2019

NIGERIAN UNIVERSITIES ICT MINIMUM GUIDELINES

(ICT Policy Document)

This policy document is expected to serve as guidelines for ICT development in Nigerian Universities

National Universities Commission

Table of Contents

CHAPTER 3

Abbreviations and Acronyms

1. CDs Compact Discs
2. CD-ROMS Read only memory compact discs
3. CDRW Read/Write CD
4. DBA Database administrator
5. DVDs Digital Video Discs
6. Director, ICT Chief Information Officers
7. FTP File Transfer Protocol
8. ICT Information and communication Technology
9. IS Information System
10. IP Internet Protocol
11. IPSec Internet Protocol Security
12. LCD Liquid Crystal Display
13. MIS Management Information System
14. LAN Local Area Network
15. NAS Network Attached Storage
16. NFS Network File System
17. NUS Nigerian University System
18. NUC National Universities Commission
19. OS Operating system
20. PDAs Personal Digital Assistant
21. PSTN Packet Switched Telephone Network
22. POC Point of Contact
23. SSH Secure Shell
24. SANs Storage Area Networks
25. SDLC Software Development Life Cycle
26. SLA Service Level agreement
27. SQL Structured Query Language
28. Telnet A terminal emulation program for TCP/IP networks such as the Internet
29. TCP Transmission Control Protocol

30. UPS Uninterrupted Power Supply
31. WAN Wide Area Network

CHAPTER 1

1.0 INTRODUCTION

Information Technology (IT) can be defined as the acquisition, processing, storage and dissemination of vocal, pictorial, textual and numerical information by microelectronics based combination of computing and telecommunications. IT is the branch of engineering that deals with the use of computers and telecommunications to retrieve, store and transmit information. The merging of computing, information communication and technology have made ICT an important aspect of our socio- economic development. In other words, ICT has become a vital tool for any activity or business process for any organization.

In recent times, the Nigerian Government has given particular attention to the use of ICT to support socio-economic development and act as an engine for sustainable development. In line with attaining its goal and strategic objective of becoming one of the first twenty economies in the World, the Government has identified ICT as a major driving force towards engendering global competitiveness.

In accordance with the National ICT policy, The National Universities Commission (NUC) whose mandate is to regulate and ensure delivery of qualitative education in the Nigerian University System (NUS) has recognized the pertinent role ICT plays in achieving its mandate. Therefore, the NUC has set out this ICT policy as an underlying guideline for proper, efficient and effective use of ICT to succeed in achieving its mission and objectives.

This ICT policy would articulate policy guidelines and framework as programs of action to be adopted by the NUC to guide the implementation and use of ICT in all Nigerian Universities.

1.1 VISION

To further improve the standards of Nigerian Universities and subsequently make them centers of excellence in Africa where the potential of ICT is harnessed to serve as a catalyst for effective teaching, research and innovation.

1.2 STATUS OF ICT IN NIGERIA

1.3 APPLICATIONS OF ICT TO EDUCATION

In Nigeria, there is increasing awareness for the use of Information and Communication Technologies (ICTs) in teaching and learning. ICTs, which include radio and television, as well as newer digital technologies such as computers and the Internet—have been touted as potentially powerful enabling tools for educational change and reform. When used appropriately, different ICTs are said to help expand access to education, strengthen the relevance of education to the increasingly digital workplace, and raise educational quality by, among others, helping make teaching and learning into an engaging, active process connected to real life. We can identify at least five levels of technology use in education: presentation, demonstration, drill and practice, interaction, and collaboration. There are a number of ICT applications which aid learning and teaching, some of which are discussed below

1.3.1 TELECONFERENCING

Teleconferencing refers to "interactive electronic communication among people located at two or more different places." There are four types of teleconferencing based on the nature and extent of interactivity and the sophistication of the technology:

- Audio-conferencing
- Audiographic conferencing
- Video-conferencing; and
- Web-based conferencing.

Audio-conferencing involves the live (real-time) exchange of voice messages over a telephone network. When low-bandwidth text and still images such as graphs, diagrams or pictures can also be exchanged along with voice messages, then this type of conferencing is called audiographic conferencing. Non-moving visuals are added using a computer keyboard or by drawing/writing on a graphics tablet or whiteboard.

Videoconferencing allows the exchange not just of voice and graphics but also of moving images. Videoconferencing technology does not use telephone lines but either a satellite link or television network (broadcast/cable). *Web-based conferencing*, as the name implies, involves the transmission of text, and graphic, audio and visual media via the Internet; it requires the use of a computer with a browser and communication can be both synchronous and asynchronous.

Teleconferencing is used in both formal and non-formal learning contexts to facilitate teacher-learner and learner-learner discussions, as well as to access experts and other resource persons remotely. In open and distance learning, teleconferencing is a useful tool for providing direct instruction and learner support, thereby minimizing learner isolation.

1.3.2 E-learning

Although most commonly associated with higher education and corporate training, e-learning encompasses learning at all levels, both formal and non-formal, that uses an information network—the internet, an intranet (LAN) or extranet (WAN)—whether wholly or in part, for course delivery, interaction and/or facilitation. Others prefer the term online learning. Web-based learning is a subset of e-learning and refers to learning using an Internet browser (such as Internet Explorer). E-learning is comprised of all form teaching and learning that involve the use an electronic medium. The information and communication system, whether networked or not, serve as specific media to implement the learning process. The term is still most likely be utilized to reference out-of-classroom and in-classroom educational experiences via technology, even as advances continue in regard to devices and curriculum. It is essentially the computer-enabled transfer of skills and knowledge. This is especially very useful in distance learning programmes.

1.3.3 Telecollaboration

Online learning involving students logging in to formal courses online is perhaps the most commonly thought of application of the Internet in education. However, it is by no means the only application. Web-based collaboration tools, such as email, message boards and real-time chat connect learners to other learners, teachers, educators, scholars and researchers, scientists and artists, industry leaders and politicians—in short, to any individual with access

to the Internet who can enrich the learning process. The organized use of Web resources and collaboration tools for curriculum appropriate purposes is called telecollaboration. Judi Harris defines telecollaboration as "an educational endeavour that involves people in different locations using Internet tools and resources to work together. Much educational telecollaboration is curriculum-based, teacher-designed, and teacher-coordinated. Most use email to help participants communicate with each other. The best telecollaborative projects are those that are fully integrated into the curriculum and not just extra-curricular activities, those in which technology use enables activities that would not have been possible without it, and those that empower students to become active, collaborative, creative, integrative, and evaluative learners.

1.4 STATEMENT OF PURPOSE

This policy seeks to guide developers and users of ICT resources on appropriate standards to be adopted by Nigerian Universities. Its objectives include to:

- Provide guidance in developing a pervasive, reliable and secure *communications infrastructure* which shall conform to recognized International standards and support all services in line with the priorities of the individual Universities;
- Provide a framework for development and management of ICT *network services* that shall ensure the availability, enhanced performance, security, and reduce the cost of running the ICT infrastructure;
- Establish information and implement *security* requirements across the Universities' ICT infrastructure;
- Provide a framework, including guidelines, principles and procedures for the development and implementation of ICT (*Software Information System)* projects in Nigerian Universities;
- Guide the handling of *organizational information* within the ICT departments and the Universities as a whole by ensuring compliance with applicable statutes, regulations, and mandates for the management of information resources; and thereby establish prudent practices on *Internet* and the *University Intranet* use;
- Uphold the integrity and image of the Universities through defined standards and guidelines for ensuring that the content of the Universities' *websites* is accurate, consistent and up-to-date;

- Serve as the direction pointer for the ICT departments' mandate in *supporting users*, empowering them towards making maximum use of ICT services and resources and specifying the necessary approaches;
- To guide the process of enhancing user utilization of ICT resources through proper *training*
- Outline the rules and guidelines that ensure users' PCs and other *hardware* are in serviceable order, specifying best practices and approaches for preventing failure.
- To provide a paradigm for establishing the Universities' *database service* that will support groups working on systems development, production and any other groups;
- Inform departments carrying out projects financed in whole or in part by the NUS, of the arrangements to be made in *procuring* the goods and services for the projects.
- Finally, to promote widespread use of ICT applications in faculties and departments for efficient teaching, research and learning.

1.5 SCOPE OF THE POLICY

This Policy applies to any person accessing, developing, implementing and/or using ICT based information and resources owned, managed, supported or operated by or on behalf of the Nigerian Universities. Thus, this policy covers all Universities staff, students and any other organization accessing services over Universities ICT resources as well as persons contracted to develop, repair and/or maintain Universities ICT resources.

1.6 APPROVAL OF POLICY DOCUMENT

This document stipulates policy guidelines and describes critical areas in the development and application of ICT in Nigerian universities. It lays out a roadmap in terms of the NUC's mission and strategy for guiding and supporting Nigerian Universities by using ICT as an enablement tool. The ICT policy would form the basis for the development of ICT in all Nigerian universities over the next five (5) years. The policy was developed in the NUC and was formally adopted by the members of the management on the _____2019. The policies are also dynamic and open to reviews in order to meet the changing uses of the ICT structure within the NUS. However, such changes should only be made by the NUC. It is recommended that the review process should start two (2) years before the expiration date of the current document.

CHAPTER 2

2.0 NETWORK DEVELOPMENT AND MANAGEMENT POLICY

2.1 Introduction to network policy

The information and communications infrastructure at the various Nigerian Universities have grown into complex networks over which education, research and business of the Universities are conducted. It is thought that the network should integrate voice, data and video, to form 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.

The Universities' network functions shall be broken down into the following areas:

- University ICT Infrastructure Development
- University Backbone
- Campus Local Area Network
- Inter-Campus Access
- Private Access to ICT facilities
- Connection to and usage of ICT facilities
- New or changed use of ICT equipment
- Monitoring of network performance.

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

2.2 Objectives of network policy

The objective of this policy is to establish a comprehensive and uniform Network Development and Management policy that manages ICT infrastructure for the various Universities. This policy would lay out the arrangements and responsibilities for the development, installation, maintenance, and use and monitoring of the University's ICT networks to ensure that the networks are sufficiently adequate, reliable and resilient to support continuous high levels of activity.

2.3 Scope of network policy

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

2.4 General network policy

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

2.5 Universal availability

- The University network shall form part of the general fabric or infrastructure of the University.
- The University network will be designed and implemented in such a way as to serve those located at the University campuses and, to a lesser extent, those located elsewhere.
- The ultimate goal is that every building within the University in which research, teaching or support activities take place should be connected. And every member of the University should have capability to access the University ICT infrastructure.
- There will be one coherent network supporting access to all general information services provided to the University members. There may be separate private networks where they are warranted.

2.6 Reliability

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

2.7 University ICT Infrastructure Development

2.7.1 Development plan

The ICT departments at the individual Universities are expected to prepare a network development plan.

This plan should advise on appropriate developments aimed at ensuring the adequacy of the University's ICT infrastructure in the future. This plan will also take account of the University's strategic plan; usage and demand patterns; technological change; security; management and cost implications.

2.7.2 ICT network provision in new and refurbished buildings

- Network provision for new and refurbished buildings shall be made in accordance with the specification published from time-to-time by the ICT departments.
- Where the Network requirements are of specialized nature the ICT Director concerned shall seek further guidance from the network manager.
- All new buildings to be erected in the University shall incorporate an appropriate structured data wiring system to allow connection to the University network.

2.8 University Backbone

The Network Backbone for Universities shall comprise inter-building cabling systems with one or more "Gateway" interfaces at each building or its immediate environment. This would enable the network(s) within each building connect to the Backbone.

2.8.1 Structure of University backbone

- Single or multiple buildings shall be connected to one another through the University Network Backbone.
- The ICT Units shall be in charge of the planning, installation, maintenance and support of the University Network Backbone.
- Connection to the University Network Backbone shall be approved by the Director of the ICT department.
- The ICT Units shall strictly adhere to relevant network standards and hence maintain such records. In addition the Units shall constantly keep abreast of developments in these standards, both nationally and internationally.

- The University Network Backbone at any particular point in time shall be charged with the aim of facilitating the traffic flow between connected buildings or networks.

2.9 Campus Local Area Networks (LANs)

The Campus LANs comprise of all the necessary wiring, cabling and related network equipment within existing buildings that connect to the LAN gateways. These LAN gateways are used to channel traffic to and from the University Network Backbones.

2.9.1 Structure of Campus LANs

- The network (s) within each building shall be set up with provision made for a point of connection to the University Network Backbone. In cases where this is not immediately possible, multiple building gateways may be considered.
- All network protocols used for communicating through the gateway and networks in existing buildings must use approved configuration parameters including approved network identifiers.
- Networks in existing buildings which connect to the University network shall meet overall University network security and management requirements.
- In cases where challenges arise in connecting any building to the University Network Backbone, the Head of the ICT Unit shall consult with other stakeholders on the allowance, usage and subsequent inclusion of alternative configurations.

2.10 Inter-campus connections

The Inter-campus connections shall consist of the necessary services and related equipment that would allow access to the central University backbone by a remote campus, remote university office and other institution for collaboration and resource sharing.

2.10.1 Structure of inter-campus connection

- Wherever feasible, the network(s) within each remote site shall be set up with provision for a point of connection to the University Network Backbone. In cases where this is not immediately possible, multiple building gateways may be considered.
- Network protocols used for Inter-campus connections must use approved configuration parameters including approved network identifiers.

- Inter-campus links connecting to the University Network Backbone shall meet overall University network security and management requirements.

2.11 Private networks

Every Department or unit may install networks independent of the University Network Backbone provided that the installation adheres to the University policies and standards for installation and it does not interfere with the University Network.

2.11.1 Structure of private networks

- The ICT department shall provide Campus Gateways for private departmental networks where the private network caters for all the building occupants.
- Private departmental networks may extend between buildings.
- The ICT department may provide links for these networks but any extra expense incurred above the University Network Backbone requirements shall be charged to the Department.

2.12 Access to ICT facilities

2.12.1 Communications rooms, cabinets and ICT network equipment

- It should be ensured that all communications rooms and cabinets shall be locked at all times.
- Access to communications rooms and cabinets, and interference with ICT network equipment is strictly prohibited to non ICT staff members.
- Except in cases of an emergency, access to communications rooms, cabinets and ICT network equipment shall be restricted to designated members of staff of the ICT department. Any necessary access must have prior written consent of the Director of the ICT department.

2.12.2 Access in an emergency

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

- During the course of an emergency e.g. fire or any other disaster, security staff and/or staff of the Estates Department and/or the emergency services may enter these areas, without permission, to deal with the incident.

2.12.3 Contractors

- Prior approval or written authorization must be sought from the Director if ICT by all contractors providing ICT network services.
- Contractors shall conform to and observe any specific access conditions which apply within the areas in which they will be working. These access conditions include, that in all cases University ICT personnel shall accompany contractors working in main server rooms.

2.12.4 Installation of cabling

Every electrical power cable installation and changes in facilities housing ICT equipment shall be approved and managed by the Estates Department in consultation with the Director ICT in writing.

2.12.5 Network equipment

- The installation and maintenance of active network equipment including hubs, switches and routers connected to the University's network shall be carried out only by authorized ICT staff members.
- In cases where the ICT Head grants permission to other personnel besides the authorized ICT staff to maintain and install hubs and switches, such permission will in every case exclude the point at which these hubs and switches connect to the University's network infrastructure.

2.13 Connection and Usage of ICT facilities

2.13.1 Connecting to the ICT network

- Initial connections of desktop services equipment to the ICT network can only be made by authorized members of staff.
- All connections to the University's ICT networks must conform to the protocols defined by the University's ICT policy and with the requirements that apply to Internet Protocol (IP) addresses.

- Individual computer workstations connected to the ICT network should not be used to offer other services like acting as servers without the prior consent of the Director of ICT.

2.13.*2* External access to servers on the backbone network

- Where specific external access is required to servers on the backbone network, the Director of the-ICT department shall ensure that this access is strictly controlled and limited to specific external locations or persons.
  - Compliance with access arrangements as stipulated in this ICT Policy shall be monitored by the Director of ICT.
  - Sanctions and penalties shall be carried out in cases of abuses of or failure to comply with these arrangements shall result in immediate restriction to or disconnection from the network.

2.13.3 Domain name services

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

2.13.4 Electronic mail

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

2.13.5 Suspension and/or termination of access to ICT networks

A. University Employees

- A staff's access to the University's ICT networks will be revoked automatically:
  - **i.** at the end or termination of his or her employment or research contract;
  - **ii.** at the request of his or her Dean of Faculty/Head of Resource Centre/Head of Department or School or Head of Unit;
  - **iii.** Where he or she has breached these regulations.
- The University reserves the right to terminate or temporarily place an embargo on staff's access to the University's ICT networks where the user is suspended or awaiting the results of an investigation.

- Changes in employment status must be communicated as soon as possible to the Administration Registrar so that appropriate actions can be taken as regards the email and account status of these users, either to suspend or delete them as appropriate.

B. Students leaving the University

The Department of ICT shall be regularly updated with the records and information of students leaving the University so their accounts can be disabled or deleted.

C. Procedures on Restriction of Use

- Any breach of ICT policies shall be reported or communicated in writing to the Director of ICT.
- 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.
- Upon receipt of any such complaint, the Director of the ICT department shall classify the complaint as "serious" or "non-serious." A "non-serious" complaint shall be defined as a breach of policy which does not subject the University to a cost nor any risk.
- When a complaint is classified as "non-serious," the Director, ICT is authorized to impose some form of penalty.
- When a complaint is classified as "serious," the Director, ICT shall refer the complaint to the ICT Committee for appropriate action. The possible penalties may be any one or a combination of the following:
  i. Notification of the suspension will be communicated to the relevant Dean and/or Head of Department or Section;
  ii. Suspension of the account shall be for a minimum period of four weeks. Formal approval of the relevant Dean and/or Head of Department or Head of Section and a signed undertaking to abide by the Rules of Use shall be required before reinstatement of the account.
  iii. Permanent disabling of the account shall be taken, where the severity of the offence warrants such action.

iv. Accounts may be reinstated before the end of the suspension period where either the student or staff presents information to the Director of ICT, which indicates that he or she was not involved in the transgression of the Rules of Use, or the Dean and/or the Head of Department or Head of Section requests the account be reinstated for course related work only (e.g. completion of an assignment). In this case the student or staff is required to sign an undertaking to abide by the Rules of use.

v. A system administrator responsible for supporting users can make a recommendation to disable an account to the Director of ICT. The Director of ICT shall review the request and if there is considered to be, on the balance of probability, a transgression of the ICT Rules of Use, the account shall be suspended.

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

vii. Users should note that suspension of access to ICT facilities also includes access to the terminal server password access, and as such dial-up modem access will be disabled where a user account is suspended.

viii. Staff and students whose access has been suspended shall have the right to appeal in writing to the ICT committee set up by the Director of ICT.

2.13.6 Internet Protocol (IP) addresses

- The Communications and Networks Head is required to maintain a central record of IP addresses and may remove inactive IP addresses after six months.
- The Communications and Networks Head of the ICT department shall plan and allocate Blocks of IP addresses to different network segments and notify the relevant ICT officers.
- The ICT officers, after distribution of the allocated IP Block shall notify the Communications and Networks Head who shall in turn update the IP address master record.

- All computers connected to the ICT network shall have unique IP addresses assigned to them.
- The IP addresses assigned to equipment shall be recorded visibly on the casing of the equipment.

2.13.7 Inventory Control

In order to maintain proper audit and inventory control, the ICT officer shall be required to record in their local equipment inventory records the IP address assigned to each item of equipment for which they are responsible, together with the location of such equipment.

2.13.8 Connection of privately owned computers to the University Network

Students and members of staff are only allowed to connect their personal computers or workstations to the University network after it has been certified that their systems meet the minimum specification determined by the Director of ICT and that it poses no risk to the University network.

2.13.9 Additional or changed equipment

- Due advance notice shall be given to the Director of ICT of any plan to add, replace or to relocate desktop equipment that are connected or that may require connection to the University's ICT network.
- The Director of ICT shall assess the likely impact on the University's ICT networks of the proposed change. The Director of ICT shall give approval for the proposed change only where appropriate adjustments can be made to accommodate any effects on network traffic that this change may cause.

2.13.10 External data communications

- Express permission and written consent must be sought from the Director of ICT before any external connections to the University's Network is made.
- It must be ensured that every external data communications is channelled through the University's approved links.
- The use of modems, leased or other means of access to other networks on equipment located on premises owned, managed or occupied by the University that are linked to the ICT network infrastructure, is prohibited, unless a proposal and justification for such connection has been authorized in writing by the Director of ICT.

2.13.11 Web filtering

In order to ensure efficiency and high availability of internet services to all users, the director of ICT shall ensure all web-based and non-web internet traffic, including MP3 traffic and other high bandwidth intensive services that may not have direct educational or research value are adequately filtered, where and when necessary in conformity with the ICT Policy and relevant ICT Guidelines.

2.14 Monitoring of Network Performance

The Head of the Network Unit in the ICT Department shall ensure regular monitoring of the ICT network performance and usage. Periodic reports and documentation shall be maintained.

2.15 Software development and acquisition procedure

The purchase of Open source Software shall be encouraged in a bid to reduce cost and engender creativity.

In addition, as a way of encouraging ingenuity and skills development within the University system, every University shall be encouraged to develop their own in-house Bespoke Software. The sharing of Enterprise-wide Software between Institutions should also be encouraged in a bid to reduce costs.

The following guidelines shall be followed when Software is to be procured or developed within the University;

- The introduction of a new system will start with the identification of the need. This will be in the form of a Development Request / Requirement analysis with generalised information of requirements that should be forwarded to the IT Services Software Development.
- In the case of a costly and/or complex system, an outline Investment Appraisal will be required that should clearly detail why a new system should be introduced, give an indication of the resources required to deliver and how the system will be supported after introduction.
- Priority will be given to systems, which deliver benefit to the whole University as opposed to purely local solutions. IT Services in partnership with the proposer will then work to

identify the correct solution starting with checking the availability of a suitable application on the market.

2.16 Data Protection Policy

2.16.1 Disclosure of Information/ information in transit

- There must be procedures put in place to notify staff and students of each University of the reasons their information will be held in the University's database, how it will be used and the Institutions or Establishments that they might share their Information with.
- The Personal data obtained of staff and students must be adequate, relevant and not excessive in relation to the purpose(s) for which they are been requested.
- The Staff and students of each Institution have the right to access data or information held concerning them.
- Access to an individual's personal information should not be given to persons other than the individual concerned or other authorised personnel.
- Some disclosures of information may occur because there is a statutory requirement upon the University to disclose e.g. with a Court Order, for medical purposes or to aid Police investigation because other legislation requires disclosure.
- In instances where information or data need to be transported, only reliable transport couriers with adequate security and sufficient packaging policies should be used.

2.16.2 Data and Information Accuracy

The *accuracy* and *correctness* of Data and Information on staff and students must be ensured at all times by carrying out periodic updates of staff and student information.

2.16.3 Information Retention

- Any *transient* data or information (i.e. information not in the **main** record) of any student or staff must have a maximum life span after which it must be deleted or destroyed from whichever medium it is stored. Individuals will reserve the right to make formal complaints or take legal action against any institution that keeps transient information about them beyond a predetermined number of years.

Chapter 3

3.0 Security and Business Continuity Management

In order to ensure that the incidence of unauthorized access to computer systems and infrastructure is completely prevented or reduced to the barest minimum, and to ensure business activities of the institution are not obstructed at any giving time. The following guidelines is to be enforced:

3.1 Physical Access Control

- The Chief Information Officer (Director, ICT) or any personnel filling the same post in all Universities shall ensure that only authorized staff or personnel are granted access to server rooms, computer labs and other major ICT facilities.
- The rooms or spaces housing these equipments must be adequately secured at the doors and windows and the keys or access codes to these rooms should reside only with the Director, ICT.
- An Asset register is to be maintained by all units in the ICT Department to keep track and take inventory of all hardware and software in the Department and a central register is to be maintained by the ICT Department to keep inventory of the Computer equipment in the University.
- All ICT equipment must be labelled appropriately for identification.
- All entrances to secured areas must be appropriately labelled “Only Authorized Person is allowed”.
- Access controls and security surveillance equipment like CCTV cameras shall be installed in secure areas to prevent unauthorised access, theft and tampering with computing facilities both during and after working hours.

3.2 Safety Rules

- Adequate safety and Audit policy must be put in place by the ICT Department in each University to prevent anticipated threats that may damage physical devices
- Installation of newly purchased equipment must be carried out only by authorised personnel after due consultation of the installation manuals of such equipment. Any

damage or malfunction that may result from non-adherence to this guideline will attract a penalty.

- The Department of ICT will ensure that electrical devices are adequately protected from power surges by installing Uninterrupted Power Supply (UPS) and surge protection devices wherever practical.
- Provisions should be made by the ICT Department to protect both indoor and outdoor equipment from fire, water and physical damage.
- All ICT resource and infrastructure shall be ergonomically correct and shall not entail physical or physiological impact or damage for user.
- Measures must be taken to ensure that all information and software are removed from redundant hardware before it is retired or decommissioned.
- Expired confidential information stored on paper must be shredded or held in a secure area in preparation for incineration.

3.3 Logical Control and Access to the Internet:

Access to the University networked facilities (Local Area Network) shall be controlled through the following:

- All staff and students shall be provided with a username and password to be able to access both the computer systems and the internet.
- All traffic passing through the firewall must be capable of being logged and audited.
- The ICT Department shall maintain control over data packets and connection requests by means of a centralized firewall that will adequate filter data traffic.
- All Users (staff and students) are not allowed to view or visit sites with offensive materials (e.g. pornographic sites, sites used to spread hate and racial or religious intolerance). Defaulting users should have their username and passwords disabled.
- All users must not download or upload offensive material on the University Network.
- All users are prohibited from using the computer facilities to write or spread any form of malware or spam mails either in the form of viruses, Trojans, worms etc.

3.4 Network Control:

- In order to have any third party network connections to the University network, clearance should be sought from the Department of ICT.
- Express permission need be sought from the Chief Information to connect any equipment (Computers, workstations and Laptops, PDA and smartphones), and/or removable device such as USB drives, memory sticks, CD ROMS, and DVDs to the University Network.
- Adequate measures must be put in place to protect the University network infrastructure from email spam, intruder or hackers, virus, worms and other disruptive software.

3.5 User Responsibilities

- All users should take reasonable care to safeguard the ICT equipment in their possession.
- Users must take all reasonable steps to ensure that computer equipment in their possession or under their control are protected at all times against theft, accidental or deliberate damage.
- The Universities ICT facilities should only be accessible for use by University staff and students, all Visitors and guests desirous of use must obtain permission from the User Support Unit.

3.6 Antivirus

- The Department of ICT will ensure adequate protection of all computers and other devices connected to the network by installing approved industry standard Antivirus Software. Under no circumstance should the installed Antivirus software be a Pirated copy. Adequate sanctions and penalties shall be meted out to erring Departments and Universities.
- For computers not connected to the network, the officer in charge at the Department should liaise with the Directorate of ICT to have updates done regularly.
- All data whose source is not from within the department and any external software shall not be installed or executed or used in any other fashion unless it is scanned for viruses and any other malware using the University's Antivirus software.
- In the cases where a viral activity is noticed in any of the computing systems or facilities, users should call the attention of ICT helpdesk or any other ICT technician available.

3.7 Backup and Disaster Recovery

- Provision must be made by all Universities to have their Information and Data backed up in a safe, secure and fireproof data safe. Preferably in a separate building or location.

3.8 Resource Management - Physical

3.8.1 Procurement

- The NUC shall assist the Universities with preparation of technical specifications for the purpose of procuring goods and services related to ICT whenever need arises.
- The NUC shall also assist the Procurement offices of Universities in cases of emergencies to identify reputable companies or registered providers to reduce any delay in procurement.

3.8.2 Replacement of Infrastructure

The life cycle of the infrastructure is dependent on the type procured by the University. On average, hardware shall be replaced after every five years depending on the availability of funds. While for software the life cycle is dependent on the release of newer versions and shall be upgraded accordingly, depending on availability of funds.

CHAPTER 4

4.0 MANPOWER DEVELOPMENT AND CAPACITY BUILDING

4.1 Introduction

It is essential to ensure that all students and staff (academic, administrative, support and managerial) of Universities are given the required ICT training and that this is done on a continual basis in order to equip beneficiaries with the requisite skills to fully exploit the ICT environment in the NUS.

4.2 ICT Literacy

It shall be mandatory for all University staff and students to be literate users of ICT services provided by the ICT Units. As such, all members of staff shall be regularly trained on the latest ICT technologies in line with the demands of their job functions. In particular, academic staff shall be given training aimed towards the proper usage of ICT infrastructures for teaching and research purposes.

These trainings shall be carried out by the Universities in collaboration with the NUC. Therefore, training shall focus on equipping the staff and students with effective skills making them capable of exploiting provided ICT resources.

4.3 Training Modes

External Training: On the occasion that training is not possible within the University, external ICT training shall be carried out by the NUC in response to needs of such Universities as may be assessed from time to time.

Internal Training: ICT training of universities staff and students is to be carried out on a continuous basis and shall be conducted on the campuses of the individual universities.

In addition to this, the Universities shall be responsible for the following:

I. Creating organizational (trainer capacity, training management) and technical (practice lab and computer based training tools, self-paced training mode) conditions assuring continuous in-house training capabilities in the long-term.

II. Ensure and require that all students and staff are trained on a continuing basis to equip them with the requisite skills in their different disciplines.

III. Develop university wide and global training/learning networks based on academic interests groups and research collaborations.

IV. Establish appropriate common infrastructure and software responsive to academic needs through designated centralised unit.

4.4 Trainees/ Trainers

- The NUC shall jointly with Universities' departments nominate trainees (core ICT staff) for external ICT training when the need for such training arises.
- The general staff (teaching and non teaching) should be regularly trained on the basic IT skills and competencies needed to access the University Network.
- As regards to training, NUC should give consideration to those Universities that are proactive in the use of their ICT facilities
- An individual shall be appointed in every University who shall be recognised as the Director, ICT (DICT) or any other designation as the University deems fit.
- The Director, ICT shall jointly with the ICT departments in their various campuses, and in response to assessed needs nominate trainees and a copy of this list shall be forwarded to the NUC. The number of trainees shall be as targeted in the Strategic Plan for the University.
- The Core ICT staff should consist of individuals that possess competencies and qualifications in at least one of these unit or areas; Network Management, Software development and management, Content Development, maintenance and Help desk support, Electronic archiving and management, and database administration.

4.5 Training Resources

The NUC shall in liaison with either the Head of ICT Units of Universities or their Vice Chancellors identify appropriate trainers for training of staff and students in the University communities. These shall be as demanded by the needs of the institutions. The ICT Units shall liaise with the various departments in their institutions to provide the necessary resources to facilitate training.

Importantly, the trainees must be a mixture of people with relevant qualifications in the various areas which are to include; Network Management, Software Development and Database Management, Maintenance and Helpdesk Support, Content Development and E-Learning, Web Administration and Development, and Electronic Archiving and Management.

4.6 Infrastructure

It shall be the University's responsibility to select, source and acquire any appropriate infrastructure and/or software in accordance to perceived needs of such institutions through its Director, ICT.

During training, top priority shall be given to physically challenged individuals and as such, all facilities deployed to Universities for the sake of training shall be accessible to those with disabilities.

4.7 Sustainability

The NUC shall oversee and promote sustainability of this policy by ensuring that the Universities fulfill the following;

i. Provide funding for acquisitions and maintenance of equipment, and training;
ii. Regularly updating of computers and related equipment according to their life cycle
iii. Networking is to be a continuous process as new building facilities for academic and administrative purposes spring up.
iv. Acquiring ICT hardware and software from a common source to reduce cost and enable easy maintenance.
v. Periodic training of ICT staff to upgrade their knowledge in modern trends.
vi. Setting up of maintenance workshops.
vii. Holding regular workshops and conferences to ensure that the ideas on improvements are constantly exchanged.
viii. During accreditation, both Departmental and Institutional, the level of ICT usage in service delivery (teaching, learning, administrative and community service) will be considered as major scoring point.

4.8 SUPPORT

On the occasion where additional support is required, the NUC shall provide such assistance to Universities in the form of informed help on academic and administrative computing and information to all categories of staff and students of the affected University.

Consequently, support for training on computing services shall be provided by the University with strong user support to ensure integrated access to new information services as they may arise. The level and type of support in the University shall be reviewed continually to allow the introduction of new activities. These activities shall properly reflect the changing needs of the Universities.

Furthermore, appropriate incentives and support packages shall be made available to Universities which shall be transmitted to their faculties and staff as encouragement in the creative use and application of ICT for teaching, research and service.

4.9 Acknowledgment of training

The ICT Units shall issue certificates to staff and students on successful completion of necessary training courses and examinations.

CHAPTER 5

5.0 EQUAL OPPORTUNITIES POLICY

5.1 Accessibility:

This portion of the policy is concerned with ensuring that physically-challenged individuals have access to Information and Communications Technology (ICT), given the relatively large number physically-challenged persons in the country especially those within tertiary schooling age (17 – 30 years).

In view of the foregoing, it is therefore pertinent that the ICT policy governing the Nigerian University system make adequate provision for physically-challenged individuals.

5.2 Guidelines

- Incorporation of accessibility into all learning curricula in Institutions involved in the training of students for web design.
- It should be ensured that any form of training and capacity development organised by the Universities incorporate Accessibility principles in their teaching resources.
- All Universities while procuring Hardware for their ICT departments must dedicate a predetermined percentage of their Purchase to Assistive accessories such as Screen readers, Braille Display and Optical recognition software that could help disabled individuals have access to the contents on a web site.
- In the Purchase of Software, provisions must be made to procure Software that is adapted to the needs of disabled students and lecturers.
- In the design of websites, accessibility principles must be incorporated to ensure that the information on such sites is accessible to disabled individuals. These principles include;

    i. Provision of text equivalents for all non texts objects on the page to enable functionality of accessories.

ii. Provision of a site search.

iii. Descriptive titles should be used on every page.

iv. Design pages to enable users customize it.

v. Avoid the use of colours only to indicate things on the web.

vi. All Computer laboratories must have at least one specially trained IT Professional that can attend to the need of students with special needs and the disabled.

5.3 Distance Learning or off site student Guidelines.

- For students engaging in Distance Learning courses, it must be ensured that Lecture notes and pre recorded lecture videos are available online.
- It should be ensured that provisions are made for students to submit their Coursework and Assignments online.
- Provisions must be made for students to have unfettered correspondence with their Lecturers via emails, school intranet or Departmental Portals. This correspondence should include ability to apply for test rescheduling, extenuating circumstances, review and questions on projects and coursework.
- Students must have access to Library resources and e-journals without having to be physically present on the school premises.
- Students must be able to view test scores and lecturer's comments on the Departmental Portal or Intranet.
- Every Lecturer and Teaching staff must have access to a computer and internet service either at home or while on the school premises.
- Each Department should have a well stocked Computer Laboratory accessible to all registered students during the Term time.

5.4 Gender / Ethnic / Religious issues.

- It must be ensured that access to University ICT resources is not based on gender, religious and/ or ethnic considerations.

- It must be ensured that the posts of the Chief Information Officer or any other professional post is not reserved for any particular gender so long as the individual possesses the pre requisite qualification.

CHAPTER 6

6.1 Maintenance of ICT Equipment

6.2 Introduction

The Maintenance Section of the ICT Units of Universities is important and shall cater to users of the systems by ensuring timely maintenance and/or repairs of all equipments.

6.2 Operational Maintenance

I. At the first level of maintenance and support, users shall resolve basic problems as they may occur. This repair does not include dismantling or having access to the equipment by opening.

II. If such issues cannot be resolved, maintenance and support may advance to the second level. At this stage, the Head of ICT Unit or any assigned officer with the requisite competencies in each campus shall offer support to the users.

III. If issues persist, the third level shall involve introducing specialist Maintenance Engineers, which could include consultants and/or external professionals.

IV. The fourth and final level shall involve the specialist Maintenance Engineers to work in liaison with vendors, suppliers and hardware manufacturers to troubleshoot, repair and/or replace any faulty equipment.

6.3 Hardware Maintenance

The Universities ICT Units shall maintain and support all hardware/peripherals (which may include desktop computers, laptop computers, printers, scanners, digital cameras, projectors, power backup systems and network equipment) which are constantly required by students and staff for use in their offices, computer rooms, libraries, laboratories and lecture theatres to perform their daily tasks. Such users of the hardware shall strictly adhere to the ICT procurement policy for the hardware in order to ensure proper usage and guarantee support by the ICT Unit.

6.4 Privately owned ICT equipments/peripherals

The Universities ICT Units shall not be responsible for the replacement, repair and/or upgrade of privately owned equipment/peripherals.

6.5 Computer Systems/Peripherals

As regards ICT equipment's, departments/faculties of Universities who purchase their own equipment, with the aid of their ICT Units, shall be responsible for the following:

I. Providing the appropriate operating environments such as floor space, air conditioning, ventilation, backup power supply, etc.

II. Overseeing all necessary Installations and administration of ICT equipments.

III. Ensuring routine maintenance and upgrade of equipments.

IV. Taking full responsibility for all expenses incurred during repair, maintenance, and upgrade of equipments.

V. Ensuring full compliance with the NUC's Procurement and Disposal Policy concerning old and obsolete equipments.

VI. Full compliance with the NUC's security policy, including installation and regular updates of all anti-virus software.

In addition, any supply of spare parts to support such ICT equipments and peripherals shall be the solely the responsibility of the Universities.

6.6 Tools and equipment

Universities shall acquire and continually stock all necessary support tools for maintaining their ICT equipments. These tools shall be maintained centrally at the ICT Units.

6.7 Repair Centres

Every University shall have a designated repair facility. This facility shall take the form of a designated room/building/space especially reserved for the purpose of carrying out all necessary hardware repairs and maintenance on ICT equipments. The ICT Unit of the University shall have custody of such facility.

6.8 Preventive maintenance

The ICT Units are to draw up schedules for regular servicing and maintenance of all equipments. The frequency and methods of servicing of ICT equipments shall be carried out

according to the recommendations of the manufacturers of such equipments. However, where justified by the case, service shall be provided on the basis of request.

6.9 Outsourced Servicing Agreement

Equipment not able to be supported by ICT Units shall as far as possible be placed on maintenance contracts with external bodies.

6.10 Obsolescence of Equipments

ICT equipment shall be declared obsolete according to the recommendations of the manufacturer. The ICT Units' repair and maintenance teams shall periodically conduct maintenance to identify, retire and replace all equipment categorized as at "end-of-life."

6.11 Warranty guidelines

The repair and maintenance teams of ICT Units shall keep accurate records of the warranty of individual equipments and use such information as and when needed to operationalize the warranty and/or guarantee for such equipments.

Appendix

The procedures and guidelines contained in this appendix, give details of the minimum

Specification required to develop a new, functional ICT Department.

Infrastructure

- All buildings should make provision for LAN cabling. If buildings are still at construction stage, the LAN cables should be enclosed in trunks or pipes and sealed in the walls.
- Power infrastructure and alternate sources; also include surge protection and redundant provisioning at the design level.
- Provision should also be made for fibre cabling crossing during road construction (for future development and expansion).
- Campus wide LAN preferably using fibre between buildings in addition to wireless technology.
- Internet access using fibre or Microwave Radio. Bandwidth to be calculated based on the number of PCs. Ideally, 512/256kbps dedicated for each 50PCs.
- Access computers for students in access labs. UNESCO recommended ratio 5:1 (students: PCs). A more realistic ratio in our case may be 20:1
- Data center with adequate power back up for 24/7 operations.
- Staff access computers. At least 2:1 ratio.
- At least one training laboratory with about 50 computers for the training of staff.

Human resources/ capacity

- Qualified System analyst with proven integrity should be made part of the project team.
- Within the first 2 years of licensing, the University should make plans to join the NgREN (Nigerian Research and Education Network).
- Equipment should be the popular brands instead of generic ones.
- Determine the size of required bandwidth.
- ICT governance structure: ICT Committee, ICT Department, ICT Management Committee comprising of Heads of units.
- Every teaching and admin staff should be computer literate i.e. have at least basic computer appreciation. Every academic staff should be able to use the internet, communicate via emails,

handle multimedia facilities like whiteboards, projectors, etc and should be able to make presentations using PowerPoint as well as other office tools.

- All science and Engineering students and staff should be able to use at least one electronic lab tool relevant to their discipline e.g. MATLAB, AUTOCAD.
- All accounting/ finance processes must be automated. The University can acquire Applications like Sage, Quickens, and Peachtree etc.

  There should be a policy of trade-in of computers within 3 to 5 years of use. A few of each mode should be retired into the computer/ electronics engineering lab for students' practices.

  Content
- A University website
- Internal Email server.
- A DHCP Server to ease the problem of IP address conflicts.
- A DNS server. It helps to save on the bandwidth of resolution is done internally.
- Firewall to protect against intruders.
- Campus wide antivirus license.
- Bandwidth management Solution such as SQUID etc. This is vital to monitor and manage the scarce bandwidth.
- Automated financial record system to include payroll and general ledger required.

University should develop in-house competences to manage databases rather than outsource them