Ahmadu Bello University ICT Policy

November 2023

Published and Printed by:
Ahmadu Bello University Press Limited, Zaria,
Kaduna State, Nigeria.
Tel.: 08065949711.
E-mail:abupress2020@yahoo.com
abupress2013@gmail.com
Website: www.abupress.com.ng

Foreword

Our Journey towards the adaptation of Information and Communication Technology in Ahmadu Bello University is as old as the beginning of the use of computer in Nigeria when the first computer was acquired in the late 1960s. So far, the University that attained some level of maturity in the stock pile of her ICT infrastructure and services. It is therefore apparent that an ICT policy is needed to be a guide in the quest of the University for attaining a Centre of Excellence in teaching/learning and search.

I am pleased to introduce the University's new ICT Policy, which has been developed to guide our academic and administrative activities in the digital age. The policy is aimed at providing a comprehensive framework for the use of ICT resources, including hardware, software and networks to enhance teaching, learning, research and administrative operations at the University.

As we strive to become a world-class institution, it is essential that we leverage the power of technology to improve our academic and administrative processes. With the implementation of this new ICT policy, we will be better equipped to address the challenges of the 21st century, including the need for enhanced collaboration, access to information and online learning opportunities.

The policy outlines the University's expectation for the appropriate use of ICT resources, including guidelines for responsible and ethical behavior online. It also establishes protocols for the management of ICT resources, including security and data privacy measures, disaster recovery and business continuity planning.

I urge all members of the University community to familiarize themselves with the ICT Policy and to take an active role in its implementation. As we work together to create a dynamic and innovative learning environment, the proper use of technology will be essential to our success

Thank you for your cooperation and support.

Sincerely,

Professor Kabiru Bala
Vice Chancellor

Table of Contents

1 Introduction 1
1.1 Policy Statement 1
1.2 Broad Policy Objectives 2
1.3 Scope of the University ICT 3
2 University Data Communications, Network Development and Management Policy 3
2.1 Introduction 3
2.2 Specific Policy Objectives 4
2.3 Policy Scope 4
2.4 Policy Statements 5
2.4.1 University ICT Infrastructure Development 5
2.4.2 University Data Centre 5
2.4.3 University Backbone (Network Core) 6
2.4.4 Campus Local Area Networks (LANs) 7
2.4.5 Distribution Network 7
2.4.6 Wireless Networks 8
2.4.7 Virtual Private Networks (VPN) 8
2.4.8 Network Equipment Installation and Access to Data Centre 10
2.4.9 Connection to and Usage of the University Network 11
2.4.10 Additional or Changed Equipment 12
3 Bandwidth Purchase and Usage 13
3.1 Introduction 13
3.2 Policy Objectives 13
3.3 Policy Scope 13
3.4 Policy Statements 13
3.4.1 Bandwidth Procurement 13
3.4.2 Bandwidth Management and Utilization 13
3.4.3 Pooling of Internet Bandwidth Acquired by Units 14
4 Cyber Security Policy 15
4.1 Introduction 15
4.2 Policy Objectives 15
4.3 Policy Scope 15
4.4 Policy Statements 15
4.4.1 General Use and Ownership Policy 15
4.4.2 Conditions of Use of Computing and Network Facilities 19
4.4.3 Bring Your Own Device 21
4.4.4 Password Policy 21
5 Systems Backup and Recovery Policy 22
5.1 Introduction 22
5.2 Policy Objectives 22
5.3 Policy Scope 23
5.4 Policy Statement 23

6 Computer Laboratory & Digital Centre 23
6.1 Introduction 23
6.2 Policy Objectives 24
6.3 Policy Scope 24
6.4 Policy Statements 24
7 Software Development, Acquisition, Support and use 25
7.1 Introduction 25
7.2 Policy Objectives 25
7.3 Policy Scope 25
7.4 Policy Statements 25
8 User Support Services 26
8.1 Introduction 26
8.2 Policy Objectives 26
8.3 Policy Scope 26
8.4 Policy Statements 27
9 ICT Equipment and Systems Maintenance 28
9.1 Introduction 28
9.2 Policy Objectives 28
9.3 Policy Scope 28
9.4 Policy Statements 28
10 Email Account Use Policy 28
10.1 Introduction 28
10.2 Policy Objective 29
10.3 Policy Scope 29
10.4 Policy Statements 29
11 ICT Skills Capacity Building and Training 30
11.1 Introduction 30
11.2 Policy Objectives 30
11.3 Policy Scope 30
11.4 Policy Statements 30
12 Information Systems Administration 32
12.1 Introduction 32
12.2 Policy Objectives 32
12.3 Policy Scope 33
12.4 Policy Statements 33
12.4.1 Services 33
12.4.2 Service Level Agreements (SLAs) 35
13 Systems Administration 36
13.1 Introduction 36
13.2 Policy Objectives 36
13.3 Policy Scope 36
13.4 Policy Statements 36
13.4.1 Responsibilities to the University 36

13.4.2 Copyrights and Licenses 37
13.4.3 Modification or Removal of Equipment 37
13.4.4 Data Backup Services 37
13.4.5 Misuse and Security Breach 38
13.4.6 System Integrity 38
13.4.7 Account Integrity 38
14 ICT Procurement and Decommissioning 39
14.1 Introduction 39
14.2 Policy Objectives 39
14.3 Policy Scope 39
14.4 Policy Statements 39
14.4.1 Procurement of ICT Equipment 39
14.4.2 Decommissioning 40
15 Social Media 40
15.1 Introduction 40
15.2 Policy Objectives 41
15.3 Policy Scope 41
15.4 Policy Statements 41
15.4.1 University Official Social Media Sites 41
15.4.2 Staff Social Media Activity 42
15.4.3 Students Social Media Activity 42
16 E-Learning Tools Use 43
16.1 Introduction 43
16.2 Policy Objectives 43
16.3 Policy Scope 43
16.4 Policy Statements 43
17 Website use and Update 44
17.1 Introduction 44
17.2 Policy Objective 44
17.3 Policy Scope 44
17.4 Policy Statements 45
18 Information Systems Use 45
18.1 Introduction 45
18.2 Policy Objectives 45
18.3 Policy Scope 46
18.4 Policy Statements 46
19 References 47

1 Introduction

Ahmadu Bello University Zaria University is one of the first generation universities in Nigeria saddled with the responsibility of developing high-level human power in various disciplines. The University has continued to invested substantially in Information and Communication Technology (ICT) to support the emergence and sustenance of competitive world-class teaching, learning and research environment, and to break new grounds in the dissemination of knowledge and information of the highest quality. Iya Abubakar Institute of Information and Communication Technology (IAIICT), which is the ICT hub of the University, is mandated to drive the Policy. The Institute is to, amongst others, empower the University by building its capacity to take a pride position as one of the best ICT-driven universities in Africa and the world.

The University ICT Policy provides a structure and clear guidelines for handling all the relevant ICT activities to support the achievement of the ICT Vision. Broadly, the Policy spells out best practice, defines the roles and responsibilities of all user groups as well as provides guidance in the delivery, implementation, and usage of ICT. This Policy shall serve, alongside other related published documents, as the reference document on the University ICT standards. The Policy shall be reviewed, as the need arises, to ensure it remains relevant and aligned to the goals of the University.

1.1 Policy Statement

This Policy describes and documents the acceptable guidelines that support the University's goals and objectives on teaching, learning, research, and support services. These are general guidelines on what can be done, and what should not be done, on the University ICT Infrastructure in order to ensure efficient and effective use of University ICT resources; protect ICT resources from injurious actions, including virus attacks, data loss, unauthorized access, network and system failures, and legal problems. This policy seeks to guide designers, developers and users of information and ICT resources on what standards are appropriate and acceptable to the University.

1.2 Broad Policy Objectives

The broad objectives of the Policy are to:

i. Guide in developing a pervasive, reliable and secure c*ommunications infrastructure* conforming to recognized international standards that support all services in line with the priorities of the University;
ii. Provide a framework for development and management of ICT *network services* that shall ensure the availability, reliability, enhanced performance, security, and reduction in the cost of running the ICT infrastructure;
iii. Establish information requirements and implement *security* across the University's ICT infrastructure;
iv. Provide a framework, including guidelines, principles and procedures for the development and implementation of *Management Information Systems* in the University;
v. Guide the handling of *organizational information* within 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;
vi. Uphold the integrity and image of the University through defined standards and guidelines for ensuring that the content of the University's *website* is accurate, consistent and up-to-date;
vii. Serve as the direction pointer for IAIICT's mandate in supporting users, empowering them towards making maximum use of ICT services and resources and specifying the necessary approaches;
viii. Guide the process of enhancing user utilization of ICT resources through training;
ix. Outline the rules and guidelines that ensure users' PCs and other hardware are in serviceable order, specifying best practices and approaches for preventing failure;
x. Provide a paradigm for establishing the University's database service that will support groups working on systems development, production and any other groups;
xi. Inform departments carrying out projects financed in whole or in part by the University, of the arrangements to be made in procuring ICT goods and services for the projects.

1.3 Scope of the University ICT

People to Whom Policy Applies

This Policy applies to any person who accesses University ICT resources, whether affiliated with the University or not, whether on campus or from remote locations, including but not limited to students, staff, contractors, consultants, temporary employees, guests, and volunteers. By accessing University Information Technology Resources, the user agrees to comply with this Policy.

Definition of ICT Resources

ICT resources for the purposes of this Policy include, but are not limited to, University-owned optic fiber that connects campuses across Zaria, distribution and access networks, wireless networks, servers, exchanges, internet connections, terminals, applications, and personal computers. ICT resources include those owned by the University and those used by the University under license or contract, including but not limited to information recorded on all types of electronic media, computer hardware and software, paper, computer networks, and telephone systems. ICT resources also include, but are not limited to, personal computers, servers, wireless networks and other devices not owned by the University but intentionally connected to the University-owned ICT resources while so connected.

Other resources are software that comprise operating systems, which includes device drivers and add-ons, application software developed within the University or acquired from third-party vendors or obtained from open-source outlets and data generated from staff and students' information, academic records, comprising of students' registration and examination records as well as alumni records, inventory of physical assets, etc.

2 University Data Communications, Network Development and Management Policy

2.1 Introduction

The ICT infrastructure at the University has evolved into a large, complex network over which the education, research and business of the University are conducted. It is envisaged that the network will integrate voice, data and video, to

form a unified information technology resource for the University Community. Such a network shall demand adherence to a centralized, coordinated strategy for planning, implementation, operation and support. Decentralization shall be implemented through appropriate University structures.

The Enterprise network shall comprise the Core (backbone), Distribution and Access Layers. The Core and Distribution shall be based on single-mode optic fiber while the Access shall be based on CAT6 (or any better technology). Where necessary, wireless networks should be incorporated into any of the Core, Distribution or Access. University data communications and network shall be broken down into the following areas:

i. University ICT Infrastructure Development
ii. University Data Centre
iii. University Backbone (Core)
iv. The Distribution Network
v. The Access Layer
vi. Wireless Networks
vii. Virtual Private Networks (VPN)
viii. Connection to, access and usage of ICT facilities
ix. New or changed use of ICT equipment
x. Monitoring of network performance

2.2 Specific Policy Objectives

The objective of this policy is to establish a comprehensive and uniform Network Development and Management policy as a guide for the installation, expansion, maintenance and administration of the University ICT infrastructure.

This Policy defines the arrangements and responsibilities for the development, installation, maintenance, use and monitoring of the University's network infrastructure to ensure adequacy, reliability, security and resilience to support high levels of activities.

2.3 Policy Scope

This Policy applies to any person accessing or using the ICT infrastructure owned, managed, supported or operated by, or on behalf of the University. These include all University staff and students; any organization accessing services over

University networks; persons contracted to repair or maintain the University's ICT networks; and suppliers of network services.

2.4 Policy Statements

2.4.1 University ICT Infrastructure Development

Network Development plan

A five-year network development rolling plan is to be prepared regularly by the IAIICT, advising on appropriate developments aimed at ensuring the adequacy of the University's ICT infrastructure in the future. The plan should take into account but not limited to:

i. the University's Strategic Plan;
ii. the ever-changing University computing needs, growth in demand usage of the backbone; technological advances that introduce smarter and innovative methodologies;
iii. economic and budgetary constraints.

ICT Network Provision in New and Refurbished Buildings

i. Network provision for new and unserved buildings shall be made in accordance with the specifications published from time-to-time by IAIICT.
ii. All new buildings to be erected in the University shall incorporate an appropriate structured cabling system to allow connection to the University network.
iii. Network Design for all new and unserved buildings shall be performed or vetted by the IAIICT prior to implementation.
iv. Network devices and or services procurement shall equally be vetted by IAIICT to ensure strict compliance with design and security considerations

2.4.2 University Data Centre

i. The University shall maintain a Data Centre to act as the ONLY central repository for all University databases and web/content/resource hosting;
ii. In cases where there are constraints in hosting an application in the Data Centre, consultations and subsequent recommendations by the Director IAIICT shall be sought to allow for alternative solutions.

iii. The Data Center shall operate on a 24/7 basis as much as possible. Where downtime is inevitable, adequate arrangements must be put in place for the University Continuity.
iv. The Data Centre shall have a robust security infrastructure required to protect the systems, software, applications and data;
v. The Data Centre shall have standard security devices like firewall, intrusion detection system, intrusion prevention systems, fire prevention, disaster resistant backup capacity, remote monitoring and management, etc.;
vi. There shall be a Data Centre replication point at Site II which must be up-to-date at all times;
vii. Any network or computing device not procured directly by the University but is approved to be installed in the University Data Centre or anywhere on the University network shall become the property of the University; except third party donor project items where the agreed terms and conditions dictate otherwise.

2.4.3 University Backbone (Network Core)

The University shall provide a resilient, secured and stable fast data communications network as an enabler to the processing, storage, dissemination and accessing of information or ICT-enabled services as it relates to the various teaching, learning, administration and research needs of the University.

The University Network Backbone shall form the hub of the Campus-wide network comprising of an inter-building cabling system, together with one or more intermediate distribution "Gateway" interfaces at each building or in the path to each building which will connect the Backbone to the network(s) within each building. The network backbone shall obey the following:

i. The University Network backbone shall connect, singly or severally, to buildings, not to individual departments or units.
ii. The planning, installation, maintenance and support of the University Network Backbone shall be the sole responsibility of IAIICT.
iii. Connection to the University Network Backbone shall be guided by the Policy and approved by the Vice Chancellor, on the recommendation of the Director, IAIICT.
iv. IAIICT shall adhere to and maintain copies of all relevant networking standards and keep abreast of national and international developments on these standards.

v. The University Network Backbone should always aim at facilitating the traffic flow between connected buildings or networks.

2.4.4 Campus Local Area Networks (LANs)

The computer network within each campus building shall form a Campus Local Area Network (LAN). IAIICT shall take responsibility for the Campus LANs, namely, the necessary wiring and related equipment within existing buildings to allow connections to the backbone network. The LAN shall conform to the following:

i. Connection between buildings shall be using single core optic Fiber as much as possible. A layer-three fiber enabled switch shall be provided for connection to the distribution network. Connection to the distribution point shall be via optic fiber cable.
ii. Each building shall have a LAN based on CAT 6 UTP cable. The cable must be of extremely high quality to ensure durability and reliability.
iii. An appropriate and well documented IP plan for easy implementation and reference shall be put in place.
iv. Building networks connecting to the University network shall meet overall University network security and management requirements.
v. In cases where there are constraints to connecting any building to the University Network Backbone, consultations and subsequent approvals by the Director IAIICT shall be made to allow for alternative configurations.
vi. Any LAN device not procured directly by the university but approved to be installed in the university network shall become the property of the university.

2.4.5 Distribution Network

The University Distribution Network refers to all the aggregated inter-connected segments of the network. The Inter-campus connections shall consist of the necessary services and related equipment that allow a remote campus or remote university office to access the University's network services.

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

ii. Network protocols used on inter-campus connections must use approved configuration parameters including approved network identifiers.
iii. Inter-campus links connecting to the University network shall meet the University network security and management requirements.

2.4.6 Wireless Networks

This refers to the provision of connectivity to network services (intranet/internet) using wireless technology through authorized Access Points.

i. The University shall support the provision of reliable and secured near-ubiquitous Wireless Access Points across the University Campuses.
ii. Installation, configuration, maintenance, and operation of University wireless networks serving on any property owned or rented by the University, are the sole responsibility of IAIICT.
iii. Any request for installation of wireless devices/communication devices that will ride on the University's network infrastructure must be approved by the Vice Chancellor on the recommendation of the Director, IAIICT.
iv. Any unapproved installation of wireless communications equipment is prohibited, and will be confiscated/impounded if found and person(s) responsible appropriately sanctioned.
v. Any wireless device not procured directly by the University but approved to be installed in the University network shall become the property of the University.
vi. Only approved Wireless Access Points shall be allowed to operate on the network.
vii. The configuration of such Wireless Access Points shall strictly comply with IAIICT's approved network and security configuration standards to achieve consistency and performance standards.

2.4.7 Virtual Private Networks (VPN)

Virtual Private Network provides a protected connection when using public networks. It encrypts your internet traffic and disguises your online identity in real-time. This makes it more challenging for outside parties to monitor your online activities and steal data.

a. Dual (split) tunneling or similar activities are not acceptable, only a single network connection is allowed. Any exception must be requested through the NIS and approved by the Director of IIAIICT.
b. Good and up-to-date anti-virus should be used on the personal computers connected to University's internal network via VPN.
c. Users found to have violated the VPN access policy may be subject to loss of privileges of services and/or be subject to disciplinary action.

i. Users of University ICT services shall be granted rights to use VPN connections if they intend to gain access to the University ICT intranet services through public networks.
ii. By using the VPN technology, users are subject to the same rules and policies that apply while on campus.
iii. It is the responsibility of the user with VPN privileges to ensure that unauthorised users are not allowed access to the University networks through their credentials.
iv. All VPN services are to be used solely for approved University business or academic purpose.
v. All VPN services usages shall be logged and are subject to auditing.
vi. Network protocols used on VPNs and communicating through the gateway must use approved configuration parameters including approved network credentials.
vii. All VPN accesses shall be strictly controlled, using either a one-time password authentication or a strong passphrase.
viii. All computers connected to the University's internal networks via VPN shall use the most up-to-date antivirus and anti-malware software recommended by the University.
ix. VPN users shall automatically be disconnected from the University's network after fifteen minutes of inactivity and the user is required to logon again to reconnect to the network. Pings or other artificial network processes to keep the connection open indefinitely are strictly prohibited and shall be deemed to constitute an abuse and shall be sanctioned appropriately.

2.4.8 Network Equipment Installation and Access to Data Centre

Network Equipment Installation

i. Only designated staff of IAIICT are to install and maintain active network equipment including APs, switches and routers connected to the University's ICT networks.
ii. Nobody is allowed to install and maintain any network device (access points, switches or routers) without authorization of the Director IAIICT.

Access to Data Centre and Network Equipment

i. Access to University Data Centre and other network equipment installations shall be restricted to authorized IAIICT personnel only. However, where a non-ICT staff is necessarily involved, approval of the Director, IAIICT must be sought.
ii. Movement of any network/computing equipment and/or installation shall be authorized only by the Director IAIICT, in accordance with this Policy document.
iii. All network equipment and/or installation shall be labelled according to the University approved ICT nomenclature specification.
iv. The Network Infrastructure Unit (NIS) shall maintain an updated Network Equipment Asset Register.
v. All University units shall maintain a service schedule for all network equipment.
vi. IAlICT equipment to be installed on the University network shall comply with approved University specifications as spelt out by the IAIICT from time to time.
vii. All installations or modifications of any network equipment shall be guided by this Policy document and as approved by the Director, IAIICT and supervised by the NIS.
viii. All third-party connections to the University network shall comply with the provisions of this Policy.
ix. All contractors or third-party access to data center or network equipment installation shall be authorized and supervised by the NIS.
x. In the event of fire or other emergencies, security personnel and other relevant staff may access the affected areas to deal with the incident.

2.4.9 Connection to and Usage of the University Network

Connection to the University Network

i. All connections to the University networks must conform to the standards defined by IAIICT and with the requirements that apply to Internet Protocol (IP) addresses.
ii. Only designated staff of IAIICT, or other staff authorized by the Director, IAIICT, may make connections of desktop services equipment to the University network.
iii. Computer workstations connected to the University network will not be set up to offer services to other users, for example, to act as servers, without due evaluation to ascertain the level of risk or otherwise. More so, a written consent of the Director, IAIICT has to be obtained. Such workstations must be regularly monitored by NIS along with owners to ensure compliance and mitigate any breaches.

External Access to Servers on the Backbone Network

i. External access means access by persons external to the University; access to the backbone network from external locations.
ii. Where specific external access is required to servers on the backbone network, the Director, IAIICT shall ensure that this access is strictly controlled and limited to specific external locations or persons.
iii. The Director, IAIICT will monitor compliance with access arrangements as stipulated in this Policy and the relevant ICT Security Policy on Server Security issued by the University from time to time.
iv. Abuses of or failure to comply with stipulated arrangements shall result in immediate restriction or disconnection from the network.

External Data Communications

i. All external data communications shall be channeled through University approved links.
ii. No external network connections shall be made without the prior consent of the University Management (or the Vice-chancellor). The Director, IAIICT must conduct risk assessments and advise the Management appropriately.
iii. The installation and use of leased or private links on premises owned, managed or occupied by the University shall require the prior written consent of the Vice-Chancellor.

iv. The use of modems, leased or other means of access to other networks on equipment located on premises owned, managed or occupied by the University that are linked to the University ICT network infrastructure is prohibited unless a proposal and justification for such connection has been approved by the Director, IAIICT, after appropriate risk analysis must have been conducted.

Restriction and/or Suspension and/or Termination of Access to Networks

i. A user's access to the University network will be revoked automatically:
   a. at the end of studies, employment or research contract.
   b. on the request of the Director/Dean of the School/Registrar/Head of Department or Head of Unit; where there is a breach of these regulations.
ii. The University reserves the right to revoke a user's access to the University network where the user is suspended pursuant to a disciplinary investigation.
iii. The Registrar will establish mechanisms to ensure that changes in employment/student status are communicated immediately to the Director IAIICT so that their network access and e-mail accounts can be suspended or deactivated as appropriate.

Web Filtering

IAIICT shall be responsible for the implementation of appropriate filtering facilities for web-based and non-web Internet traffic, including MP3 traffic and other bandwidth-intensive services that may not have direct educational or research value, where and when necessary, in conformity with the ICT Policy and relevant ICT guidelines that promote efficient and high availability of Internet services to the majority of users.

2.4.10 Additional or Changed Equipment

i. University units shall notify the Director IAIICT in advance and at the earliest opportunity, of any plan to add items of desktop services equipment or to replace or to relocate desktop equipment that are connected or that may require connection to the University network.
ii. The Director IAIICT shall assess the likely impact on the University networks of the proposed change. The Director IAIICT shall approve the

proposed change only where appropriate adjustments can be made to accommodate any effects on network traffic that this change may cause.

3 Bandwidth Purchase and Usage

3.1 Introduction

Bandwidth purchase and usage policy is dedicated to ensuring efficient and judicious network utilization with the intention to meet the growing bandwidth requirements of the entire University.

3.2 Policy Objectives

To ensure optimum efficiency in the purchase and utilization of bandwidth in a manner that guarantees fair share to all users of the wired/wireless network bandwidth.

3.3 Policy Scope

This Policy applies to all University staff, students and guests.

3.4 Policy Statements

3.4.1 Bandwidth Procurement

The procurement of bandwidth shall be according the Public Procurement Act of the federation.

3.4.2 Bandwidth Management and Utilization

i. IAIICT shall manage the bandwidth resources of the University and ensure effective and fair utilization by all users.
ii. Internet bandwidth will not be over utilized as to prevent access to critical information, research and online educational material.
iii. Unauthorized persons/users are not allowed to access internet facilities within the campus network.
iv. Use of internet is allowed as long as it does not violate the Policy or degrade the performance of the network or divert attention from work or studies.

v. No user may damage, alter, or degrade equipment providing internet and network connections, thus hindering others in their use of the Internet.

vi. Users shall not:

a. Download or store music, media or any other files where copyright issues may be of concern.

b. Use the University Internet facility for running private businesses.

c. Use the University facilities to gain unauthorized access to any computing, information, or communications devices or resources.

d. Upload, download, or transmit:

i. copyrighted materials belonging to third parties.

ii. offensive, fraudulent, threatening or harassing materials.

iii. propagate computer viruses, run peer-to-peer software, send and/or receive unofficial files or undertake in activities that cause network congestion.

vii. In cases where a user violates this Policy, IAIICT may revoke access to the network and initiate appropriate disciplinary procedures against the user.

3.4.3 Pooling of Internet Bandwidth Acquired by Units

i. Internet bandwidth acquired by any unit or department of the University under any programme/project shall be pooled with the University Internet bandwidth, and be treated as University's common resource.

ii. Under particular circumstances that may prevent such pooling with University Internet bandwidth, such network should be totally separated from the University campus network. All the computer systems using that network should have separate IP address scheme (private as well as public) and the University gateway should not be specified as alternative gateway. Such networks should be adequately equipped with necessary network security measures as laid down by this Policy. One copy of the network diagram giving details of the network design and the IP address schemes used shall be submitted to IAIICT for proper scrutiny prior to deployment:

4 Cyber Security Policy

4.1 Introduction

Cybersecurity by this Policy refers to the protection of University ICT infrastructure and information assets against any compromise or attack that may affect its confidentiality, integrity and/ or availability.

4.2 Policy Objectives

To ensure the protection, rigidity and stability of all University ICT infrastructure, the information held therein and services against any cyber threats.

4.3 Policy Scope

This Policy applies to all University-owned ICT infrastructure, digital information and services.

4.4 Policy Statements

4.4.1 General Use and Ownership Policy

Role of IAIICT

i. WHILE IAIICT IS CHARGED TO BE COMMITTED TO THE PROVISION OF A REASONABLE LEVEL OF PRIVACY, IT SHALL, HOWEVER, NOT BE LIABLE FOR ANY BREACH IN THE CONFIDENTIALITY OF PERSONAL INFORMATION STORED OR TRANSMITTED ON ANY NETWORK OR DEVICE BELONGING TO THE UNIVERSITY.
ii. The data created and transmitted by users on the ICT systems shall always be treated as the property of the University, until determined otherwise.
iii. IAIICT shall protect the University network and the mission-critical University data and systems. IAIICT shall not guarantee the protection of personal data residing on University ICT infrastructure.
iv. For security and network maintenance purposes, IAIICT staff shall monitor equipment, systems and network traffic at any time as provided for in the Network Development and Management section of this Policy.
v. IAIICT shall reserve the right to audit networks and systems periodically to ensure compliance with this Policy and other regulatory provisions that may come into effect from time to time.

Role of IAIICT in cyber security

a. Cyber Security policies should conform to all applicable ICT policies, including but not limited to the data center and network equipment (2.4.8), password policy, Wireless Access, Computer Laboratory and digital center Access to the data centre Protected against physical intrusion as well as exposure to water, dust and fire Power outages of fluctuations should be avoided. Supported by a backup power supply

   The Directorate for ICT Support

   1. Maintain baseline sources configurations that are up to date and well-documented for all hardware and software.
   2. Develop and implement a patch management plan
   3. Implement network filtering to protect the network against malware-related threats
   4. Ensure the controlled and audited usage of ICT administrative privileges
   5. Implement centralized monitoring and real-time analysis of all ICT network device event security logs.
   6. Ensure the limited and controlled use of network ports and controls
   7. Standard operating procedures such as back-up of data, logging events, and environmental monitoring should be established by the staff of NIS

8. The firewall must be regularly tested for configuration errors that may represent weakness and consistency of the firewall rule set to confirm the current status matches the expected requirement.
9. The IAIICT reserves the right to grant request (s) to open the firewall. It will evaluate the risk of opening the firewall to accommodate requests. Where the risk is acceptable, granting of requests will be dependent on network infrastructure limitations and the availability of required resources to implement the request.

Users

i. Ensure compliance to the cyber security policy
ii. Report any cyber security incident to IAIICT

Users should avoid

i. sharing of individual access passwords
ii. Usage of any pirated software on University computing devices
iii. Utilizing of any illegal peer-to-peer software
iv. Any user action that contravenes the Computer Misuses Act (2011) or the Anti-pornography Act (204)
v. Any user action that violates the rights of any person or entry's legally registered copyright and/or Intellectual Property
vi. Introduction/uploading of any malicious software onto any University computing device or network
vii. Any action that disrupts the normal functioning of any university computing device or network
viii. Unauthorized networks port reconnaissance, and/or network and/or software penetration
ix. Using university computers and/or the network to interfere with a system or network outside the university
x. Using any university computing devices and/or networks to send out spam
xi. Using of university computing devices and/or networks for any gambling activity
xii. Using of university computing devices and/or networks for any personal commercial purposes

Password Policy

Rules

a) The Unit responsible, shall define the password strength and lifecycle specification for all user categories from time to time
b) All default system or hardware passwords shall be changed
c) All users shall ensure the privacy of their passwords
d) NIS shall implement and maintain centralized authentication, authorization, and accounting service mechanism for all network core equipment to all ICT resources
e) All local developed applications shall support password encryption and user role segregation

3. **Backup and recovery**

a. Backup documentation is required which includes identifying of all critical data, programs, documentation, and support items that would be necessary to perform essential tasks during a recovery period.
b. Documentation of the restoration process must include procedures for the recovery from single-system or application failures, as well as for a total data center disaster, scenario, if applicable.
c. Backup and recovery documentation must be reviewed and updated regularly to account for new technology, business changes, and migration of applications to alternative platforms.
d. Recovery procedures must be tested on annual basis.

4. Software development, Acquisition, support and use 7.1

The university shall build internal capacities to develop its own software for the major information system.

Securing Confidential and Property Information

i. University data contained in ICT systems shall be classified as either confidential or non-confidential. Examples of confidential information include but are not limited to: payroll data, human resource data, accounting data, student examination results data and research data. Employees shall take all necessary steps to prevent unauthorized access to confidential information.
ii. Users shall keep passwords secure and shall not share accounts. Shared accounts are strongly prohibited. Users are responsible for the security of their passwords and accounts. System-level passwords shall be changed

each month; user-level passwords shall be changed periodically, at least once every six (6) months.

iii. 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.

iv. Postings on blogs or newsgroups by users with their University official email addresses shall contain a disclaimer stating that the opinions expressed are strictly those of the users, unless they are in the course and within the scope of official duties.

v. All hosts connected to the University Internet, intranet or extranet, whether owned by the user or the University shall always be required to have approved virus-scanning software with an up-to-date virus database installed.

vi. The user shall exercise caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horses, and should immediately seek help of IAIICT if inadvertent action had been taken to curtail the spread of the compromise.

4.4.2 Conditions of Use of Computing and Network Facilities

Unacceptable Activities

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

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

ii. Deliberate or inadvertent introduction of malicious programs into the network or server, for instance, viruses, worms, Trojan horses or e-mail bombs.

iii. Sharing of the University user accounts and passwords—users shall bear full responsibility for any abuse of shared accounts.

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

v. Making fraudulent offers of products, items, or services originating from any University account.

vi. 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 permitted 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.

vii. Port scanning or security scanning unless prior notification to NIS is made and approval is granted.

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

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

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

xi. Using any program, script or command, or sending messages of any kind, with the intent to interfere with, or disable, another user's access proviledges, via any means, locally or via the Internet, intranet or extranet.

xii. 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.

Wireless Network Users Responsibilities

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

ii. The University accepts no responsibility for any loss or damage to the user computing device consequently to connection to the wireless network.

iii. 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.

iv. Users shall authenticate on the wireless network for every session.

v. 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.

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

vii. Wireless network users shall get their Internet Protocol (IP) addresses automatically; a valid IP address shall be granted when connected. Use of static IP addresses is prohibited.

Appropriate use of Electronic Mail

i. Electronic mail and communications facilities provided by the University are intended for teaching, learning, research, outreach and administrative purposes.
ii. All official communications shall be via ABU domain email addresses
iii. Electronic mail may be used for personal communications within appropriate limits.

4.4.3 Bring Your Own Device

The University shall allow the usage of personal devices on the University network as long as such users comply with the Policy and offer a similar level of protection as specified in the Policy. Such usage will be subject to the following:

i. On no account that sensitive or confidential University information shall be stored on such devices.
ii. The University will provide an acceptable level of protection for such personal devices as enshrined in the ICT Policy from time to time.
iii. The University shall have the right to investigate/audit such devices in case of any malicious activity, cybercrime or fraud that affects the University.

4.4.4 Password Policy

i. All default passwords auto-generated during account creation must be changed at the first login.
ii. Birthdays and other personal information such as address and phone numbers shall not be used for passwords.
iii. Users shall use strong passwords that contain both upper and lower case characters, numeric characters, special characters.
iv. All system-level passwords such as root, Windows server administration, application administration accounts, shall be changed at least once every month or as planned by the IAIICT Network Security team.
v. All user-level passwords such as for email, web, and desktop computer shall be changed at least once every six (6) months.

vi. User accounts that have system-level privileges granted through group memberships or programs such as "SA" shall have passwords distinct from all other accounts held by such users.
vii. Passwords shall not be inserted into email messages or other forms of electronic communication.
viii. Passwords for the University accounts shall not be used for other non-University accesses such as personal ISP account, Yahoo Mail, Gmail, and Bank ATM.
ix. All passwords shall be treated as sensitive, confidential University information. Users shall not share the University passwords with anyone.
x. Users shall not use the "Remember Password" feature of applications like portals, and Email system.
xi. Users shall not write passwords down and store them anywhere in their offices.
xii. Where an account or password is suspected to be compromised the affected passwords shall be changed immediately. IAIICT shall be alerted immediately to investigate the incident if it affects critical University information systems or processes.
xiii. All user-level and system-level passwords shall conform to the password construction guidelines.
xiv. Every user has a responsibility to protect their accounts and must ensure that they report any suspicious breach of their accounts to IAIICT for appropriate actions.

5 Systems Backup and Recovery Policy

5.1 Introduction

Data backups are a requirement to enable recovery in the case of events such as system failure, natural disasters, system compromise, data entry errors, or system operations errors. All backups must conform to the best practice procedures.

5.2 Policy Objectives

To ensure that there is no loss of information and that there shall be successful recovery of data

5.3 Policy Scope

This data backup policy applies to all University entities who use computing devices connected to the network or as stand-alone and who process or store critical data owned by the university.

5.4 Policy Statement

i. The units are responsible for arranging adequate data backup procedures for the data held on computer systems assigned to them.
ii. IAIICT is responsible for the backup of data held in servers and related databases.
iii. The responsibility for backing up data held on the workstations of individuals falls entirely on the user.
iv. The frequency of backup should be determined by the sensitivity of the data and or agreed schedule(s) where necessary.
v. Copies of the backup media, together with the backup record, should be stored in a safe location.
vi. Records of what is backed up and to where must be maintained by the unit/owner responsible.
vii. Regular tests of restoring data/software from the backup copies should be undertaken once per semester to ensure that they can be relied upon for use in an emergency.
viii. The backup media must be precisely labeled and accurate records must be maintained of backups done.
ix. Units that need files restored must submit a request to the IAIICT for that purpose.
x. Official systems shall only be restored by personnel approved by IAIICT

6 Computer Laboratory & Digital Centre

6.1 Introduction

Computer laboratory here includes all computer labs used for teaching, CBT centre, digital centre.

6.2 Policy Objectives

The objective of the Policy under this section is to ensure that computer labs are functional at an optimal level at all times.

6.3 Policy Scope

This policy applies to all University students, staff and guests who have been granted access to use university owned computer laboratories. It is also applicable to university administrators having a laboratory under their custody.

6.4 Policy Statements

i. Computer laboratories at all units of the University shall have attendants deployed by IAIICT who will be responsible to the Head of Department/Unit for ensuring that the facilities are:
   a. Compliant to ICT approved baseline setup and configurations
   b. Routinely checked for unauthorized connections
   c. Accessed only by authorized students and/ or researchers with valid ABU ID card and must be able to produce the card upon request
   d. Labelled according to approved ICT nomenclature
   e. Professionally serviced and maintained

ii. Any device not procured directly by the university but approved to be installed in the university laboratory shall become the property of the university.

iii. Heads of Departments/units shall ensure that all Computer Lab Facilities in their Departments/units are:
   a. Locked down to prevent physical theft of any component
   b. Protected against exposure to water leakages, fire and or dust
   c. Located in strongly burglar proofed rooms

iv. The use of Labs shall be subjected to the following:
   a. All persons using the lab are responsible for backing up their own data and protecting their own information.
   b. Smoking, food and beverages, are prohibited in the labs.
   c. Audio output or sound playing devices are permitted only with the use of headphones.
   d. Lab equipment shall only be used for business purposes with the approval of the Vice Chancellor.

e. Disabling computers by disconnecting cables, removing hardware, installing software or locking workstations by unauthorised persons will be considered as vandalism and treated as such.
f. Cables (power and network) shall not exposed. They shall be neatly terminated and well insulated or wrapped with tape to conform with approved safety standards.

7 Software Development, Acquisition, Support and use

7.1 Introduction

The University shall develop internal capacity to develop its own software for the major information systems.

7.2 Policy Objectives

The objective of the policy is to define clear software development and acquisition processes in order to optimize the use and value of university resources.

7.3 Policy Scope

The policy refers to all software used to support university functions either developed internally or outsourced (including off-the-shelf software).

7.4 Policy Statements

i. IAIICT shall periodically define the Systems Life Cycle methodology for:
   a. systems and software engineering for both in-house and outsourced development
   b. acquisition of off the shelf software
   c. maintenance of software

ii. All software shall undergo testing and quality assurance before installation in any production environment within the University and ensure provision for:
   a. Information classification
   b. Usage of the least privilege principle
   c. Segregation of roles
   d. Audit trails

iii. All software under this policy shall comply with the Software Licensing and Ownership and Cyber Security Policies
iv. All acquired software shall, where necessary, contain provisions for technical support and upgrades
v. All university units shall, where necessary, make use of open-source software based on a risk-based assessment as referenced in the cybersecurity policy
vi. All University Units undertaking the development or acquisition of any software shall ensure compliance with this policy and plan for end-user training
vii. This policy does not apply to software development within the university for academic or educational purposes

8 User Support Services

8.1 Introduction

The University shall ensure the provision of ICT Services within the University as well as define the Unit responsible for ICT as the central coordination point of contact for all ICT support. The ICT support shall cater for all areas under the University network, computing devices, hardware, software and implementation of ICT initiatives, projects and programs at all campuses and their related technical support.

8.2 Policy Objectives

The objective is to deliver optimal user support services in line with the strategic direction of the University.

8.3 Policy Scope

The Policy scope under this section provides a centralized structure for the management of all ICT support services in the University and it shall apply to all University-owned ICT applications and devices.

8.4 Policy Statements

Roles

i. The IAIICT shall define processes and procedures for the delivery of optimum ICT support services, subject to the approval of the Vice Chancellor.
ii. The IAIIICT shall adopt an appropriate Business Model for the provision of ICT services.
iii. The IAIICT shall create a business development unit for the commercialization of ICT products and services.

ICT Services Support

ICT Services Support is, by this Policy, defined as such operations carried out by authorized personnel to ensure efficiency, stability and continuity of any ICT service or equipment so as to it meets its intended use requirements.

Responsibilities of ICT Services Support Personnel

The University shall provide, through the IAIICT, the necessary work tools, safety gear and training for all ICT services support personnel. Accordingly, such personnel shall:

i. Ensure adequate protection against tampering with, alteration or theft of ICT devices;
ii. Safeguard the security of systems and information;
iii. Provide assistance and guidance to users towards compliance with the ICT Policy;
iv. Provide technical support in line with approved ICT procedures for any system, service, device downtime or breach;
v. Ensure the installation and configuration of all hardware and software is aligned to approved ICT standards;
vi. Ensure safe custody and authorized usage of all University software licenses, copyright and usage keys.

9 ICT Equipment and Systems Maintenance

9.1 Introduction

The University recognizes the important role of the Hardware Engineer/Technician/Manager in providing quality services to its users, by ensuring that the equipment is well maintained and repaired in good time. This policy will guide the Hardware Engineer/Technician /Manager at the Central Facility as well as those at the various units.

9.2 Policy Objectives

The Policy in this section aims at ensuring that the rules and guidelines governing maintenance of ICT equipment and systems meet University approved standard.

9.3 Policy Scope

This policy specifies the general approach to providing maintenance services on ICT equipment and systems in the University.

9.4 Policy Statements

IAIICT shall maintain and provide support in the repair or replacement of computer wares where possible. However, where such wares are privately owned, their maintenance shall be governed terms and conditions of agreement between the University and the third party.

Equipment with special maintenance requirements which cannot be provided by the IAIICT shall be maintained through outsourcing. Similarly, equipment under warranty shall be maintained as specified by the terms of the warranty.

10 Email Account Use Policy

10.1 Introduction

The University shall provide email resources to support collaboration in administration, teaching and learning as well as scholarly research.

10.2 Policy Objective

The objective of the policy statement to set forth the University's policy concerning the use of, access to, and unauthorized disclosure of email and to assist in ensuring that the University's email resources serve the purpose for which they are intended.

10.3 Policy Scope

This policy applies to all University staff and students using university emails.

10.4 Policy Statements

i. The facility shall be used primarily for academic and official purposes and to a limited extent for personal purposes.
ii. Using the facility for illegal purposes is a direct violation of the university's ICT policy and may entail the withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages, broadcasting unsolicited personal views on social, political, religious matters, and the generation of threatening, harassing, abusive, obscene or fraudulent messages/images.
iii. Users should not open any mail or attachment that is from an unknown and suspicious source. Even if it is from a known source, and if it contains any attachment that is suspicious or looks dubious, users should get confirmation from the sender about its authenticity before opening it. This is very much essential from the point of security of the user's computer, as such messages may contain viruses that have the potential to damage the valuable information on your computer.
iv. Users should not share their email accounts with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.
v. Users should not intercept, or attempt to break into others' email accounts as it is infringing the privacy of other users.
vi. While using the computers that are shared by other users as well, any email account that was accidentally left open by another user, should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.

vii. Impersonating email account of others will be taken as a serious offence under the university ICT security policy.
viii. It is ultimately every individual's responsibility to keep their e-mail account free from violations of the university's email usage policy.

11 ICT Skills Capacity Building and Training

11.1 Introduction

The adoption of Information and Communications Technology (ICT) products and tools will require the attendant training to enable effective usage. This requires a dedicated approach within the University to be able to plan for such gaps as well as develop and implement appropriate training when the need arises.

11.2 Policy Objectives

The purpose of the policy under this section is to:

i. Identify skills gaps and training needs among members of the University community.
ii. Provide guidelines for planning, organizing and conducting ICT training and capacity building in the University to achieve efficient and effective utilization of resources.
iii. Undertake capacity building towards the improvement of technical capacities of its staff as per and when the need arises;

11.3 Policy Scope

This policy applies to all ICT related capacity building and training activities that support the various functions of the University.

11.4 Policy Statements

ICT Literacy

All University staff should 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.

ICT Capacity Building Assessment

IAIICT shall:

i. coordinate the periodic assessment of existing ICT skills capacity amongst all user groups to be able to identify gaps in partnership with Heads of Departments
ii. undertake a periodic capacity skills assessment to identify knowledge gaps within its technical staff to be able to seek appropriate capacity building programs.

ICT Capacity Building Delivery Methods

IAIICT shall:

i. develop Capacity Building modules and courseware for identified ICT skills gaps.
ii. Implement such capacity building with either internal resource personnel or with subject matter experts as per the nature of the required ICT capacity building.
iii. Coordinate the identification of any external expertise for specialized training needs.
iv. Through the University ensures the presence of well-equipped ICT training computer labs.
v. In partnership with Heads of Department identify Trainees for such capacity-building programs.

Mode of Training

i. Internal ICT user training targeting the University community shall be scheduled conducted on a sustained basis.
ii. External ICT training shall be organised by IAIICT in response to needs as may be assessed from time to time when training is not possible within the University.

Trainees

IAIICT shall jointly with DAPM nominate trainees for ICT training when the need arises.

Training Resources

IAIICT in liaison with DAPM shall identify the appropriate trainers. The University shall provide requisite resources to facilitate the training.

12 Information Systems Administration

12.1 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:

i. availability of the database service to the intended customers
ii. flexibility in terms of access through the use of different interfaces
iii. administration and management of the same service

12.2 Policy Objectives

These policies have been developed to achieve the following objectives:

i. 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
ii. 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
iii. ensure that the University's data resources are firmly controlled based on prescribed standards and that data changes are audited.
iv. enhance the efficiency with which database applications are developed, deployed and used.

12.3 Policy Scope

This policy document shall be a point of reference among stakeholders on all matters relating to database services within the University.

12.4 Policy Statements

12.4.1 Services

The University database services, maintenance of user accounts; backup, and recovery shall be carried out in accordance with the provisions on ICT Security and Internet as provided in this Policy, while training will be in accordance with the relevant provisions the Policy.

The IS application process will be carried out in accordance with the Software Development, Support and Use section of the Policy.

An appropriate channel of communication that allows the Database Administrator (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:

i. Authorisation and Access Control
   a. Authorisation and data control: Access to the production (and replication) databases shall be restricted to production applications and through reporting tools.
   b. Authorisation outside of these applications shall be approved by the client controlling the data and will be maintained and controlled by DBA.
   c. 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.
   d. Developers shall have a special role for functional development and integration databases that they support.

ii. Storage of Database Usernames and Passwords
   a. Database usernames and passwords may be stored in a file separate from the executing body of the program's code. This file must not be readable.
   b. Database credentials may reside on the database server. In this case, a hash number identifying the credentials may be stored in the executing body of the program's code.
   c. Database credentials shall not reside in the documents tree of a web server.
   d. Passwords or passphrases used to access a database must adhere to this Policy's provisions on Passwords.

iii. Retrieval of Database Usernames and Passwords
   a. If stored in a file that is not source code, then database usernames and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the username and password must be released or cleared.
   b. The scope to which database credentials are stored must be physically separated from the other areas of code, for example, the credentials must be stored in a separate source file.
   c. For languages that execute from source code, the credentials' source file must not reside in the same browsable or executable file directory tree in which the executing body of code resides.

iv. Access to Database Usernames and Passwords

a. Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.
b. Database passwords used by programs are system-level passwords as defined by this Policy's provisions on Passwords.
c. Developer groups must ensure that database passwords are controlled and changed in accordance with this Policy's provisions on Passwords.

v. Development Support
   a. DBA shall provide support to the development group.
   b. Support activities shall include but 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 modelling.

vi. Operational Support

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

vii. Monitoring and Tuning
   a. Once the data and applications have been moved to production, the DBA shall utilize various tools to monitor their operation.
   b. The DBA shall make modifications to the data size allocations, reorganization frequency, and copy and frequency only in liaison with the relevant Project Leader.
   c. The DBA shall bring application inefficiencies to the attention of the relevant Project Leader and make recommendations, if desired, on ways to tune them and make them more efficient.

12.4.2 Service Level Agreements (SLAs)

The DBA shall respond to service request in accordance with University (IAIICT) Service Level Agreements

13 Systems Administration

13.1 Introduction

System Administrators are individuals having the responsibility for ensuring the proper operation of IT resources of the University. They are expected to have the technical capability for performing system administration duties. If a user is granted system privileges on a machine, they are also bound by the System Administrator's rules listed here. These resources include shared systems, individual-use desktop and laptop systems, and networks and network equipment belonging to the University. This section outlines the policies and procedures for managing, installing, upgrading, and maintaining systems in the University.

13.2 Policy Objectives

To establish the responsibilities and provide guidance to System Administrators and other users for the ethical and acceptable use of systems.

13.3 Policy Scope

This policy applies to all users of University information technology resources as well as those charged with the support of these resources. University information resources by this Policy refers to all individually controlled or shared, stand-alone or networked information resources which may either be owned, leased, operated, or contracted by the University.

13.4 Policy Statements

13.4.1 Responsibilities to the University

The System Administrator shall ensure the following

i. take responsibility of activities originating from his/her accounts;
ii. take precautions against theft of or damage to the system components;
iii. take precautions that protect the security of a system or network and the information contained therein;
iv. promulgate information about specific procedures that govern access to and use of the system, and services provided to the users or explicitly not provided;

v. to ensure problems are detected and fixed with the cooperation of system administrators of other information technology resources, whether within or outside the University;
vi. comply with the technical direction and standards established by University (IAIICT) and other guidelines or standards defined by the

13.4.2 Copyrights and Licenses

i. Systems Administrators and users of University information technology resources shall respect copyrights and licenses to software and other online information.
ii. In addition to software, all other copyrighted information (text, images, icons, programs, etc.) retrieved from computer or network resources shall be used in conformance with applicable copyright and other law.
iii. Any System developed for use in the University shall be deemed property of the University and any employee or contractor found in unauthorized possession of the system or part of it shall be appropriately sanctioned based on University regulations or prosecuted based on the laws of the Federal Republic of Nigeria.

13.4.3 Modification or Removal of Equipment

i. System administrators shall not attempt to modify or remove computer equipment, software, or peripherals that are owned by others without proper authorization. Notwithstanding, such authorization may be granted for any University-owned equipment through written permission of the Director, IAIICT.
ii. Information technology resources that are retired or transferred to another location must have all data and licenses removed prior to release of the equipment.

13.4.4 Data Backup Services

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

13.4.5 Misuse and Security Breach

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.

i. Systems Administrators shall report in writing critical security breaches to the Director IAIICT immediately upon discovering the breach.
ii. Systems Administrators shall immediately investigate any possible breach reported to them.
iii. System Administrators shall maintain appropriate system logs useful in tracing and identification of individual user's systems activity for a minimum of 30 days. System administrators shall beware that any log is subject to subpoena or other legal process.

13.4.6 System Integrity

i. Systems Administrators shall be responsible for maintaining all aspects of system integrity, including obtaining releases and fixes that assure the currency of operating system upgrades, installation of patches, managing releases, installation of anti-virus software, updates of virus definitions, and the closure of services and ports that are not needed for the effective operation of the system.
ii. System Administrators shall be responsible for prompt renewals of stipulated vendor hardware and software agreements, or as may be described in the vendor support contracts.
iii. Systems Administrators shall remain familiar with the changing security technology that relates to their system and continually analyze technical vulnerabilities and their resulting security implications.
iv. Systems administrators shall ensure all identified vulnerabilities are addressed promptly.

13.4.7 Account Integrity

i. Systems Administrators shall manage accounts on a timely basis, providing new accounts and deleting old accounts in a prompt manner.
ii. Systems Administrators shall ensure user accounts are disabled and deleted based on the access rules for the environment and in compliance with all licensing.

iii. Systems Administrators shall ensure that secured passwords are used and that passwords are changed frequently, within the limits of the system environment.
iv. System Administrators shall ensure that accounts can be traced to an individual person (or a group of people in the case of group accounts) and that the accounts have system access that matches the authorisation of the user.
v. System Administrators shall ensure that stored authentication data (e.g., password files, encryption keys, certificates, personal identification numbers, access codes) are appropriately protected with access controls, encryption, shadowing, etc. - e.g., password files must not be world-readable.

14 ICT Procurement and Decommissioning

14.1 Introduction

This section provides general guidelines on the procurement of ICT equipment and services including installation and training as applicable.

14.2 Policy Objectives

To guide the procurement of all University ICT equipment and services towards ensuring standardization of all ICT related assets, transparency, timely delivery, quality assurance, value for money as well as compatibility with existing infrastructure and services.

14.3 Policy Scope

This policy shall apply to all the units or entities of the University in the procurement of ICT equipment and services.

14.4 Policy Statements

14.4.1 Procurement of ICT Equipment

i. All ICT equipment acquisition shall adhere to the provisions of the subsisting Public Procurement Law of the Federal Republic of Nigeria.

ii. All procurements relating to ICT equipment and services shall be subjected to experts advice.
iii. Acquisition of all major ICT equipment and services by any unit of the University shall be on the recommendation of IAIICT to ensure compliance with standards.
iv. All major ICT equipment and services procured shall be inspected by the IAIICT to ensure compliance with approved specifications prior to acceptance.
v. All acquired ICT equipment and services shall be properly documented and inventory maintained in accordance with the University guidelines on asset register.
vi. All ICT equipment and services without proper documentation and approval shall be prevented from use on the University infrastructure.
vii. Whenever suitable, software applications shall be developed in-house.
viii. Unless otherwise specified, procurement of all ICT equipment and services shall include installation, testing, appropriate training and commissioning.

14.4.2 Decommissioning

i. ICT hardware shall be replaced periodically in accordance with user needs and changes in technology. While for software the life cycle should be dependent on the release of the new versions in accordance with the software maintenance agreement.
ii. The University shall replace all consumables by the manufacturers' specified date of expiry.
iii. The disposal of obsolete equipment shall be governed by relevant provisions of the University Disposal policy.

15 Social Media

15.1 Introduction

Social media is referred to as any software that provides electronic social interaction amongst its subscribers and communities. Though it is the right of staff to own and use social media, staff are responsible for what they post or do on social media. However, the University expects fair use by staff in case the University network is used in a social media interaction. Official social media

handles owned by the University must be used by an authorised person and only then that the University may be liable for any information shared on the handle.

15.2 Policy Objectives

To guide the appropriate usage of social media by the University staff as well as enhance personal and professional reputation online.

15.3 Policy Scope

This policy applies to all University staff and official social media sites.

15.4 Policy Statements

The following statements shall govern both the usage of official University social media sites as well as staff social media activity:

15.4.1 University Official Social Media Sites

i. Only the University's official social media sites will be allowed to make use of University trademarks and symbols. The University will not be liable for any claim to any post in any parody social account.
ii. Only authorized personnel of the University shall be allowed to make postings on the university official social media sites.
iii. Any information shared across the university social media sites shall comply with the principles of fair use and University policies in the domains of conflict of interest and University trademark and symbol protection.
iv. Information shared across the University social media sites should not make reference to any biased statements on matters such as politics, religion, race, gender, sexual orientation, inter alia; statements that contain obscenities or vulgarities.
v. Administrators of Official University Social Media Sites shall not such sites for personal purposes.

15.4.2 Staff Social Media Activity

Staff social media activity shall:

i. Respect the Laws relating to copyright and other intellectual property rights, defamation, privacy, and other applicable laws.
ii. Not portray others in an unfavourable light in respect of matters including, but not restricted to, religion, gender, sexual preference, race, nationality or disability.
iii. Adhere to the University Confidentiality agreements and information disclosure.
iv. Ensure only public information is posted on Official University Social Media Sites. Sharing confidential information (which may include confidential mails, research not yet in the public domain, information about students or staff or personnel matters, non-public or not yet approved documents or information) is not allowed.

15.4.3 Students Social Media Activity

i. Students are personally responsible for content they post or share via social media. It is essential that students respect the privacy and the feelings of others at all times, and understand that the content posted via social media is a permanent record which is shared instantaneously with a potential global audience.
ii. Students must not use the University's logo on personal social media sites or other websites.
iii. A student's personal online or social media profile may reference the University as their place of study, but it must be made clear that comments / posts / shares made by the account holder are made in a personal capacity only.
iv. Any communication by a student made in a personal capacity through social media must not breach copyright, confidentiality or contains information that discredits the University in any way.
v. If there is doubt about the accuracy of information to be shared on a social media network or site, then students shall refrain from posting, commenting, liking or sharing such information.

16 E-Learning Tools Use

16.1 Introduction

This policy is designed to support the University to carry out its online educational activities by using ICT to enable University's staff, and students to engage in transformative teaching and learning in and beyond the traditional classroom setting. E-learning tools here include learning management systems (LMS), Computer Based Test (CBT) and other technologies.

16.2 Policy Objectives

To define standard procedures and guidelines that govern and promote efficient use of technologies to support teaching, learning and research.

16.3 Policy Scope

This policy applies to all University students, staff and any person charged with the support of university e-learning technology resources.

16.4 Policy Statements

i. The university may adopt online collaboration using known tools such as Moodle, Google Meets, Microsoft Teams, Zoom, Big Blue Button etc. However, the use of free and open-source shall be encouraged.
ii. IAIICT is responsible for technical support of the University LMS and CBT.
iii. The University shall ensure and require that all students, teaching staff and other relevant personnel receive training on a continuous basis to empower them with the requisite skills to fully exploit the digital learning environment in their different disciplines.
iv. The University shall encourage and support the use of the learning management system and other technologies in both face-to-face and online learning environments.
v. All students will have an LMS account created when they join the university. They will be enrolled in the courses they have registered for the semester and will have access to the courses. each student will only have access to his account and be advised to set up a strong password.

vi. All users of the LMS are responsible for maintaining the security of usernames, passwords and any other access credentials assigned. Access credentials may not be shared or given to anyone other than the user to whom they were assigned.

vii. CBT test shall only take place on university-approved platforms and venues.

viii. The regulations for the use of CBT shall be determined by the Directorate of Academic Planning and Monitoring from time to time.

ix. There is an obligation on Employees who are studying University Courses, who also have a level of administrative access to LMS or CBT to contact the Course Examiner for the Course/s the Employee is studying to alert them to this fact. During their study, the Employee is not permitted to access the relevant Course environments, or applicable Systems, using their administrator access.

x. In line with policy item (5) on backup of University records and information, CBT results must be backed up and archived for future references by stakeholders or as the need arises.

xi. It is the responsibility of all stakeholders of CBT examinations to ensure that deployed staff are properly briefed about the conduct of the examination and their expected individual roles.

17 Website use and Update

17.1 Introduction

This Policy acknowledges the importance of the Web in providing relevant information on the University to the public, while also recognizing that users have responsibility to make use of this resource in an efficient, ethical, and legal manner. In this regard, Webmasters and Web content owners are expected to abide by the highest standards of quality and responsibility.

17.2 Policy Objective

To ensure that the University Website provides comprehensive and up-to-date information about the University that is open to the public.

17.3 Policy Scope

This applies to persons and units involved in content generation, processing, review, approval and updating.

17.4 Policy Statements

i. IAIICT shall be responsible for the day-to-day management of the University Website.
ii. Heads of Units of the University shall be responsible for content generation, review and approval while the IAIICT shall the responsibility for processing and updating.
iii. University units having the capacity of developing, maintaining their websites may be allowed to do so subject to approval by the IAIICT. These websites must conform to the University policy provisions on Websites.
iv. Websites of all units shall be under the University's main domain and accessible from the University's main Website.
v. All materials to be posted on the University Website shall comply with the necessary copyright provisions, where applicable. The reproduction, retransmission or republication of all or part of any document or content on the Website shall strictly adhere to the necessary copyright provisions.
vi. The University shall not be held responsible for any loss or damage arising from the use of the University websites.

18 Information Systems Use

18.1 Introduction

This policy stipulates acceptable and prohibited access to the University's network and Information Systems, as well as delineates roles and responsibilities of members of staff, students and other stakeholders of the University. Information systems include university portals, Exams Processing software, Human Resources management system and other systems developed or purchased by the university to enhance its services. The policy aims at protecting the Information assets from illegal access and by extension, assuring the privacy of individuals against any form of abuse as enshrined in the Data Protection Laws of Nigeria. This includes, but not limited to, unauthorised use or copying of data or code.

18.2 Policy Objectives

To define the standard procedures and guidelines that govern the use of university information systems and ensuring that they are fully complied with.

18.3 Policy Scope

This policy encompasses the fair use of the University's network, information systems and other computing devices by users which include staff, students and visitors to the University.

18.4 Policy Statements

i. Staff, students and visitors to the University shall use only the computers, computer accounts, computer files, etc., of the University for which they have authorization.
ii. University information systems shall not be installed on private computers without authorization.
iii. It is prohibited for a user to use other users accounts or attempt to capture or guess their passwords.
iv. Users are responsible for the appropriate use of all resources assigned to them, including the computer, the network address or port, software and hardware.
v. The University is bound by contractual and license agreements with respect to third-party resources and users are required to comply with all such agreements.
vi. Users are responsible for protecting their passwords and all access credentials assigned to them.
vii. Users must comply with the relevant provisions of this Policy for any specific set of resources to which they have been granted access as well strictly comply with the terms and conditions for use of resources they have been granted access.
viii. Users shall not use any software, hardware or other resources in a manner that could harm, disrupt or degrade performance of any part of the system in the University.
ix. The University shall take all necessary measures to protect and safeguard its ICT resources, as much as possible.

19 References

1. University of Southern Queensland ICT Information Management and Security Policy. https://policy.usq.edu.au/documents/13340PL
2. Hekima University College ICT Policy http://hekima.ac.ke/images/downloads/HUC-ICT-policy-manual.pdf
3. Makerere University Information & Communication Technology Policy https://policies.mak.ac.ug/sites/default/files/policies/ICT%20POLICY%20%28APRIL%202016-2020%29.pdf
4. University Of Rochester Information Technology Policy https://tech.rochester.edu/policies/information-technology-policy/
5. Shivaji University, Kolhapur IT Policies & Guidelines http://www.unishivaji.ac.in/uploads/bcud/2020/policy/ITpolicy16Jan2020.pdf
6. The University of Nairobi Information & Communication Technology Policy Guidelines. https://cees.uonbi.ac.ke/sites/default/files/cees/ICTC%20Policy%2014-Nov-2014.pdf