in facilities housing ICT equipment are approved and managed by the Registrar (AFP) in consultation with the Manager, ICT in writing.

2.10.5 Installation of Equipment

The specification(s) of any equipment to be installed in communications rooms and cabinets and the installation of such equipment, require the prior written consent of the Manager, ICT.

2.10.6 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 Manager of ICT agrees that academic staff or the ICT Department's technical staff may install and maintain hubs and switches within local staff or student networks, such permission in every case specifically exclude the point at which these hubs and switches connect to the University's network infrastructure.

2.11 Connection and Usage of lCT Facilities

2.11.1 Connecting to the ICT Network

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

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

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

2.11.2 External Access to Servers on the Backbone Network

Definition

External access means access by persons external to the University; access to the backbone network from external locations. The following shall apply with respect to external access:

a) Where specific external access is required to servers on the backbone network, the Manager ICT ensures that this access is strictly controlled and limited to specific external locations or persons.

b) The ICT Manager will monitor compliance with access arrangements as stipulated in this ICT handbook and the relevant ICT Security Policy on Server Security issued by the University from time to time.

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

2.11.3 Domain Name Services

All Domain Name Services (DNS) activities hosted within the University are managed and monitored centrally, for the whole University, by the ICT Department.

2.11.3 Electronic Mail

Electronic mails or emails are received and stored on central servers managed by the ICT Department from where it can be accessed or downloaded by individual account holders.

2.11.5 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 Registrar (ASA) and/ or Head of Human Resource;

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 AFP /ASA will establish mechanisms to ensure that changes in employment/ student status are communicated immediately to the Manager ICT so that their network access and e-mail accounts can be suspended or deleted as appropriate immediately.

2.11.6 Additional or Changed Equipment

a) The Manager ICT is advised in advance and at the earliest opportunity, of any plan to add items of desktop service equipment, replace or relocate desktop equipment that are connected or require connection to the University's ICT network.

b) The Manager ICT assess’ the likely impact on the University’s ICT networks of the proposed change. The Manager ICT gives 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 are channeled through university approved links.

b) No external network connections are made without the prior written consent of the Manager, ICT.

c) The installation and use of leased or private links on premises owned, managed or occupied by the University requires the prior written consent of the Registrar AFP.

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

2.11.8 Web Cache Provision

a) The ICT Department is responsible for provision and management of University web cache facilities for incoming web traffic.

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

2.11.9 Web Filtering

The Manager, ICT is responsible for the implementation of appropriate filtering facilities for web-based and non-web Internet traffic. This includes MP3, MP4 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 Handbook and relevant ICT guidelines that promote efficient and high availability of Internet services to the majority of users.

2.12 New or Changed Use of ICT Equipment

a) The Manager, 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 Manager, 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. The Manager, ICT, shall effect such changes after approval.

2.13 Monitoring of Network Performance

The Network Administrator, ICT Department monitors and documents 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 Impersonating, mimicking, or masquerading as a legitimate source.

e) Denial of Service-Procedures or actions that can prevent a system from servicing normal and legitimate requests as expected.

f) Ping attack - A form of a denial of service attack, where a system on a network is "pinged," that is, receives an 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 ICT Department is committed to the provision of a reasonable level of privacy, the ICT Department 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 ICT Department protects the University's network and the mission-critical University data and systems.

c) The ICT Department shall not guarantee protection of personal data residing on University ICT infrastructure.

d) Users shall exercise good judgment regarding the reasonableness of personal use of ICT services.

e) 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, they shall consult the relevant ICT staff.

f) For security and network maintenance purposes, authorized staff within the ICT Department monitor equipment, systems and network traffic at any time as provided for in the network and development policy. The ICT Department reserve the right to audit networks and systems on a periodic basis to ensure compliance with this ICT Handbook.

3.2.2 Securing confidential and proprietary information

a) University data contained in ICT systems is classified as confidential or non-confidential.

b) 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

c) 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.

d) 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.

e) 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'.

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

g) 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 are 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

b) Property Policy, other relevant policies, or the University's code of conduct.

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

d) Sharing of the University user accounts and passwords; users shall take full responsibility for any abuse of shared accounts

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

f) Making fraudulent offers of products, items, or services originating from any of the University's account.

g) 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.

h) Port scanning or security scanning, unless prior notification is made to ICT Department management.

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

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

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

l) 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.

m) 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 is 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 because 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 Wireless network is provided to support teaching, research or related academic activities at the University.

f) 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 is granted when connected.

h) 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

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

ii. Are courteous and polite;

iii. Are consistent with University policies;

iv. Protect others" right to privacy and confidentiality;

v. Do not contain obscene, offensive or slanderous material;

vi. Are not used for purposes that conflict with the University's interests;

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

viii. Do not carry harmful content, such as Viruses

ix. Are not for commercial purposes

3.3.3.2 Confidentiality and Security

i. Electronic mail is inherently NOT SECURE.

ii. As the University networks and computers are the property of the University, the University retains the right to allow authorized ICT Department officers to monitor and examine the information stored within. It is recommended that personal confidential material is not stored on or sent through University ICT infrastructure. Users must ensure integrity of their password and abide by University guidelines on passwords.

iii. Sensitive confidential material shall NOT be sent through electronic mail unless it is encrypted.

iv. Confidential information is redirected only where there is a need and with the permission of the originator, where possible.

v. 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.

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 ICT 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 (Portable on Demand Storage):**

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

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) 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 Menageries, 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) All passwords shall be treated as sensitive, confidential University information.

f) 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.

j) The ICT Department shall be alerted immediately to investigate the incident, if it affects critical University information systems or processes.

k) As a proactive defense procedure, password cracking or guessing tools may be performed on a periodic or random basis by the relevant ICT staff. If a password is guessed or cracked during one of these scans, the affected user shall be required to change the password immediately.

3.6 Server Security

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 monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group establishes 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 Manager, ICT.

a) All servers are registered with the ICT Department. At a minimum, the following information is 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 Monitoring

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

b) Security-related events are reported to the ICT Information Security Officer, who shall review logs and report incidents to the Manager ICT. Corrective measures are 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 of the ICT Security and Internet Policy

For performing an audit, any access needed is provided to members of the University ICT audit team when requested. This access includes:

a) User level and/or system level access to any computing or communications device.

b) b) Access to information (such as electronic or hardcopy) that may be produced, transmitted or stored on the University ICT infrastructure.

c) 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

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 ICT Department on all operational issues regarding the Laboratory. Heads of units shall formally inform the ICT Department of the names and contacts of their computer Laboratory Administrators.

b) Computer Laboratory Administrators are 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 are responsible for the Laboratory's compliance with all the University ICT policies.

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

e) The ICT Department 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 ICT Department with adequate justification. The ICT Department shall study such proposals for relevance, review it for any security concerns, and must approve before implementation is allowed to proceed.

g) g) No computer laboratory shall replicate the core production services offered by the ICT Department.

h) Production services are 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.

i) The ICT Department 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 goes through screening firewalls. Computer laboratory network devices (including wireless) shall nor cross-connect a laboratory to a production network, circumventing screening firewalls.

b) Computer laboratories are 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 is prohibited. In addition, no University confidential information shall reside on any computing equipment located in such laboratories.

3.9 Anti-Virus

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

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

c) c) Computer Laboratory Administrators and owners of computers, in consultation with the relevant ICT Department personnel are responsible for executing required procedures that ensure virus protection on their computers. Computers are first being 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.

3.10 Virtual Private Network

a) Authorized users of University ICT services are 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 is 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.

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

e) 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

3.11.1 Required Physical Security

a) Secure marking: All University computer hardware shall be prominently marked, by either 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 is kept at least 1.5 meters 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.

f) 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.

g) 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.

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

i) 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.

j) Detection device test: A walk test of movement detectors is 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.

k) 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 are 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 are 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 is restricted to authorized University staff only.
h) All non-ICT Department 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 is the only authorized person to assign system, network or server passwords for relevant access to the system.
b) The System Administrator is 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 ICT Department servers are recorded in confidence with the Manager, ICT, and the record safely stored under lock and key for emergencies.
d) System audit facilities are enabled on all systems to record all log-in attempts and failures, and to track changes made to systems.

3.12 Systems Backup

3.12.1 Responsibility

All ICT Department 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, Network Administrator, Web Administrator and Database Administrators or its equivalent. The responsible staff shall arrange to perform backups as scheduled at all times. The System Administrator 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.

3.12.5 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 are stored in a locked fireproof safe within an access-controlled room.

b) A complete copy of the current removable backup set should 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 Backup Plans

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

3.13 Internet Usage

a) All software used to access the Internet is part of the University standard software suite or approved under the ISO standard.

c) All users should ensure that Internet access software incorporates the latest security updates provided by the vendors.

d) 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.

e) All Internet access software are configured to use stipulated gateways, firewalls, or proxy servers.

f) Bypassing any of these servers is strictly prohibited.

g) Accessed Internet sites shall comply with the University General Use and Ownership Policy.

h) Internet access traffic through the University ICT infrastructure is subject to logging and review.

i) The University Internet access infrastructure should not be used for personal solicitations, or personal commercial ventures. All sensitive University materials transmitted over the Internet shall be encrypted.

j) 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

a) Documentarist- This is the person who prepares and edits all the documents needed during the Information System development process.

b) 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.

c) 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 organization 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.

d) 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.

e) 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.

f) 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.

g) 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

h) User Interface - The method by which an operator or user interacts with a software program.

i) Organization chart - is a diagram that shows the structure of an organization and the relationships and relative ranks of its parts and positions/jobs.

k) 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 Software Development Policy Statements

The Systems Administration section within ICT Department is responsible for developing, and maintaining university wide administrative and academic systems. In order to provide a standard and reliable support to university community, ICT Department has come up with a flexible policy, which will govern system development & support in the University.

4.4.1 External ICT Departments:

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 ICT Department. ICT Department will need to verify if the University already has licenses for the software requested or not. In addition, ICT Department will verify if proposed software is compatible and conforms to university standard development software/operating systems.

d) MIS shall not provide any support to any systems built outside of ICT Department. MIS will not accept to inherit any systems developed outside of ICT Department or purchased without approval from ICT Department.

4.4.2 Project Planning & Organization

a) Prior to the computerization or acquisition of any University information system, the Manager, ICT in consultation with the relevant authority shall constitute an IS project team comprising all the relevant stakeholders.

b) The Manager, 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 Manager for them to be included.

e) 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.

f) The Manager, ICT shall ensure that each IS Project has an organization chart.

a) The roles and responsibilities of the different persons involved in the project development and implementation shall be clearly defined.

4.4.3 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) 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 Manager, 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.

4.4.4 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 Documentarist 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 Documentarist 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.

4.5.6 Monitoring and Evaluation

a) The Project Leader shall put in place modalities for ensuring that the system developed is reviewed
b) 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.

4.5 MIS Support and Use

4.5.1 Technical Support

The Manager, 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.

4.5.2 User Requests

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

4.5.3 Response to Requests

This shall be done as per the ICT Department service charter

4.5.4 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.

4.5.5 Tracing Data Update

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

4.5.6 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 Manager (MIS).

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

4.6 System Ownership

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

4.7 Accessibility to Information Systems

This is done as per the ICT Department service charter.

5. USER SUPPORT SERVICES POLICY

5.1 Definition of Terms

a) ICT project. Any ICT work or undertaking should have 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 for corporate Information Systems used by the University.

5.2 Introduction

The ICT Department acquires 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 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 Statements

5.4.1 University ICT projects and services

The Manager 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.

5.4.2 Advocacy

The ICT Department through User Support services provides 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 Department.

5.4.3 Support Coverage

a) Support sites are designated by the ICT Department.

b) The ICT Support function provides qualified support personnel at each University campus. ICT Support personnel are deployed in accordance with the assessed support load per support site (or campus). The load shall be proportional to the extent to which ICT services are in use, determined mainly by the expansion of the University's 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.

5.4.5 Infrastructure Support

The ICT User Support function assists 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 provides support for 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 (Tablets), UPSs, network access hardware, among others.

5.5.7 Software and MIS Support

a) ICT User Support supports 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. The supported categories shall include PC Operating Systems, PC Applications and Client Software, Security and Antivirus, PC backup support, among others.

5.4.8 ICT Services Support

c) The ICT Department 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.

d) Services acquisitions shall meet the minimum specifications as outlined in the ICT Procurement Policy in order to guarantee support by ICT.

5.4.9 Departmental Support

a) The ICT support function shall act as the second equivalent, for University Basic Operation Units to help with significant problems.

b) The ICT Department staff shall be available to provide basic and routine cleaning and simple troubleshooting for machines except where such computer laboratories are directly owned by the ICT Department.

5.4.10 Network Devices

The ICT Department owns 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.

5.4.11 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.

5.5 Escalation of Support Requests

Where necessary the ICT Support function escalates user support requests to appropriate ICT Department/sections and to other University functional units.

5.6 Support Resources

The University Management shall provide office and workshop space; furniture; and basic office amenities to ICT Support function.

5.6.1 Tools and Equipment

Each 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 the main campus ICT Department.

5. 6 .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 Department may determine from time to time.

5. 6 .3 Logistical Resources

a) Towards realizing the set support standards such as tum-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.

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 ICT Department 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 Department building in Killifish Campus.

6.2 Introduction

The University recognizes the important role of the Maintenance Services in providing quality services to its users, by ensuring that their equipment is well maintained and repaired in good time. This policy will guide the maintenance personnel at the Central Facility at the Main campus

6.3 Policy Objective

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

6.4 Policy Statement

6.4.1 Operational Logistics

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

b) At the second level, the network administrator in each campus shall offer support 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 ICT Department maintains and supports the supportable hardware 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 University Procurement Policy in order to guarantee support by ICT Department.

6.5.3 Privately Owned Computer Equipment/Peripherals

The ICT Department 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 Department:

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. Full compliance with the Procurement and Disposal Act.
e) Full compliance with the University's security policy, including installation and regular update of the anti-virus software.
f) Supplies for spares to support such systems and peripherals shall be the responsibility of the department.

6.5.5 Tools and Equipment

Each 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 main campus ICT Department.

6.5.6 Campus Workshops

Each campus shall have a designated repair: facility. This facility shall take the form of a room reserved for conducting all hardware repair and maintenance activities. The ICT Department 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 based on request.

6.5.8 Outsourced Service Agreement for Critical Equipment

Equipment not supportable by ICT Department shall as far as possible be placed on maintenance contracts.

6.5.9 Obsolescence of Hardware

ICT hardware is 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."

7. ICT TRAINING POLICY

7 .1 Introduction

A variety of products and services are developed or procured by the ICT Department 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 Key Aspects of the ICT Training

7.3.1 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.

7.3.2 Mode of Training

a) External ICT training shall be organized by the ICT Department 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.

7.3.3 Trainees

The ICT Depart shall jointly with user departments nominate trainees for external ICT training when the need for such training arises.

7.3.4 Training Resources

The ICT Department 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.

7.3.5 Training Needs and Curriculum Development

Project Leaders and service developers shall establish ICT training needs in liaison with user departments and service consumers. In cases where the ICT Department is not well placed to train in a given area, the ICT Department will identify and recommend appropriate training and work out the requirements of the training.

a) The ICT Department shall develop curricula for all training including development of source material. To this end, the ICT Department shall where possible:

- recommend curriculum for all external training
- provide training materials on-line via the University website
- conduct on-line assessment tests and examinations

b) Where external training is sourced, the ICT Department 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 ICT Department 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 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 Policy Statements

8.4.1 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) Development Support

i. OBA 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.

8.4.2 Service Level Agreements (SLAs)

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

9. SYSTEMS ADMINISTRATION POLICY

9.1 Policy Statements

9.1.1 Responsibilities to the University

The System Administrator ensures 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

v. within or outside the University, to find and correct problems caused on another system by the use of the system under his/her control;

vi. comply with the technical direction and standards established by the ICT Department and other guidelines or standards defined by the unit

9.1.2 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.) retrieve from computer or network resources shall be used in conformance with applicable copyright and other law.

9.1.3 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 Manager ICT.

ii. Information technology resources that are retired or transferred to locations unrelated to Pwani University must have all data and licenses removed prior to release of the equipment.

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

9.1.5 System Integrity

i. Systems Administrators are 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 are 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 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 those 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 matches the authorization of the user.

v. System Administrators shall ensure that stored authentication data (e.g., password files, encryption keys, certificates, personal identification numbers, and 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.

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

g) 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, videoconference, facsimile, and VOIP services. ICT Department implements and supports the telecommunications infrastructure.

10.3 Policy Objective

The Telecommunications Policy acts 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 Statements

a) University ICT projects and services

The Manager, ICT ensures that ICT Communication services are available to facilitate users with technical and logistical support in the administration and management of University functions.

b) Advocacy

The ICT Department through ICT Communications function provides 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 ICT office.

c) **Support Coverage**

The ICT Communications function provides qualified support personnel at each University campus. ICT Communications personnel are deployed in accordance with the assessed support load per support site (or campus). The load shall be proportional to the extent to which ICT Services are in use, determined mainly by the expansion of the University telecommunications infrastructure and number of users thereof.

d) **Procurement Support**

The ICT Communications function assists 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

University 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 verifies all Telecommunications acquisitions and purchases.

e) **Infrastructure support**

i. The ICT Communications function assists 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 is also being 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 PABXs 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 supports 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 ICT Department supports 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 ICT Department owns telecommunications infrastructure active devices such as PABXs, switches, routers, call managers and related equipment including enclosures, and are 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 escalates user support requests to appropriate ICT Department and to other University functional units.

j) Support resources

i) Tools and equipment

Each 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 includes 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) Radio communications equipment

ICT Department 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 Authority of Kenya (CAK). 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.

11.0 INFORMATION SYSTEMS ACCESS CONTROL POLICY

11.1 Introduction

The purpose of this policy is to assist in preventing any unauthorized access to Pwani University systems. Insufficient systems access controls or unmanaged access to information could lead to unauthorized disclosure or theft of information. The purpose of this policy is to define the correct use and management of access controls at Pwani University.

11.2 Objectives of policy

The key objective of this policy is to set controls, which can be applied to help reduce the risks associated with accessing the university systems.

11.3 Policy Statement

Only authorized users are granted access to information systems, and users are limited to specific defined, documented and approved applications and levels of access rights. Computer and communication system access control is to be achieved via user IDs that are unique to each individual user to provide individual accountability.

Who is affected: This policy affects all staff of Pwani University as well as non-employees such as ICT service providers. Employees who deliberately violate this policy will be subject to disciplinary action.

Affected Systems: This policy applies to all information systems owned or operated by Pwani University. Similarly, this policy applies to all platforms (operating systems) and all application systems.

Entity Authentication: Any user (remote or internal), accessing Pwani University networks and systems, must be authenticated. The level of authentication must be appropriate to the role of the user in the system.

System Access Controls: Access controls will be applied to all Pwani University systems to ensure that data is not improperly disclosed, modified, deleted, or rendered unavailable.

11.3.1 User Access Management

Access Approval: System access will not be granted to any user without appropriate approval. Line managers are expected to immediately notify Deputy Vice Chancellor Administration Finance Planning (Non-Teaching Staff) or Deputy Vice Chancellor Academic and Student Affairs (Teaching Staff) and report all significant changes in end-user duties or employment status.

Each user must be allocated access rights and permissions to computer systems and data that:

- Are commensurate with the tasks they are expected to perform.

- Have a unique login that is not shared with or disclosed to any other user.
- Have an associated unique password that is requested at each new login.

Users are expected to fill a system access control form, PU/ICT/FORM/ICT/09 01/00

in Appendix 1

User access rights will be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

User privileges are to be appropriately changed if the user is transferred to a different job.

Limiting User Access: PU approved access controls, such as user logon scripts, menus, session managers and other access controls will be used to limit user access to only those information systems applications and functions for which they have been authorized.

Standard of procedures **(PU/ICT/SOP/04)** in Appendix 2 will provide guidelines on creation, modification and deletion of user accounts.

11.3.2 Access Restriction

11.3.2.1 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 Manager ICT upon receipt of any such complaint, the Manager 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 or any high risk.

c) When a complaint is classified as "non-serious,” the Manager ICT is authorized to suspend the account for a minimum period of four weeks. The following shall apply:

   i. A system administrator can make a recommendation to suspend an account to the Manager, ICT. The Manager, 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.

   ii. An account may also be suspended, if a request has been made to the Manager, ICT from a systems administrator of another system, with a reasonable and accepted case for suspension.

iii. 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.

d) When a complaint is classified as "serious," the Manager ICT shall refer the complaint to the Deputy Vice Chancellor AFP 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 DVC AFP (Non-Teaching Staff) and/or DVC ASA (Teaching Staff). Suspension of the account shall be for a minimum period of four weeks.
ii. Permanent disabling of the account shall be taken, where the severity of the offence warrants such action.

e) Reinstatement of Accounts

i. Accounts may be reinstated before the end of the suspension period where either the student or staff presents information to the Manager ICT, which indicates that he or she was not involved in the transgression of the Rules of Use, or the Registrar (ASA) and/or Head of Human Resource requests the account be reinstated for employment/course related work only (e.g. completion of an assignment).
ii. The Vice Chancellor may recommend reinstatement of the suspended/disabled account following a successful appeal

11.3.3 User Responsibilities

It is a user’s responsibility to preve
gain unauthorized access to Pwani university systems by:

- Following the Password Policy Statements outlined in Pwani University ICT handbook
- Ensuring that any PC they are using that is left unattended is locked or logged out.
- Leaving nothing on display that may contain access information such as login names and passwords.
- Informing line managers of any changes to their role and access requirements.

11.3.4 Policy Compliance

Compliance Statements: User’s seeking
must sign a system access request form, **PU/ICT/FORM/ICT/09**, in Appendix 1 prior to issuance of a user-ID. A signature on the systems access request form indicates the user understands and agrees to abide by Pwani university policies and procedures related to computers and information systems.

Audit Trails and Logging: Logging and auditing trails are will be conducted when a user makes access to Pwani University systems.

11.3.5 Confidential Systems:

Access to confidential systems will be logged and audited in a manner that allows the following information to be deduced:

- Access time
- User account
- Method of access

Audit trails for confidential systems should be backed up and stored in accordance with Pwani University back-up and disaster recovery plans. All system and application logs must be maintained in a form that cannot readily be viewed by unauthorized persons.

11.3.6 Access for Non-Employees/Third Party Access

Individuals who are not employees, contractors, consultants, or service providers must not be granted a user-ID or otherwise be given privileges to use Pwani University computers or information systems unless the written approval of the Department Head has first been obtained. Before any third party or business partner is given access to this PU computers or information systems, an agreement defining the terms and a responsible manager at the third party organization must have signed conditions of such access.

11.3.7 Unauthorized Access:

Employees are prohibited from gaining unauthorized access to any other information systems or in any way damaging, altering, or disrupting the operations of these systems.

12.0 ELECTRONIC RECORD MANAGEMENT SYSTEMS POLICY

12.1 Definition of Terms

Classification: The systematic identification and arrangement of business activities and / or records into categories according to logically structured rules.

Conversion: The process of changing records from one medium or format to another.

Document: Recorded information or object, which can be treated as a discrete unit.

Migration: The act of moving records from one system to another, while maintaining their authenticity, integrity, reliability and usability.

Preservation: Processes and operations used in ensuring the technical and intellectual survival of authentic records over time.

Records: Information created, received and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business.

Records management: The efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.

Records system: An information system which captures, manages and provides access to records through time

12.2 Introduction

E-records management is a vital function in a University; this policy helps in maintaining standards in e-records management. This policy shall endeavor to provide basic guidelines on managing of electronic records in the university.

12.3 Policy Objectives

The main objective of this policy is to have a document, which can serve as a guide to the entire university, in order to have standards in e-records management.

12.4 Policy Statements

Each department must have in place adequate systems for documenting its principal activities and ensuring that it creates and maintains records possessing authenticity, reliability, integrity and usability. There must be a clear allocation of responsibility within each department for all aspects of record keeping, including classifying documents and secure disposal. The ownership of information must also be clarified, so that there is no ambiguity regarding responsibility for its maintenance and disposal. Shared drives, mailing lists and role accounts should be used as a default.

Line managers should ensure that when a member of staff leaves, responsibility for records held on personal drives or other areas not accessible to colleagues is transferred to another member of staff; and out of date information deleted.

Records systems must be adequately documented, so that their effective operation does not depend on the memory of individual members of staff. They should also be periodically reviewed and modified where necessary, to ensure that they continue to support local needs. In particular, electronic systems storing data that may be required for evidential purposes should be regularly monitored and audited: it must be possible to demonstrate the reliability of the system, so that the integrity of the data cannot be questioned.

12.4.1 Creating Records

Records must be accurate and complete, so that it is possible to establish what decisions and actions have been taken, and why. The quality of the records must allow staff to carry out their work efficiently, demonstrate compliance with statutory and regulatory requirements, and ensure accountability and transparency expectations are met.

Information should be compiled at the time of the event or transaction to which it relates, or as soon as possible afterwards, and protected from unauthorized alteration or deletion. Where relevant, templates should be used, so that documents are produced consistently and quickly.

Standardized referencing and titling are essential, so that information can be promptly identified and retrieved. Naming conventions and glossaries should be used to ensure the consistent use of terms. Version control is also required for the drafting and revision of documents, so that different versions can be distinguished and the latest version readily identified.

12.5.2 Classification

All records will be organized logically, so that they can be easily and speedily retrieved. A classification scheme or filing structure should be devised, based on an analysis of a department's fun
documents are organized appropriately and consistently. Similar records should be grouped together: if the contents of folders are too diverse, it will be difficult to locate material and assign appropriate retention periods.

12.5.3 Access and security

It must be possible for staff to retrieve the information they need to carry out their work. Records that are consulted frequently should be kept nearby. Semi-current records (i.e. those referred to occasionally or which need to be retained for legal or regulatory reasons) should be stored offsite.

Records shall be made available as widely as possible. Information that other staff use or may require shall be stored on a shared drive or within a centralized filing system, so that departments can operate efficiently when individuals are absent. Where appropriate, data should also be shared across Pwani University in order to avoid wasting resources recreating information that already exists and storing duplicate data unnecessarily. Information that is only accessible to a single person should therefore be kept to a minimum.

Appropriate levels of security must be in place to prevent the unauthorized or unlawful use and disclosure of information. Electronic records containing confidential information must be stored securely when not in use, and access only provided to authorize staff. Screens should be locked when computers are unattended. Restricted electronic data should be protected through the use of access controls and, where appropriate, encryption.

Information held in digital systems shall also be protected from unauthorized alteration, copying, movement or deletion: if possible, the systems should maintain audit trails allowing all actions to be traced to specific people, dates and times. It is essential that any data held on portable storage devices, such as laptops, USB flash drives, portable hard drives, Compact Discs (CDs), Digital Video Discs (DVDs), and any computer not owned by Pwani University (PU), is kept secure and protected from theft.

12.5.4 Preserving records

Departments shall develop procedures to ensure that records of continuing value remain accessible, usually on a network drive or central server, so that they are backed up and safeguarded from hardware and software failure. Records shall be stored in conditions appropriate to their medium and format, taking into account operational needs, retention periods and costs. They shall be protected in storage from potential hazards, such as fire and flood. Environmental conditions within storage areas shall be maintained at stable levels to minimize the risk of the records deteriorating.

Records shall be reviewed annually. Where necessary, electronic records shall be converted to newer formats and migrated to other systems, so that they are always accessible and usable. Processes shall also be in place to protect documents from being inadvertently overwritten, for example, by using templates when creating new versions of documents.

A small percentage of Pwani Universit
permanent preservation for their long-term reference or historical value,
providing evidence of PU's most sig
documenting its policy formation, and tracing the development of its fabric and infrastructure. The officer designated in writing shall develop selection criteria for records that are to be retained permanently.

12.5.5 Retention schedule

A retention schedule lists the main categories of records held by an organization, and how long they are to be retained in order to meet operational needs; comply with statutory and regulatory requirements; support accountability and protect the interests of staff, students and other stakeholders. It provides a uniform system for the disposal of information, preventing it from being either discarded prematurely or kept unnecessarily.

12.5.6 Disposal

Records shall be reviewed regularly and working copies, trivial emails, out-of-date reference material and unnecessary duplicates destroyed to prevent ephemeral material taking up space required by declared records.

Disposal of records, shall be controlled by the retention schedule (See Appendix 3), and carried out by authorized staff. When the retention period expires, all copies are destroyed, wherever they are held. Destruction shall also be documented, to provide evidence that retention schedules have been followed. Restricted or sensitive records shall be kept secure whilst awaiting destruction and be destroyed confidentially. Electronic data must be deleted so that it is completely erased and irrecoverable.

Software systems should include functionality to delete data, where appropriate, in order to avoid long-term retrieval problems and contravention of the Data Protection Principle. Records shall not be destroyed if they are required in connection with an on-going or pending investigation, grievance, complaint or legal dispute.

12.5.7 Vital records

Records that are vital to the continued functioning of PU in the event of a disaster (e.g. fire, flood, virus attack) shall be identified and protected. These include records that would recreate PU’s le
rights, and ensure that it continues to fulfil its obligations to its stakeholders (e.g. current financial information, contracts, proof of title and ownership and research data). Vital records shall be stored on central servers, so that they are protected by appropriate back-up and disaster recovery procedures. Standard of procedures on electronic records management are indicated in Appendix 3 (PU/ICT/SOP/04).

13. INFORMATION SYSTEMS INCIDENT MANAGEMENT POLICY

13.1 Definitions

An Information Systems Incident is the occurrence or development of an unwanted or unexpected situation, which indicates:

a) a possible breach of an information security framework policy or
b) a failure of information security controls which have a significant probability of compromising business operations or
c) systems failure due human, software, hardware or natural causes.

Examples of information incidents include:

- The loss or theft of data or information.
- The transfer of data or information to those who are not entitled to receive that information.
- Attempts (either failed or successful) to gain unauthorized access to data or information storage or a computer system.
- Changes to information, data or system hardware, firmware, or software characteristics without the ICT's department, knowledge, instruction, or consent.
- Unwanted disruption or denial of service to a system.
- The unauthorized use of a system for the processing or storage of data by any person.
- Introduction of malware into a computer or network, e.g. a phishing or ransomware attack
- Breaches of physical security e.g. forcing of doors or windows into secure room or filing cabinet containing confidential information left unlocked in accessible area

Classified information is information that is confidential, highly confidential or requires enhanced protection to ensure integrity or availability due to its nature.

13.2 Introduction

Information systems incident management is a vital function in a university; this policy helps in maintaining standards in handling reporting of data loss in ICT systems. The guidelines of this policy seeks to ensure timely response to information systems incidents.

13.3 Policy Objectives

The objective of this policy is to ensure a consistent and effective approach to the management of information systems incidents, including communication through email on events and weaknesses. It enables the efficient and effective management of incidents by providing a definition of an incident and establishing a structure for the reporting, recording and management of such incidents.

13.4 Policy Statements

Incidents are reported promptly and responded to in a quick, effective and orderly manner in order to reduce the negative effect of incidents, to repair damage and to inform policy and mitigate future risks.

13.5.1 Incidence Management

All members of the University shall be made aware of the procedure for reporting information systems incidents and their responsibility to report such incidents. All Incidents shall be reported promptly to the IT Service Desk in accordance with incident reporting procedures**.** See standard of procedures in Appendix 4 (PU/ICT/SOP/06).

All incidents shall be managed in accordance with the Incident Management Response Procedure. The severity of the incident shall be assessed and the management response shall be proportionate to the threat.

Key information about serious incidents, including the impact of the incident (financial or otherwise), shall be formally recorded and the records shall be analyzed in order to assess the effectiveness of information security controls. New risks identified because of an incident are assigned to the relevant risk owner. All risks are mitigated promptly in to eliminate loss of data.

A representative of every department shall be trained in digital evidence collection, retention, and presentation, in accordance with legislative or regulatory obligations. Authorized individuals shall report serious incidents to the appropriate external authorities where relevant.

13.5.2 Responsibilities

All members of the University are responsible for reporting actual or suspected information systems incidents to the relevant internal contact as soon as possible in accordance with the incident reporting procedure.

Contractors using the University's inf
required to note and report any significant information security weaknesses in those systems or services.

The responsibility for reporting serious Information Systems Incidents to external authorities lies with Management unless otherwise delegated in the Incident Management Standards Operating Procedure.

14. BACK UP RETENTION POLICY

14.1 Introduction

Back up retention is a vital function in a University; this policy helps in maintaining standards in systems data kept in storage media. This policy endeavors to provide guidelines to the university on retention of data

14.2 Policy Objectives

The main objective of this policy is to have a document, which can direct the university, to have uniform standards in backup retention.

14.3 Policy Statement

This policy applies to backups of user data that are copied onto any backup media, including disk-to-disk storage. User data is stored on disks on our computer systems.

Periodically, backup copies of this data are saved onto storage media. This is useful in case of a system failure (and files have to be restored from the backup media) or in the case of a user accidentally erasing one of their files (and again, that file can be restored from the backup media).

14.3.1 Retention Period and Media Rotation

The retention period for back-up media is set in such a manner as to minimize the risk of catastrophic loss of data at reasonable media cost. This Policy directs how long these backup storage media are kept (their retention).

PU shall use the GFS (Grandfather–Father–Son) retention method for maintaining hierarchical restore points. GFS method describes a rotation scheme whereby a daily backup (the son), a weekly backup (the father) and a monthly backup (the grandfather) are created to maintain a hierarchical backup strategy.

Each week, one full daily backup (latest from that week) is promoted from a son to a father and is deemed the weekly backup. Each month, a father (latest from that month) is promoted to a grandfather and is deemed the monthly backup. For the GFS policy to work, a successful sync is needed every day.

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

14.4.2 File Retention Periods

Files, which are not deleted from a as their account is kept active. System files and log files may be retained for up to seven years for proper administration of systems and statistical analysis of log data. This holds for all servers/systems**.** Table in **Appendix 5** shall inform on retention period of backups. Standard of procedures in **Appendix 6 (PU/ICT/SOP/03)** provide guidelines on retention of back up.

14.4.3 Additional Information

Backups of data occur every day, seven days a week, 365 days a year. These backups are performed once a night. While some of the backups are performed to a storage media, most backups are actually copied to online disk storage locally at the Main Campus or at a remote location.

15. SOCIAL MEDIA POLICY

15.1 Introduction

With the rapid growth and application of social media, Pwani University recognizes the need to have a policy and guidelines, which ensure that those who use social media, either as part of their job, study, association with the University or in a personal capacity, have guidance and an understanding of best practice where social media are used, and to be aware of the potential issues and risks that can arise from its misuse.

The University expects that Pwani University staff, students and affiliates who contribute to social media will familiarize themselves with this policy and related guidelines and will act responsibly in references to Pwani University in their social media and online activities. This policy should be read and applied within the framework of the University's Statute, rules, regulations, policies and procedures as amended from time to time.

15.2 Definitions

Social Media is a broad term used to describe a range of online tools such as websites, web-based platforms and applications that are designed for online interaction, content consumption and generation. Examples of social media applications, channels and platforms include Facebook, Google Plus, Twitter, Tumblr, Snapchat, WordPress, Blogger, Wikipedia, Amazon ratings, Flickr, Instagram, YouTube, Vimeo, Viddler, Facebook Messenger, WhatsApp, Google Hangouts, chat rooms, email, etc. This list is fluid as social media continues to evolve and different applications replace others.

15.3 Policy Statement

Personal, academic and professional use of social media by Pwani University staff, students and

affiliates must not engage in misconduct. Misconduct comprises behavior within or without the precincts of the University, or whilst on official business of or representing the University, without just excuse which

a) constitutes a breach of any statute, regulation or rule of the University; or

b) constitutes a failure or refusal to comply with any punishment or order imposed or made under these rules; or

c) constitutes a failure or refusal to obey a lawful order; or

d) constitutes conduct that tends to bring the University or any part of it or a member of its staff or a student or any part of its student body into contempt or disrepute; or

e) Interferes with the governance and proper administration of the University; or interferes with the conditions necessary for teaching, learning or research.

15.4.1 Principles

General Conduct

Depending on the context, employees and students may be seen to be representing Pwani University and should, at all times, act with due care, consideration and responsibility on all

Social media fora. Particularly,

1. Users may not make official statements on behalf of the University unless they are duly authorized to do so. In the case of an emergency or crisis involving the University or members of the University Community in their capacity as such, all communication will happen under the auspices of Pwani University Communications Services.
2. Users may engage in good faith, in the best interests of the University and with the care and skill that can reasonably be expected from a person with his or her knowledge and experience.

Value-based conduct

It is expected that users reflect the core values of the University in any social media activity. These are to always act ethically, respectfully and responsibly as indicated in the table below: -

S/N	Conduct	Promoting	Preventing
1	Ethical Conduct	a) in letter and in spirit, the rules of the University and laws of the country b) Ethical treatment of people c) Ethical use of resources	a) Violation of confidentiality
2	Respectful Conduct	a) human rights and social responsibility b) equity and equal opportunity c) academic freedom and freedom of expression d) trustworthiness e) integrity f) fairness g) courtesy	a) the abuse of power b) gender, racial and other forms of harassment c) disrespect for persons and property d) discrimination on the basis of race, gender, religion, disability, gender orientation or age
3	Responsible Conduct	a) transparency b) inclusivity c) accountability d) good practice e) mutual responsibility for maintenance of an ethos and environment conducive to safety f) security and well-being	a) misuse of personal and university information and property and the name of the University b) improper conflicts of interest c) practices threatening safety, security, health or well-being d) political action which impinges on the rights of others

15.3.2 Roles and Responsibility

The relevant social media representatives are the first point of referral for all enquiries regarding a particular social media post or account since content is generated from multiple sources. The Pwani University community are advised to contact or refer questions to this person as a first step.

Should there be a likelihood of reputational or brand risk, users are advised to contact Marketing and Communications for comment/review.

Academia

All academics and research experts are encouraged to engage in public debate and to contribute to the public and digital spheres through commentary within their respective areas of expertise, and are encouraged to liaise with the ICT Manager in order to ensure effective coverage and to limit any possible negative publicity.

Students and Staff

Students and staff who require a social media presence with regards to Pwani University or its affiliates are requested to contact the ICT Manager to assist with best practices and to approve branding and the use of Corporate Identity for the channels.

16. WEBSITE POLICY

16.1 Definitions of Terms

Applet: A small application program that can be called up for use while working in another application.

Application: A computer program used for a particular type of job or problem.

Department: A functional unit within the University.

Domain: The URL used to access a website.

Footer: A line of information placed at the end of a web page for purposes of identification.

Head of Department: The person in charge of a department.

Homepage: The initial page of a website on the World Wide Web.

Navigation: The main links on a website that aid in traversing the website by its hierarchical structure.

Plug-in: Accessory software package that is used in conjunction with an existing application to extend its capabilities or provide additional functions.

Social Media: Online forms of communication, which include blogs, microblogs such as Twitter and social networking sites such as Facebook.

Sub-domain: A child of a domain.

Template: The pattern and layout of a web page.

URL: Uniform Resource Locator: a protocol for specifying addresses on the Internet.

User: A person who accesses the website with the purpose of getting information.

Web page: A single, usually hypertext document on the World Wide Web that can incorporate text, graphics, sounds, video or other digital assets.

Web server: A computer that makes web services available on the Internet.

Website: A collection of related web pages containing images, videos or other digital assets.

Website Representative: The person in charge of a departmental website.

Website Management Committee: A committee appointed by the Vice Chancellor, in charge of the University Website.

16.2 Introduction

Pwani University (PU) website is becoming a major source of information for the University community and external users. For this reason, it has become necessary for the University to put in place measures that promote its management and use to enhance her presence in the World Wide Web.

16.3 Objectives of Policy

This policy will govern the design, development, maintenance and management of cohesive and consistent user-friendly website and pages across the University. It will help students, staff and other external users to achieve their online goals easily and efficiently.

16.4 Scope of Policy

This policy governs web-based documents made available via the PU domain www.pu.ac.ke and its sub domains

16.5 Policy Statement

- The PU website aims to provide accurate, useful and timely information on all aspects of the University's activities to both members of the University and external users.
- Users of University web resources will not make use of, or publish, material that is obscene, libelous or defamatory or in violation of any right of any third party.
- Users of University web resources will not publish material which would bring the name of PU into disrepute
- All pages within the University website will conform to the University's ICT security policies
- The design of all University web pages will conform to the technical and design requirements developed by the University's Web Management Committee

16.6 Responsibility for Web Pages

- The Vice Chancellor, under whose auspices the University's website management committee operates, is responsible for the University website. The primary function of the Website Committee is to coordinate the management of the website to ensure it remains relevant in all aspects.
- Each Departmental head is responsible for legal compliance, accuracy, timeliness and completeness of the content on their web pages. They must take every reasonable care to ensure this.

- Each Departmental head should periodically audit (at least once every 3 months) content of their web pages for data accuracy, appropriateness and legal compliance.
- The Website Management Committee will design and maintain the following pages on the University website:
    - Global and local home pages
    - Index pages for Campuses, Schools, Departments, Courses, Research and staff
    - Contact pages, people finder and search facilities

- Heads of Academic and administrative units including other service areas will designate one person as Website representative, whose name will be notified to the Website Management Committee, as having responsibility for maintaining their respective web pages.
- Where there is a committee, the Chairman for the committee will designate one person (preferably part of the secretariat) as having responsibility for maintaining that committee's website. The name of the latter will be notified to the Website Management Committee. Each Chairman, in this case, will be responsible for the legal compliance, accuracy, timeliness and completeness of content in their web pages.
- Individual staff members and research team leaders are responsible for legal compliance, content of their materials and timeliness.
- Capitated bodies: Student societies/associations and clubs are an integral part of University life. Web pages affiliated to capitated bodies will be given access to the main website.
- However, if the pages are found not to be compliant with all other aspects of the University's web policy, the Website Management Committee will recommend their removal from the University website. Chairpersons of all student societies and clubs and student committees will be responsible for legal compliance and content.
- The E-learning is gaining momentum within undergraduate and postgraduate courses. In view of the pedagogic considerations of web based academic course material developed by PU academic staff, e-learning material may not be bound by University's technical and design requirements. In such circumstances, the e-Learning or academic staff are responsible for legal compliance, accuracy and completeness of their course

materials.

16.7 Website Design and Maintenance

Website for all Departments are approved by the Website Management Committee with Departments concerned contributing significantly to the design concepts for their website and being entirely responsible for their content

For purposes of branding, the design of web pages shall take the following form

PU HEADER (Section A)
NAVIGATION MENU (Section A)
SLIDER (Section B)
CONTENT (Section C)
FOOTER (Section D)

- Web pages of sections shall be designed and maintained centrally in consultation with the functional area concerned
- All web sites must use the above template as supplied by the University Website Management Committee.
- Departmental heads must ensure that University's target audiences are identified, acknowledged and their preference for relevant, understandable information is accommodated in their pages.
- All homepages will reinforce key University messages, which can be obtained in the University strategic plan.
- **A**ll the Departmental pages must display the following information on the first page:
    - The name of the department
    - Contact information
    - Copyrights should be included on the University website.

16.8 Website content management

Departmental heads are responsible for the management of their web pages.

It is required that obsolete information be removed and outdated information be updated on a regular basis.

16.9 Writing and Exporting Web Pages

- External companies/individuals writing web pages on behalf of University staff or Departments or students are not given direct access to the University server. Writing pages to the University server is the responsibility of the University Department on whose behalf these web pages are written. These pages must therefore conform to all policy, technical and design requirements of University web pages.
- All pages written for the University web should be readable on standard versions of browsers. For a stable website environment, the use of scripts, databases, processes, utilities or applications is limited. Approved languages include Hyper Text Markup Language (html), Extensible Hyper Text Markup Language (xhtml) and Cascading Style Sheets (CSS).

16.10 Navigation

- All web pages in a website must provide navigational links that appear and behave in a consistent fashion.
- All web pages must incorporate the template search tool as supplied by the University Website Management Committee.
- All web pages must include the following information when linking to information, resources or services that may require a plugin or separate application: file format, file size, and provide a link to the applet, plugin or application.
- All University Departments must ensure that their pages are listed in the University's Contact directory.

16.11 Accessibility

- All web pages must meet accepted world-class standards as detailed on World Wide Web Consortium's Web Content Accessibility Guidelines Version 2.0 found at http://www.w3.org/TR/WCAG20/
- Departmental heads are responsible for ensuring that requests for assistance in accessing information within their areas are expedited

16.12 Advertising

The University’s Webpages must not be used for commercial, non-mission-related purposes.

16.13 Registration of Web Servers

All PU web servers must be registered with the PU Website

Management Committee.

16.14 Applicability and Exceptions

This policy is generally applicable to all websites hosted on the University' domain or directly associated with the PU website. If an individual or group feels that they are unable to meet the requirements of this policy for any reason, be it technical, legal, logistical, or other, they may choose to request either an exemption to the policy or a review in policy. Such requests should be sent to the Vice Chancellor.

17 INFORMATION SECURITY AND MANAGEMENT SYSTEMS POLICY

17.1 Definition of Terms

Information Security Management System (ISMS): a systematic approach to managing sensitive University information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.

Information Security Supporting Principles: a set of principles that the policy domains are described in section 17.5.2

17.2 Introduction

Pwani University is committed to managing information security in accordance with University policies and relevant laws and regulations.

17.3 Objectives of Policy

This policy outlines how Pwani University manages and mitigates security risks to safeguard the confidentiality, integrity and availability of University information and communication technology assets and environment.

17.4 Scope of Policy

This policy applies to the University as whole, employees (regardless of their mode of employment) of Pwani University and its controlled entities. This policy also applies to contractors, service providers and other members of the University's supply chain who are provided access to the University systems or data as required delivering contracted services.

17.5 Policy Statement

Pwani University is committed to the secure management of information and systems utilizing a policy framework based on the international standard for security management systems - ISO 27001. The University will manage information security risks and controls to the extent that there are clear financial benefits to the University.

17.5.1 Information security principles

Pwani University has adopted the following high-level Information security principles to establish a sound foundation for information security policies, procedures and practices. These principles are:

- Information, in whatever form, is of fundamental importance to the University and as such the University shall manage information security within a framework based on ISO 27001.

- Information security risks are managed, taking into account broader University objectives, strategies and priorities. A risk management approach is used to identify, evaluate and mitigate risks for the University's systems and information assets

- The requirements of the ISO 27001 Standard, and therefore this policy are based on the following three elements of information security:

    - Confidentiality: ensuring that information shall be accessible only to those authorized to have access
    - Integrity: safeguarding the accuracy and completeness of information and processing methods, and
    - Availability: ensuring that authorized users shall have access to information and associated assets when required.

Pwani University's management will actively support information security within the organizational culture through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities. This will ensure information security management is embedded in University activities and processes.

Continuity of operations will be heavily dependent upon the confidentiality, integrity and continued availability of information and the means by which it is gathered, stored and processed, communicated and reported.

17.5.2 Supporting policy domains

This policy has defined 15 policy domains aligned with ISO 27001:2013 as listed below. These domains are subject areas in which management controls are defined, applied and governed by one or more local ICT department documents and are contained in the Information Security Management System (ISMS). The following table describes these domains.

Domain	**Summary**
Information Security Management System (ISMS)	The ISMS provides the framework of principles, policies, standards and guidelines for the effective management of IT Security Risk.
Access controls	Methods and controls to manage logical access to sensitive data to protect confidentiality of information as well as integrity and availability requirements. Access requirements are assessed against the Pwani University Information Systems Access Control Policy in Chapter

	11.0 of PU ICT handbook. Access to University information and systems must be: • attributable to a uniquely identifiable individual who is responsible for actions performed with their system account • based on the requirements of the individual's role • managed by passwords, according to Information and Communication Technology Passwords Procedure, formally authorized by asset owners, routinely revalidated and removed if no longer required
Communications Security	Methods and controls to manage the secure transmission of information to ensure confidentiality of sensitive data and to minimize the risk of data loss or leakage. Systems and networks will be segregated according to their respective information security risks and use appropriate control mechanisms such as firewalls/gateways, physical isolation and encryption.
Operations Security	Methods and controls that balance the need for IT Operations professionals to have privileged access to systems and networks with the requirement to maintain secure access and confidentiality of data. Management and operation of computers and networks shall be, commensurate with the business risk and value of the information assets. Access into networks will be granted on an individual user and application basis using authorized devices and secured pathways.
Physical and Environmental Security	Appropriate physical controls shall protect information assets against loss, physical abuse, unauthorized access and environmental hazards. These will include perimeter security controls, physical access controls, intruder detection controls, fire, and flood and power protection controls.
Supplier Relationships	The University will implement security controls and processes to manage supplier access to information assets. Suppliers and vendors will be given access privilege only at the level required to deliver contracted

	services and contracts must comply with information security policies.
Systems Acquisition and Secure Development	Information security controls will be specified and included as an integral part of the software development and implementation process. Security requirements will be identified prior to the development or procurement of IT systems, documented in business requirements, validated and tested prior to implementation, and regularly throughout the systems lifecycle.
Cryptography	Methods and controls for ensuring data will be secured during transmission, or storage through appropriate encryption processes. Includes methods and processes for managing keys, software and other artefacts.
Incident Management	The University will apply a consistent and effective approach to the management of information security incidents. Procedures that define the course of action when a security incident is identified will be documented and made available to all employees.
Business Continuity	The application of business continuity management shall minimize disruption to PU operations, defining the approach to resilience, disaster recovery and general contingency controls. Continuity plans shall align with the University's Business Continuity Management Framework.
Human Resources	The University will establish processes and responsibilities relating to information security during the recruitment process, employment and separation. Security checks will be conducted prior to employment and all employees will receive security awareness training upon induction, and at least annually thereafter.
Project Management	Project proposals must include a high-level risk assessment and review of the types and confidentiality levels of information the project will utilize and manage. New systems will be reviewed by the Information Security Officer prior to implementation via the change management process.

Asset Management	IT assets, including hardware, software and data shall be identified and classified and asset inventories shall be maintained. The University will dispose of public records in accordance with the University's Retention and Disposal Schedules, as recommended in PU Back up retention policy.
Data Assurance	The University will ensure that all reasonable steps are taken to monitor, review and audit information security effectiveness. This will include the assignment of security roles, maintenance of policies and processes and reporting of non-compliance.
Data Breach Reporting	The University has formal processes in place to manage a data breach and the mandatory notifications that are required under Information Systems Incidence Management Policy (Chapter 13)

18. EMPLOYEE PRIVACY POLICY

The privacy and security of the personal data collected from staff is a priority to Pwani University. PU is committed to respecting the privacy of all its employees and of the personal information collected in order to carry out its purposes, functions and activities

18.1 Definitions

Personal information is information or an opinion (whether recorded in a material form or not) about an individual whose identity is apparent or can reasonably be ascertained, from the information or opinion.

Sensitive information is a special category of personal information. It is information or an opinion about an individual's:

- Racial or ethnic origin
- Religious beliefs or affiliations
- Philosophical beliefs
- Membership of a professional or trade association
- Membership of a trade union
- Sexual preferences or practices

Sensitive information also includes health information about an individual; or genetic information about an individual that is not otherwise health information.

18.2 Introduction

In this Policy, collection, access, use and protection of employee data is described.

18.3 Policy Objectives

This policy sets out Pwani University commitment to respecting privacy and how that commitment is to be carried out

18.4 Policy Statements

18.4.1 Collection of Personal/Sensitive Information

PU will only collect personal/sensitive information that is necessary and incidental to the University's purposes, functions and activities. PU will collect personal information about an individual only by lawful and fair means and not in an unreasonably intrusive manner. So far as it is reasonably practicable to do so, information collected will be directly from the individual concerned or members of their immediate family. PU will take reasonable steps to ensure that an individual is aware of the purposes for which the information is collected.

PU will not collect sensitive information without the employees' consent unl the collection of such information is required under law. PU collects personal information from/about past, current and prospective employees (including casuals), students, parents/guardians of students, benefactors and external contractors. Personal information that PU collects includes:

- Names
- Identification Numbers
- Addresses
- Email Addresses
- Telephone Numbers
- Emergency Contacts
- Photographic Identification
- Medical Information
- Personnel administrative information, such as education and qualifications, courses, competence profile, job responsibilities
- Salaries and pensions, information relevant to payroll
- Bank details.
- Tax information
- And any other information that may be relevant to the Human Resource

18.4.2 Use and Disclosure of Personal Information

Use of Personal/Sensitive Information

The primary purpose of collecting personal information is to enable PU to carry out its purposes, functions and activities. PU will not disclose personal information to third parties without the consent of the individual, except where the disclosure is required under law or for any other authorized reason.

Access to Personal Information

PU will provide access to personal information under:

- Legislative Obligations
- Individual Consent Arrangements
- Request by the individual to access their own file (to the extent allowed under the NPPs)
- PU staff will only be provided with access to personal information where it is a necessary function of their role.

No Consent Provided

PU will only collect information without the consent of the individual or their parent/guardian where it is impracticable to gain such consent.

Removal of Information

PU will take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorized access, modification or disclosure.

PU will take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information was provided. All reasonable steps will be taken to destroy or permanently de-identity personal information if it is no longer needed for any purpose.

18.4.3 Staff Obligations

If a staff member collects, uses, discloses or handles personal information on the University's behalf, the staff member must only collect, handle, use, disclose and store the information for the agreed purposes only. It is expected that any such information or documents shall be regarded as confidential and shall remain the property of the University at all times. Therefore, such information or documents shall not be copied, transmitted, disclosed or communicated to any person or external entity not authorized to access such documents or information.

18.5 Privacy Complaints Handling Procedure

If an individual considers that there has been a breach of this policy, a written complaint must be forwarded to the Deputy Vice Chancellor, Administration, Finance & Planning (DVC AFP). The complaint must specify details of the apparent breach in writing.

The DVC AFP will undertake to investigate the alleged breach and make a determination on a complaint after receipt of the complaint. The complainant will be advised of the outcome in writing. If the DVC AFP determines that there has been a breach of the policy he or she will advise the relevant PU employees, who are directly involved, of the outcome including any action required in order to remedy the breach. PU will endeavor to assure confidentiality in relation to all complaints and matters will only be discussed with relevant staff members who are involved in the complaint.

19 USE OF COMPUTER FACILITIES POLICY

19.1 Introduction

The computing facilities at Pwani University are provided for use by students, faculty and staff. All computer users are responsible for using the facilities in an effective, efficient, ethical, and lawful manner.

The computing facilities are for the purpose of advancing the academic goals of learning, teaching, research, innovation and community outreach and for assisting in administrative operations which support these goals. It is the responsibility of all users to ensure that they are not wasting the resources, interfering with the work of others or breaching applicable policies and legislation.

19.2 Definition of terms

Computing facilities are any computer, computer based network, computer peripheral, operating system, software or any combination thereof, owned by the University or under the custody or control of the University. Equipment and software purchased from research funds administered by the University are owned by the University unless otherwise specified in the research grant or contract.

Misuse of computing facilities: Theft of computer time, abuse of computer access, unauthorized use of computing facilities and any other violation of Pwani University ICT policies and guidelines.

19.3 Policy Objective

This policy describes appropriate use of computing facilities. It also clarifies what constitutes misuse of computing facilities at Pwani University and related consequences.

19.4 Policy Statement

19.4.1 Acceptable Use of computing facilities

- Use of computing facilities for regular University duties and assignments.
- Use of computing facilities for their intended purposes.
- Authorized use of computing facilities.
- Use of computing facilities in a way that enhances performance of duties, care for and protection of computers and networks, and sensitivity to the rights of other parties.
- Reasonable use of computing facilities characterized by among others: installation of authorized software, consultation with authorized staff while reconfiguring devices, and seeking advice and support from authorized ICT officers while in doubt about the right thing to do.

- Adhering to user manuals and maintenance schedules for computing facilities.
- Adhering to policies and guidelines related to use of computing facilities.

19.4.2 Misuse of computing facilities

Misuse of computing facilities refers **to** theft of computer time, abuse of computer access, unauthorized use of computing facilities and any other violation of Pwani University ICT policies and guidelines.

Examples of misuse include, but are not limited to, the activities in the following list.

- using the campus network to gain unauthorized access to any computer system;
- knowingly or carelessly performing an act that will interfere with the normal operation of computers, terminals, peripherals, or networks;
- knowingly or carelessly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network. This includes, but is not limited to, programs known as computer viruses, Trojan Horses, and worms as well as programs that utilize a disproportionate amount of available network bandwidth.
- attempting to circumvent data protection schemes or uncover security loopholes. This includes creating and/or running programs that are designed to identify security loopholes and/or intentionally decrypting secure data; this also includes programs contained within an account or under the ownership of an account that are designed or associated with security cracking.
- deliberately wasting/overloading computing resources; this includes, but is not limited to, printing multiple copies of a document or printing out large documents that may be available online that could significantly impact other users' printing resources.
- sending unsolicited email messages to more than 15 individual recipients; if legitimate messages need to be sent to large groups of people such as classes, clubs, or other administrative groups, then distribution lists must be properly requested and utilized.
- Moving large files across networks during peak usage periods or prime hours such that it degrades resource performance, prime hours will be considered to be Monday through Friday from 8 am to 5 pm.

- storing large files on the systems that could compromise system integrity or preclude other users’ right of access to disk storage; systems administration staff may remove or compress disk files that are consuming large amounts of disk space, with or without prior notification.
- using an account for any activity that is commercial in nature, i.e., paid for by non-University funds; commercial activities include, but are not limited to, consulting, typing services, and developing software for sale.
- posting on electronic bulletin boards materials that violate existing laws or the University's codes of conduct.
- displaying sexually explicit, graphically disturbing, or sexually harassing images or text in a public computer facility, or location that can potentially be in view of other individuals.
- attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner; files owned by individual users are to be considered private property, whether or not they are accessible by other users.
- installing unauthorized devices to the campus network without prior approval; this includes, but is not limited to, the installation of network server computers (machines configured to provide file/print sharing services, DHCP services, DNS services, WINS services, web page services, etc.), network appliances, network workstations, miscellaneous internet protocol devices.
- Activities will not be considered misuse when authorized in writing by appropriate University officials for academic or administrative purposes.

19.5 Violations

Violations of this policy will be dealt with in the same manner as violations of other University policies and may result in disciplinary review. In such a review, the full range of disciplinary sanctions is applicable including the loss of computer use privileges. PU employees are responsible for understanding and observing the provisions of this policy.

20. STATEMENT OF ENFORCEMENT OF POLICIES

a) The ICT Manager, in liaison with the University Management, shall be responsible for enforcing these policies and where necessary shall take appropriate remedial measures.
b) The ICT Manager shall monitor the implementation of this policy.
c) Violation of policies in this handbook shall be addressed by appropriate University and national legal mechanisms

Consequences of Breach

Breach of this handbook shall be dealt with in accordance with the Pwani University Code of Conduct for Staff, Pwani University Code of Conduct for Students and other relevant University, National laws and policies, which may lead to disciplinary action or other relevant sanctions.

Appendix 1: System Access Request Form

PU/ICT/FORM/ICT/09 01/00

Pwani UNIVERSITY

SYSTEM ACCESS REQUEST FORM

Date: _____________

USERS DETAILS

Access required to System/Application

New User □ Existing User □ Deletion of User

Surname: ____ Other Names: ____

PF No. /ID No……………………. Job Title: ____

Department/School: ____

Extension/Mobile phone number: ______________________ Email: ________________________________

Access required to function (s): ____

____

_____

I acknowledge that:

a) My Password will at all times remain confidential to me

b) I will take all necessary precautions to ensure that no unauthorized persons can gain access to my password

Failure to adhere to the above mentioned or carelessness on my part leading to my password being used to gain an authorized entry to the above system will be viewed as a serious breach of trust and will result in severe disciplinary action.

Signature _______________________________

AUTHORIZING MANAGER/ HEAD

I confirm that the request required is in accordance with the user

Names____ Date_______________________________

Signature____________________________________

DVC AFP/ DVC ASA

Signature: ____________________________________ Date____

Authorizing Manager/Head

Names____________________________________ Date____

Signature____________________________________

Appendix 2: Standard of Procedures for Creation, Modification and Deletion of User Accounts

Pwani UNIVERSITY

STANDARD OPERATING PROCEDURE FOR CREATION, MODIFICATION AND DELETION OF USER ACCOUNTS

SOP No.	Prepared by	Reviewed	Approved by
PU/ICT/SOP/04	ICT Committee	Management Board	Chair of Council

Introduction

The purpose of this procedure is to guide the university on the standards to be implemented when creating, modifying and deleting of user accounts. This is critical in protection of sensitive data and minimizing risks of unauthorized access to university systems.

Scope

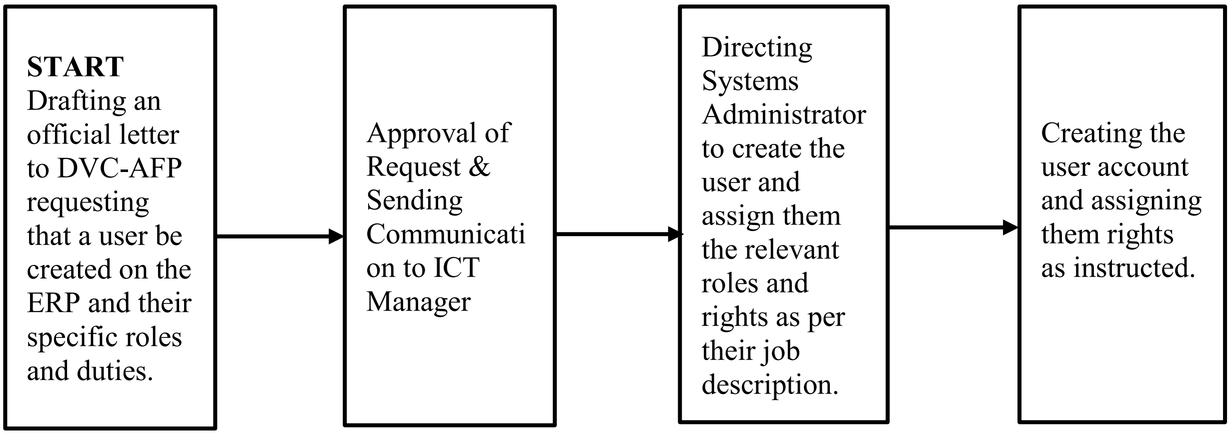
The procedure applies only to user accounts within Pwani University domain

1.0 Creation of User Accounts

1.1 Procedures and responsibilities

Procedure	Responsibility	Timeline
Drafting an official letter to DVC-AFP requesting that a user be created on the ERP and their specific roles and duties.	Head of Department	2 Hours
Approval of Request & Sending Communication to ICT Manager	Deputy Vice Chancellor-Administration Finance & Planning	1 Day
Directing Systems Administrator to create the user and assign them the relevant roles and rights as per their job description.	ICT Manager	15 Minutes
Creating the user account and assigning them rights as instructed.	Systems Administrator	30 Minutes

1.2 Process Map: Creation of User Accounts



START Drafting an official letter to DVC-AFP requesting that a user be created on the ERP and their specific roles and duties.

Approval of Request & Sending Communication to ICT Manager

Directing Systems Administrator to create the user and assign them the relevant roles and rights as per their job description.

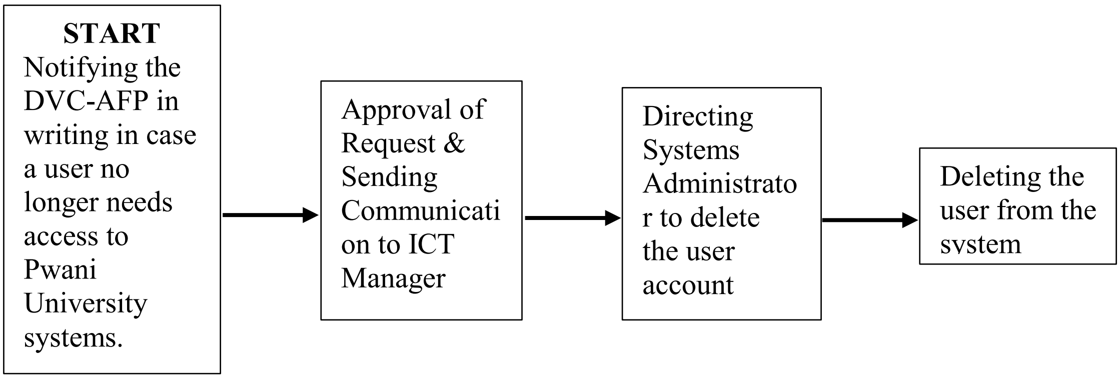
Creating the user account and assigning them rights as instructed.

2.0 Deletion of User Accounts

2.1 Procedures and responsibilities

Procedure	Responsibility	Timeline
Notifying the DVC-AFP in writing in case a user no longer needs access to Pwani University systems.	Head of Department	1 Day
Approval of Request & Sending Communication to ICT Manager	Deputy Vice Chancellor-Administration Finance & Planning	1 Day
Directing Systems Administrator to delete the user account	ICT Manager	30 Minutes
Deleting the user from the system	Systems Administrator	30 Minutes

2.2 Process Map: Deletion of User Accounts

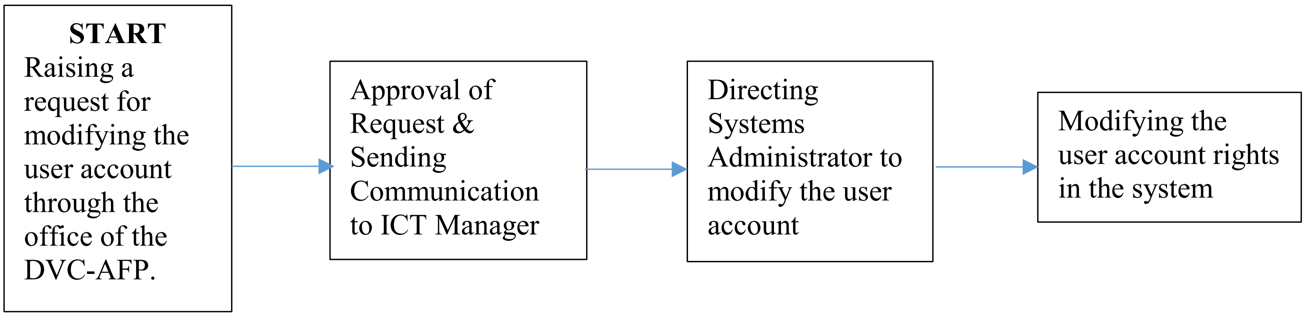

START
Notifying the DVC-AFP in writing in case a user no longer needs access to Pwani University systems.
Approval of Request & Sending Communication to ICT Manager
Directing Systems Administrator to delete the user account
Deleting the user from the system

3.0 Modification of User Accounts

3.1 Procedures and responsibilities

Procedure	Responsibility	Timeline
Raising a request for modifying the user account through the office of the DVC-AFP.	Head of Department	1 Day
Approval of Request & Sending Communication to ICT Manager	Deputy Vice Chancellor-Administration Finance & Planning	1 Day
Directing Systems Administrator to modify the user account	ICT Manager	30 Minutes
Modifying the user account rights in the system	Systems Administrator	30 Minutes

3.2 Process Map: Modification of User Accounts


START
Raising a request for modifying the user account through the office of the DVC-AFP.
Approval of Request & Sending Communication to ICT Manager
Directing Systems Administrator to modify the user account
Modifying the user account rights in the system

Appendix 3: Standard of Procedures for E-Records Management

	STANDARD OPERATING PROCEDURE FOR E-RECORDS MANAGEMENT			
	SOP No.	Prepared by	Reviewed	Approved by
	PU/ICT/SOP/02	ICT Committee	Management Board	Chair of Senate

1.0 Introduction

The purpose of this procedure is to guide employees and supervisors on the standards to be implemented when managing e-records

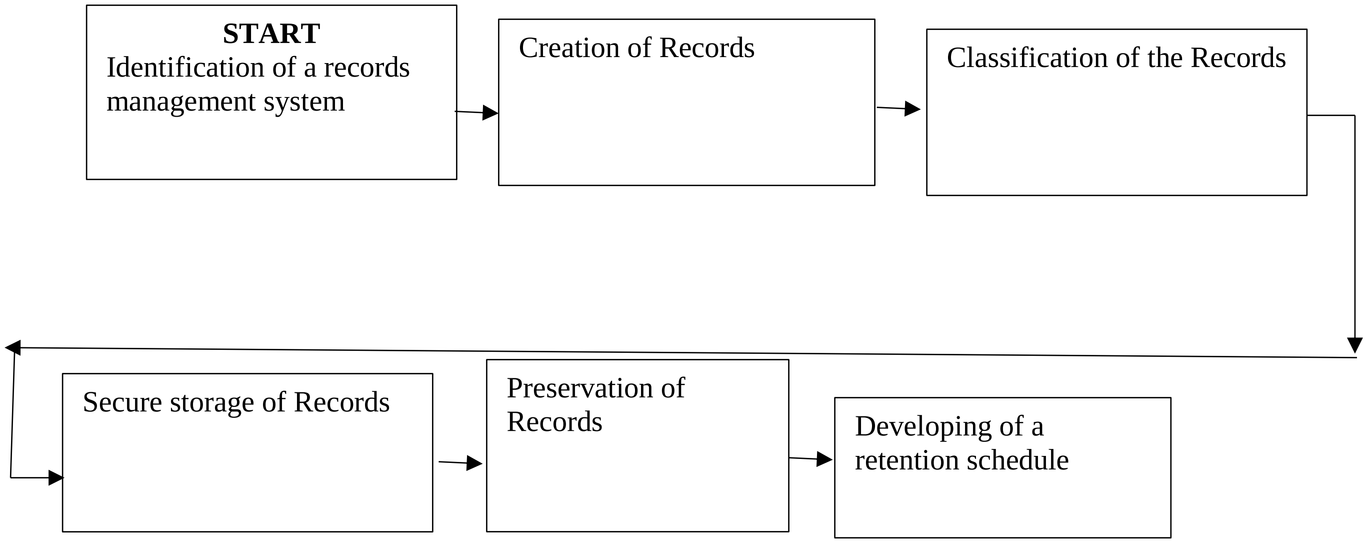
2.0 Scope

The procedure applies only to e-records management

3.0 Procedures and responsibilities

Procedure	**Responsibility**	**Timelines**
Adoption of a records management system	Head of Section	1 Hour
Creation of Records	Administrative Assistant/Secretary	1 Hour
Classification of the Records	Administrative Assistant/Secretary	1 Hour
Secure storage of Records	Administrative Assistant /Secretary	2 Hours
Preservation of Records	Administrative Assistant /Secretary	2 Hours
Developing a Retention Schedule	Administrative Assistant /Secretary	2 Hours

4.0 Process Map


START
Identification of a records management system
Creation of Records
Classification of the Records
Secure storage of Records
Preservation of Records
Developing of a retention schedule

Appendix 4: Standard Operating Procedure for Information Systems Incident Management

Pwani UNIVERSITY	**STANDARD OPERATING PROCEDURE FOR INFORMATION SYSTEMS INCIDENT MANAGEMENT**			
	SOP No.	**Prepared by**	**Reviewed**	**Approved by**
	PU/ICT/SOP/06	ICT Committee	Management Board	Chair of Council

1.0 Introduction

The purpose of this procedure is to guide employees and supervisors on the standards to be implemented on Information Systems Incident Management.

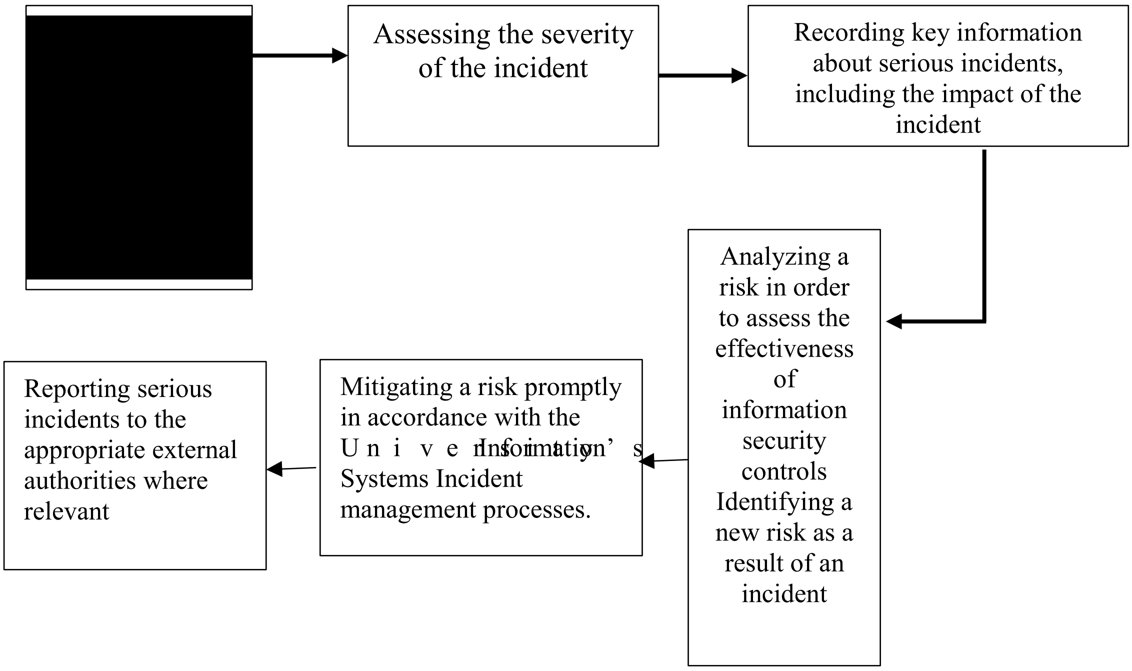
2.0 Scope

The procedure applies only to Information Systems Incident Management

2.2 Procedure and responsibilities

Procedure	**Responsibility**	**Timeline**
Reporting promptly to the IT Service Desk on occurrence of an incident	PU staff	30 Minutes
Assessing the severity of the incident	Systems Administrator/ICT Technicians	Varies
Recording key information about serious incidents, including the impact of the incident	Systems Administrator/ ICT Technicians	30 Minutes
Analyzing a risk in order to assess the effectiveness of information security controls Identifying a new risk as a result of an incident	Systems Administrator/ ICT Technicians	1 Day
Mitigating a risk promptly in accordance with the Universi management processes.	Systems Administrator / ICT Technicians	Varies
Reporting serious incidents to the appropriate external authorities where relevant	Authorized Individuals	2 Hours

2.3 Process Map


[redacted]
Assessing the severity of the incident
Recording key information about serious incidents, including the impact of the incident
Analyzing a risk in order to assess the effectiveness of information security controls Identifying a new risk as a result of an incident
Mitigating a risk promptly in accordance with the University's Information Systems Incident management processes.
Reporting serious incidents to the appropriate external authorities where relevant

Appendix 5: Retention of Back up Timeline

Records	**Retention Period**
Accounting Records (e.g. Purchase orders, invoices	Current financial year plus six years
Payroll Records	Current financial year plus six years
Insurance Records	Current financial year plus six years
Financial Statements	Retained indefinitely
Approved budgets	Retained indefinitely
Accounts payable vouchers	6 years
Claim / imprest	10 years
Fee schedules	5 years
Income tax returns	Retained indefinitely
Banking records like deposits & withdrawals, bank statement	5 years
Grants from Central and County Government	6 years
Sales	2 years after the date of last entry
Student Medical records	6 years post-graduation
Daily transaction of Medical records	6 years
Procurement Data	6 years
Students (Admission, Registration, Enrollment and Withdrawal)	2+ years after graduation

Appendix 6 Standard Operating Procedure for Back-Up Retention

	STANDARD OPERATING PROCEDURE FOR BACK-UP RETENTION			
Pwani UNIVERSITY	**SOP No.**	**Prepared by**	**Reviewed**	**Approved by**
	PU/ICT/SOP/03	ICT Committee	Management Board	Chair of Council

1.0 Introduction

The purpose of this procedure is to guide employees on the standards to be implemented when retaining backups.

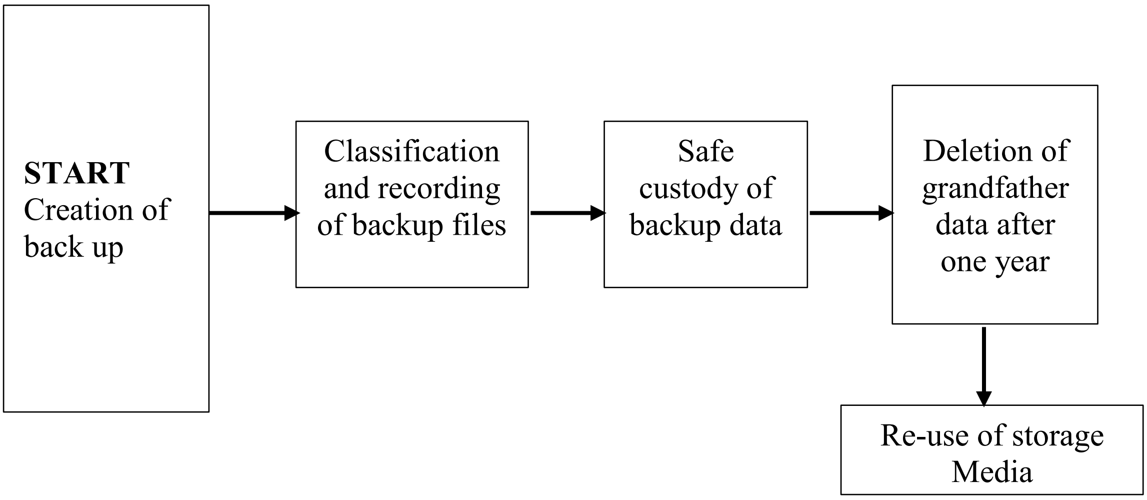
2.0 Scope

The procedure applies only to retention of backups.

3.0 Procedures and responsibilities

Procedure	**Responsibility**	**Timeline**
Creation of back up	Systems Administrator	24 Hours
Classification and recording of backup files	Systems Administrator	24 Hours
Safe custody of backup data	Systems Administrator	24 Hours
Deletion of grandfather data after one year	Systems Administrator	12 Months
Re-use of storage Media	Systems Administrator	12 Months

4.0 Process Map


START
Creation of back up
Classification and recording of backup files
Safe custody of backup data
Deletion of grandfather data after one year
Re-use of storage Media

Appendix 7 ICT Service Charter

Information and Communication Technology Department

SERVICE CHARTER

NO	SERVICE	REQUIREMENT	CHARGE (KSHS)	TIME LINE
1.	General User Support	Receipt of a filled online service request ticket	Free	Between 10 to 60 minutes
2.	Corporate E-mail Address	Receipt of a filled E-mail request form	Free	10 minutes
3.	Password Reset	Receipt of a filled Password request form	Free	5 minutes
4.	Multimedia (video, camera and public address system)	Receipt of a filled Multimedia request form	Free	2 working days on receipt of approval
5.	Graphics design	Receipt of a filled Graphic design request form	Free	2 working days on receipt of approval
6.	Networking Support	Receipt of a filled online service request ticket for network support	Free	Between 10 to 60 minutes
7.	Navision User Support	Receipt of a filled online service request ticket for Navision support	Free	Between 10 to 60 minutes
8.	Staff portal support	Receipt of a filled online service request ticket for staff portal support	Free	10 minutes
9.	Students portal support	Upon request	Free	5 minutes
10.	Wifi settings	Upon request	Free	5 minutes