Release V1.2

FRAMEWORK AND GUIDELINES FOR INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) ADOPTION IN TERTIARY INSTITUTIONS

National Information Technology Development Agency (NITDA)

August, 2019

Release V1.2

Change History

S/N	Author	Version No	Release Date	Change Details	By Who
1.	NITDA	1.0	May, 2019	First Review	NITDA
2.	NITDA	1.1	May, 2019	Second Review	Stakeholders
3.	NITDA	1.2	July, 2019	Second Review	NITDA & Stakeholders

Metadata of the Regulation

S/N	Data Elements	Values
1.	**Title**	Framework and Guidelines for Information and Communication Technology (ICT) Adoption in Tertiary Institutions
	Title Alternative	NIL
2.	**Document Identifier**	NIG-NITDA.14
3.	**Document Version, month, year of release**	Version 1.1; August, 2019
4.	**Publisher**	National Information Technology Development Agency (NITDA)
5.	**Type of Regulation Document** *(Standard/ Policy/ Technical Specification/ Best Practice /Guideline / Framework /Policy Framework/Procedure)*	Framework and Guidelines
6.	Enforcement Category *(Mandatory/Recommended)*	Recommended
7.	Owner of approved regulation	NITDA
8.	Target Audience	All Tertiary Institutions; ICT Product/Service Providers for tertiary institutions, ICT Professional Bodies, Development Partners, and General Public.
9.	Copyrights	NITDA
10.	Format *(PDF/A at the time of release of final Regulation)*	PDF
11.	Subject *(Major area of Standardization)*	ICT in Tertiary Institutions

Table of Contents

Foreword

Information and Communication Technology (ICT) has become firmly established as a necessary tool for the smooth running of any tertiary institution's Information Management strategy and associated core business processes and administration. ICTs now routinely support the processes of decision-making, policy development and service delivery, with the consequence that the effectiveness and efficiency of a tertiary institution's business processes are invariably determined by the quality of ICTs deployed as support tools.

Information and Communication Technology (ICT) has been defined by UNESCO as forms of technology that are used to transmit, store, create, share or exchange information. Such technologies include radio, TV, video, telephone (fixed and mobile), satellite systems, computer and network hardware and software, as well as the equipment and services associated with these technologies such as video conferencing, electronics etc.

ICT in education has a multiplier effect by:

1. Enhancing learning and providing students with new sets of skills;
2. Connecting students with poor or no access (especially those in rural and remote regions);
3. Facilitating and improving the training of teachers;
4. Minimizing costs associated with the delivery of education in traditional institutions.

With the understanding that effective and optimum use of technological tools must be informed by standards and policies that define systematic and informed deployment, the Federal Government of Nigeria has, in the past, and through the Ministry of Education and the Computer Professional Registration Council, initiated and adopted a number of policies and regulations designed to promote the rapid but ordered advancement of the ICT sector, and exploiting its huge potential for national development. Because of the inevitability of fast technological developments and market convergence of the global ICT industry, new ICT policy frameworks are often required, and conventional wisdom is that ICT policies and regulations should be characterized by such flexibility as will enable the sustainable development of the industry.

Dr Isa Ali Ibrahim (Pantami), PhD, FNCS, FBCS, FIIM

Director General/CEO, National Information Technology Development Agency (NITDA)

August, 2019.

PART ONE

1.0 PREAMBLE

1.1 Authority

In exercise of the powers conferred on NITDA specifically by Section 6 (a), (I) and (m) of the National Information Technology Development Agency (NITDA) Act of 2007, NITDA hereby issues the following Framework and Guidelines on Public Internet Access (PIA).

1.2 Purpose

The purpose of this Framework and Guidelines is to provide guidelines for the adoption of Information and Communications Technology (ICT) in tertiary institutions in Nigeria.

1.3 Scope

The document provides the framework and guidelines for the adoption of ICT in Nigerian tertiary institution and articulates rules that affect the use of ICT in these institutions.

1.4 Effective Date

This framework and guidelines shall take effect upon its publication. After that, it will be subject to a bi-annual review or as the need arises. NITDA shall issue further guidance on the evaluation process and timeframe to make changes and updates.

PART TWO

2.0 INTRODUCTION

2.1 Background

Outcomes of a recent comprehensive survey conducted by National Information Technology Development Agency (NITDA) reveal that quite a few Nigerian tertiary institutions have ICT policies of some type, but that the policies typically prescribe rules and regulations for 'appropriate' and 'responsible' use of facilities and resources, often to the exclusion of issues concerning e-learning and capacity building.

The goal of the Framework and Guidelines for ICT adoption in Nigerian tertiary institutions therefore, is to provide a flexible and comprehensive general framework for the deployment of ICT tools in Nigerian tertiary institutions for the effective and efficient support of the core business processes of teaching, learning, research and administration.

The National Information Technology Development Agency (NITDA) through the relevant regulatory agencies such as NUC, NBTE, NCCE, etc. will request for the adoption and implementation of the policy by:

a) All Federal tertiary institutions; and
b) All State-owned tertiary institutions.

The Framework and Guidelines prescribed in the document are designed to serve the purposes, among others, of facilitating the ability of the target tertiary institutions

- ✓ To provide fully automated and ICT driven business processes including records management, content delivery, and performance assessment, in Nigerian tertiary institutions;
- ✓ To provide suitable environments for life-long learning / continuing education;
- ✓ To develop a methodical system of collecting and disseminating data and information of relevance to national higher education issues;
- ✓ To deploy efficient management information systems;
- ✓ To broaden the horizon of educational services provision, including medium / method of content delivery;
- ✓ To promote effective information exchange best practices among and between students and lecturers;
- ✓ To deploy / enhance learning management systems and ICTs-supported library services;

- ✓ To promote technology literacy of all members of the community, especially for students;
- ✓ To develop vibrant and sustainable distance education platforms, focused on national development issues;
- ✓ To promote the culture of learning at school (development of learning skills, expansion of knowledge acquisition options, open source of educational resources, etc.);
- ✓ To institute and sustain capacity building programs in all areas of information and communication technology;
- ✓ To provide access to global digital library resources through networking initiatives, opportunities, and collaborations;
- ✓ To develop inter-tertiary institution linkages and collaborations, including content delivery with the use of Video conferencing and live video broadcast.

3.0 FRAMEWORK AND GUIDELINES

These provisions represent guidelines that:

a. Define authorities, responsibilities and accountabilities for ICT operations and management for each tertiary institution;

b. Prescribe a policy framework or template with which each tertiary institution can develop localized frameworks to derive maximum benefits from the usage of ICT, as informed by its circumstances;

c. Encourage tertiary institutions to adapt the Nigeria Government Enterprise Architecture (NGEA) developed by NITDA for use in their institutions;

d. Specify policies for the management of ICT resources and activities and concerning the following:

   a) Software acquisition, development and usage, and maintenance;
   b) Acquisition of ICT equipment, infrastructure and services;
   c) Repairs, disposal and disaster recovery;
   d) ICT networking infrastructure development;
   e) Universal access management and control;
   f) Funding of ICT equipment and infrastructure;
   g) Data and information management;
   h) Network services - Internet, email services and tertiary institution website;

i) E-learning and digital resources;

j) Cyber security issues- prohibited use of tertiary institution's ICT resources;

k) Enforcements.

4.0 SOFTWARE ACQUISITION, DEVELOPMENT AND USAGE

Every tertiary institution can benefit tremendously by developing its own software, as this will not only eliminate dependence on non-tertiary institution software for the delivery of ICT-supported critical services, but will also guarantee a ready and cost-effective customization to changing needs; As virtually all Information Management processes involving staff and students are supported by various software applications. Each tertiary institution should, therefore, strive to build a strong collaboratory interface with local and international software industries, and as much as possible, fully participate in activities of various global open source software development groups.

Policy guidelines in this section extend over the following items:

a. Software Development;

b. Open Source Software;

c. Pirated (or illegally acquired) Software;

d. Operating System software;

e. Software Uninstallation;

f. Software Copying;

g. Software Storage and records keeping;

h. Software Updates and Upgrades.

4.1 Software Development

Tertiary institutions are advised to have policies that define and prescribe processes for the development and procurement of software in a manner that increases efficiency and guarantees desired product quality assurance metrics.

Policy statements should encourage the building of capacity for in-house development of software by setting up a well-equipped Software Engineering unit staffed with high caliber software developers. Software development and acquisition policy issues should include:

i) Standardization (in-house or outsourced/off the shelf);
ii) Quality assurance strategy;
iii) Licensing and ownership;
iv) Technical support and software maintenance; and
v) Software disposal.

4.2 Open Source Software

The term 'Open source software' may be defined as "*software that can be freely used, changed, and shared (in modified or unmodified form) by anyone very often developed and shared in a public, collaborative manner*" without restrictions. Tertiary Institutions are also encouraged to adopt open source software. When open source software is to be adopted for use with tertiary institution business processes, associated policy statements shall require testing and quality assurance certifications. In addition, provisions for back end audit trails, information classification, and different user privilege levels should be required.

4.3 Pirated (or Illegally Acquired) Software

"Software piracy" refers to the unlicensed, unauthorized reproduction and illegal distribution of software, whether for business or personal use. It should be a matter of tertiary institution policy that:

i. All propriety software shall comply with developers/vendors licensing and ownership policy provisions;
ii. No pirated or unlicensed software shall be allowed on any official tertiary institution's computer systems;

iii. Members of the tertiary institution community shall be encouraged to avoid the use of pirated software with personal systems.

4.4 Operating System Software

i. It is useful to maintain standards for operating systems utilized in different environments for interoperability and efficient services delivery. Operating systems in common use include:
    - Windows Operating System;
    - Macintosh Operating System;
    - Linux Operating System;

ii. All acquired operating systems (and any other software) should make provisions for software maintenance support, and for upgrades, when desirable.

4.5 Software Uninstallation

In certain situations, it becomes necessary to uninstall software, which might have been deployed for critical business processes, and whose uninstallation may have consequences for data and information items, if not properly handled. It should consequently be a tertiary institution policy that the uninstallation of software deployed for use with tertiary institution business processes shall require formal clearance from the ICT Directorate, for the purposes of ascertaining that the uninstallation will not adversely affect records or associated processes.

4.6 Copying of Software

Staff, Students and visiting staff of the tertiary institution should be prohibited by policy, from making unauthorized copies of tertiary institution-owned software or soft documents.

4.7 Software Storage and Record Keeping

Efficient delivery of ICT support services is significantly dependent upon adequacy of records keeping. Tertiary institution policy should require the ICT Directorate to have responsibility for keeping records/inventory of interest to ICT related issues, including software acquisition documents (such as purchase receipts, service level agreements, user/maintenance manuals), original CDs, and disused or archived software.

4.8 Software Updates and Upgrades

In the typical setting, the need to improve the efficiency of a software's functionality or include an additional functionality can only be met by a software upgrade. The recommended policy is that the decision to upgrade should be informed by systematic considerations, possibly provided by a committee of ICT professionals within the ICT center.

5.0 ACQUISITION OF ICT EQUIPMENT, INFRASTRUCTURE AND SERVICES

Policy provisions concerning the procurement of ICT equipment, devices, associated infrastructure, and services, should define strategies for the effective management including acquisition policy, inventory control policy, first level equipment maintenance, and technical support policy. In addition, policy provisions should cover procedures, as well as roles and responsibilities for personnel involved. In most cases, the main responsibilities will reside with the tertiary institution's ICT Directorate, whose annual budget covers equipment purchases, equipment maintenance, Internet bandwidth, software licenses and backbone network maintenance. Typical policy provisions include:

i. Equipment, devices, or services shall be procured only from Original Equipment Manufacturers (OEM) or accredited agents/partners;
ii. Donated ICT equipment and devices shall only be accepted if they are certified as acquired from the OEM or accredited agents;
iii. The ICT Center shall develop specifications for equipment, devices, and services, to encourage standardization and consequently ease corrective and preventive maintenance processes;
iv. Bulk purchase of parts required for maintenance activities shall be encouraged, and implemented under the supervision of ICT Center personnel;
v. Business models shall be developed to prescribe service level agreement provisions for ICT services provided by vendors and services providers.

6.0 MAINTENANCE, DISPOSAL AND DISASTER RECOVERY

Orderly and well-planned maintenance of ICT devices, equipment, and associated infrastructure is of critical importance to the quality of ICT support services that the tertiary institution can expect. Policy provisions therefore should include informed guidelines for equipment maintenance, which may extend over such maintenance activities as

a. First level and routine maintenance
b. Disposal of ICT equipment, devices and software
c. Disaster Recovery and contingency plan

6.1 First Level and Routine Maintenance

The ICT Directorate should have the responsibility of providing centralized technical support services for all aspects of ICT including hardware and software. In addition, they should:

i) Train ICT asset owners on how to carry out first level maintenance, as a means of reducing equipment/devices down time; and provide manuals to serve as guide;
ii) Develop and provide user manuals that will facilitate the ability of asset owners to carry out preventive maintenance activities, and hence prolong equipment life;
iii) Maintain accurate records of maintenance activities on all ICT equipment and devices.

6.2 Disposal of ICT Equipment, Devices and Software

The ICT Directorate should be required, as a matter of policy, to prescribe ICT equipment/device replacement guidelines, including scheduled replacements, informed by pre-defined life cycle and maintenance history. Also:

i) In the case of hardware, disposal should be in compliance with practices specified by extant policy on the disposal of public assets, as well as environmental protection laws and statutes;
ii) Disposal of software should typically be informed by support life-cycle advertised by the developer.

6.3 Disaster Recovery and Contingency Plan

Disaster recovery and contingency plan specify the guidelines, resources, actions and personnel that are required to reinstate/restore the tertiary institution information/database in the event of any

loss that may arise from fire, vandalism, natural disaster or system failure. Contingency planning also ensures that the Internet and other mission critical systems do not go down for a period exceeding 24 hours. These requirements can be met with the following considerations:

i. Adequate backup systems and contingency plans shall be maintained and regularly tested for disaster recovery readiness;
ii. All units of the tertiary institution must maintain regular backup of their data;
iii. The ICT Directorate shall develop data backup guidelines and make them available to all units of the tertiary institution. In addition, cyber security best practices should be widely circulated to prevent against cyber-attacks, including denial-of-service and ransomware attacks;
iv. ICT related hardware contracts should not be approved without the expert advice and recommendations of the ICT Directorate;
v. In the case of data that is useful for critical services, cloud backup should be encouraged.

7.0 ICT NETWORKING INFRASTRUCTURE DEVELOPMENT

ICT Networking Infrastructure offers a range of technologies to assist an organization in running effectively. The key aspects of this are considered in this section.

7.1 ICT Backbone Infrastructure

Best industry practices require that tertiary institutions should have a rollout plan (typically a 5-year plan) as part of broader strategic planning considerations. Such plans will take account of the dynamic environments of computing needs, projected traffic growth, and technological advances.

7.2 Backbone Network

The following points should be noted with regard to the backbone network:

- The ICT Directorate shall, at all times, have updated versions of the tertiary institution-wide enterprise architecture, and shall be responsible for its development and maintenance;
- New technology shall only be introduced after professional tests confirm conformity with standards and performance requirements;
- Standards for structured cabling, as prepared by the ICT Directorate, shall be updated from time to time, and enforced across the tertiary institution.

7.3 ICT Project Management

Every tertiary institution should naturally be committed to continuously improving the delivery of ICT driven and supported services, within an approved budget, and should use the services of competent and qualified personnel. Well designed and managed ICT projects should further the objectives of effective and efficient services. ICT project management policies should consequently include the following provisions:

i. Assignment of responsibility for the implementation of ICT projects to the tertiary institution management through the ICT Directorate;
ii. Oversight functions to ensure that procedures conform to the tertiary institution rules and regulations possibly through the constitution of Project Implementation Team (PIT) with membership including Director of the ICT Directorate, Dean/Head/Director of the direct beneficiary faculty/ department/ directorate of the project, where applicable;
iii. Detailed functional and technical specifications must be documented and signed off by the Project Sponsor and the Director of ICT Directorate;
iv. All completed ICT projects shall be formally handed over to the ICT Directorate after ensuring that adequate training and documentation, as may apply, have been provided.

8.0 ACCESS MANAGEMENT AND CONTROL

The tertiary institution shall explore every ICT potential so as to enhance the services it offers to its staff and students. The purpose of access management and control shall be to define required access control measures to all tertiary institution systems and applications to protect the privacy, security, and confidentiality of tertiary institution information assets and systems.

Access control may be regarded in two dimensions; namely, access to physical facilities and tertiary institution buildings; and access to computing infrastructure and ICT services. A responsive ICT policy should provide for smart access to such tertiary institution buildings and facilities (Library, Hostels, etc.) as are not ordinarily open to the general public.

Policy considerations concerning access to tertiary institution computing facilities should cover:

a. ICT Infrastructure;

b. Network Control and Cyber Security;

c. Operational Environment.

8.1 ICT Infrastructure

ICT infrastructure consists of three major components:

a. The data communication network (DCN);

b. The network operations centre (NOC);

c. ICT services and computing resources for users.

8.1.1 Data Communication Network (DCN)

The data communication network includes all equipment and devices that facilitate the transmission and routing of data communication information items to various destinations across the tertiary institution. Important policy provisions for the DCN include:

i. Management of all associated infrastructural components, which is typically the responsibility of the ICT Directorate;
ii. Hosting of Domain Name Services (DNS) and servers, a responsibility of the ICT Center;
iii. Provision of redundancies for core network components to ensure uninterrupted services;
iv. Ownership of IP number space as prescribed by African Network Information Centre (AFRINIC).

8.1.2 Network Operations Centre (NOC)

Network Operations Centre (NOC-or 'Data Center') is the home for all servers and ancillary equipment that provide the hardware platform for the central network services of the tertiary institution. Industry best practices prescribe the following policy provisions:

i. Access to the NOC and network installations shall be secured and available only to authorized personnel;
ii. All NOC equipment shall be labelled in accordance to a pre-specified scheme approved by Management;

iii. The ICT Directorate shall keep an up-to-date inventory of all NOC equipment and devices, including maintenance schedules and maintenance history;

iv. Standards shall be specified for ICT equipment installed on the tertiary institution network, and authorized installations shall comply with the standards;

v. The ICT Directorate shall in collaboration with the tertiary institution's Legal Unit, define Service Level Agreements (SLAs) for use with the management of services provided by Third Party Services Providers, including ISPs and other ICT service providers;

vi. Access to NOC facilities by contractors or other Third Party shall with the authorization, and under the supervision of ICT Center personnel.

8.1.3 ICT Services and Computing Resources for Users

In addition to ICT services, the tertiary institution is obliged to provide computing resources, such as ICT equipment (computers and related accessories) that the tertiary institution community uses to access the various network services and for computer-based-examinations. Associated policy should provide for:

i. Adequate access time for users through the provision of sufficient computing facilities and access times;

ii. Ergonomic correctness of access facilities to prevent against any negative physical or physiological impact or damage to users;

iii. Secure e-mail services, with well-defined quotas, under the management of user account managers, with responsibility of assigning accounts, enforcing use rules, and periodically reviewing performance;

iv. Optimization of bandwidth utilization through the establishment and institutionalisation of an efficient cache management regime;

v. A secure, effective, and efficient intranet and associated web portal;

vi. Rights by tertiary institution authorized personnel, to audit any device attached to the tertiary institution's network, based on extant policies.

8.2 Network Control and Cyber Security

Network control and cyber security involves providing adequate barriers and controls that secure the tertiary institution's network infrastructure from intruders, hackers, virus, worms, e-mail spam and other disruptive software. The main policy objective in this case is to protect tertiary institution digital assets (including information assets) against denial of availability, compromise as well as breaches of confidentiality and integrity. Accordingly, policy provisions should include the items discussed in the sections below (8.2.x).

8.2.1 Assignment of Roles and Responsibilities

- Committee of Senate or Council to assume ownership of all cyber security risks and elucidate the tertiary institution's information risk avenues
- The ICT Center, whose responsibilities shall include:
  i. Instituting appropriate security controls and mechanism as informed by risk assessment outcomes; and maintaining an up-to-date risk register;
  ii. Development and utilization of a periodic systems and infrastructure audit, with basis in 'PDCA (Plan, Do, Check and Act)' cycle;
  iii. Instituting an effective mechanism for the control and auditing of user privileges, including administrative privileges;
  iv. A continuous monitoring, in real time, of all ICT network devices, and keeping records of outcomes of the analysis of security logs;
  v. Implementation of industry-standard protection mechanisms for the protection of wireless access services;
  vi. Regulation of access to ICT resources, enforcement of acceptable use policy, and deployment of associated standard security mechanisms and technologies;
  vii. Developing and maintaining accounts and privileges management procedure, including handing over of equipment/devices, schedules, and privileges in the event of disengagements or transfers.

8.2.2 Unacceptable Use of Resources

This policy provision specifies uses and practices that are prohibited, and include the following:

i. Sharing of personal pass phrases or passwords;

ii. Use of pirated and unauthorized peer-to-peer software on tertiary institution computing systems or devices;

iii. Uses or actions that infringe on copyright and intellectual property rights;

iv. Practices that have the potential for disrupting the normal functionality of tertiary institutions' computing systems or networks;

v. Introducing malware or malicious software into the network;

vi. Improper or immoral use of facilities including paid advertisements, Peer-to-Peer File Sharing (P2P), Business activities, pornography, Gambling, Computer Games. The ICT Directorate's networking team shall 'gray out' known sites, and continuously update the lists of sites offering the offensive services for blacklisting.

8.2.3 Antivirus

These are software utilities that protect the computers and networks from maliciously introduced applications and various malware types. Malware protection policy provisions include:

i. Availability of protective antivirus software designed to detect, remove and defend all tertiary institution computers against malicious software, malware or viruses;

ii. Subscription to services of reputable malware protection service providers for the provision of enterprise-wide, real time protection;

iii. Guidelines for computer virus management across the tertiary institution.

8.3 Operational Environment

This refers to the environment within which the ICT equipment is installed and operated. The typical working environment for all ICT facilities should have the following provisions:

a. Uninterrupted Power supply;

b. Adequate and well-maintained air conditioning system;

c. Illumination;

d. Fire protection- detectors and extinguishers;

e. Cleaning tools.

8.3.1 Uninterrupted Power Supply

This should consist of a suitable combination of the following:

a. Public power supply;
b. Standby generators;
c. Battery banks or inverters of adequate capacity (especially for centralized systems);
e. Stabilizers and power surge protectors.

8.3.2 Adequate and Well-Maintained Air Conditioning System

Air conditioning systems provides cooling that keeps the operational environment of the ICT facilities within the equipment manufacturers' recommended specifications for temperature and humidity all year round with the aid of humidity detector (Hygrometer/Psychrometer).

The tertiary institution shall ensure that server rooms and computer laboratories are equipped with properly-sized and functional air conditioning systems that operate at all times.

8.3.3 Illumination

This is a device that provides illumination. The tertiary institution shall ensure that the computer facilities are provided with functional lighting systems that operate at all times..

8.3.4 Fire Protection - Detectors and Extinguishers

These are devices used to detect and extinguish fire.

i. All computer laboratory and server rooms shall be equipped with smoke detectors and fire alarm systems.
ii. Fire extinguishers shall be provided for computer laboratories and server rooms. They shall be periodically tested to ensure that they are in good working condition.
iii. All IT personnel shall periodically be made to undergo fire prevention drills.

8.3.5 Cleaning Tools

These are tools used for keeping the operational environment clean and tidy.

i. The server room, computer laboratory and computers shall at all times be kept clean – free of dust, dirt and rubbish.

ii. Eating and drinking shall be prohibited at the computer laboratory and server rooms.

iii. The computers shall be kept clean and free from contamination.

9.0 FUNDING OF ICT EQUIPMENT AND INFRASTRUCTURE

ICT projects are necessarily capital intensive. The design, establishment and management of ICT projects require a lot of funding and financial processes. These finances are typically sourced, both internally and externally.

Policies on funding ensure systematic sourcing and consequently, continuous availability of funds. The associated provisions should be in place.

9.1 Source of Funding for ICT Equipment and Infrastructure

The provision of standard ICT services in the tertiary institution requires a huge investment of funds. Possible sources of funds are:

a. Tertiary institution budget through internally generated revenue or funds provided for government capital projects;

b. Public Private Partnership (PPP);

c. ICT Charges and fees from end-users - Students, Staff and the Public;

d. Training and support service by the ICT Directorate e.g. workshops and seminars;

e. Endowment placement or chair by individuals and corporate bodies;

f. Grants;

g. Donation by Government and private Agencies e.g. Trust Funds, Education Tax Funds;

h. Surcharges and penalties;

i. Disposal of unserviceable items;

j. Other sources as may be approved by the Head of Institution;

The tertiary institution shall create a separate ICT budget annually for ICT funding. The ICT budget votes shall have specific provisions for:

- Hardware acquisition;
- Software license fees;
- Hardware maintenance;
- System Development;

- ICT Technical Staff Training;
- ICT user training;
- ICT staff salaries;
- Equipment spares;
- Communication Fees (Bandwidth servicing).

10.0 DATA AND INFORMATION MANAGEMENT

Data and Information Management in any organization is very important and must be handled efficiently and professionally to avoid mismanagement and loss. All Institutional data and information which includes research data, library data, academic data, student data, human resource data, personnel data and financial data created, collected, maintained and recorded, shall be properly managed by the tertiary institution and/or agents working on its behalf.

In this section, policies on the following shall be considered:

a. Data Storage;

b. Data Confidentiality

c. Data Ownership

d. Copyright infringement

e. Data Retainership

10.1 Data Storage

i. The tertiary institution shall adopt a Centralized/Distributed database system of storage where each Unit/Department will have its local database. It shall also maintain a backup at the central storage which shall be managed by the ICT Directorate.

ii. The ICT Directorate shall ensure that each Unit/Department shall work out their own data security details.

10.2 Data Confidentiality

i. Authorized Users shall keep confidential record of all the tertiary institution data and information provided in confidence to the tertiary institution by other entities.

ii. Each staff member is under the obligation not to disclose tertiary institution data and information unless authorized to do so.

iii. Data and information shall be disseminated on a need-to-know basis and shall not be divulged to unauthorized persons.

iv. Breach of confidentiality through accidental or negligent disclosure shall result in disciplinary action taken against the user.

10.3 Data Ownership

i. All information acquired or created by users while carrying out the tertiary institution's business, except that which is specifically exempted as private or personal, shall be owned by the tertiary institution.

ii. Each User Department shall have individual ownership of its own data resource and ensure that the data is accurate and backed up regularly.

10.4 Copyright Infringement

i. Copying, recording or processing information which infringes any patent or breaches any copyright is not allowed.

ii. Products created from work done for the tertiary institution using the tertiary institution's ICT resources shall be the property of the tertiary institution and under no circumstances shall they be distributed or sold without proper authorization.

10.5 Data Retainership

This should be based on extant rules on data from the Tertiary Institutions retainership policies.

11.0 INTERNET, EMAIL SERVICES AND TERTIARY INSTITUTION WEBSITE

The Internet facility is primarily provided to enhance learning, teaching, research and administrative functions of the tertiary institution. The Internet complements the tertiary institution's library for research materials and information dissemination.

In this section, the following shall be considered:

a. Internet Access Acceptable Use;

b. Downloads;

c. Electronic Mail (E-mail) Services;

d. Tertiary institution's website;

e. Disclaimer;

11.1 Internet Access Acceptable Use

Large bandwidth without proper management will result in bandwidth wastage and a slow and inefficient system. Accordingly, Tertiary Institutions are encouraged to adopt the following:

i. The tertiary institution shall provide adequate bandwidth to meet the needs and demands of the users through the ICT Directorate;

ii. Only registered users shall be granted access information (username and password) to the Internet;

iii. Users must have an account to use the internet and the tertiary institution's e-mail services;

iv. The same user cannot use the same password on two different computers within an hour's interval;

v. Two users should not use the same account at the same time;

vi. All logins shall undergo both processes of authentication and authorization;

vii. Passwords must not be given out or shared;

viii. User access and activity on the tertiary institution network shall be monitored and logged;

ix. Access to heavily used sites (e.g. Yahoo mail, Google, Hotmail, Facebook) should be restricted between certain periods of the day whenever there is a need to do so. Users will be given adequate notice before such restrictions;

x. Appropriate filtering facilities for web based and non-web-based Internet traffic shall be provided to filter prohibitive and obscene websites with contents that do not have direct educational value e.g. pornography, gaming, advertorials, campaign links, sites with offensive materials relating to ethnicity, religion and gender;

xi. The tertiary institution shall restrict or suspend access to any user and at any time whenever this policy is breached.

11.2 Downloads

i. The size of data that can be downloaded is limited at specific times of the day;

ii. Unauthorized downloads, installation of programs or utilities that may flood the network, causing denial of service to other users shall be restricted;

iii. Downloading of multimedia-based files will be restricted, unless permitted by the ICT Directorate;

iv. Any computer/user causing excessive traffic congestion shall be automatically blocked after some time;

v. The tertiary institution's Internet facility shall not be used to propagate any malicious software (virus) or software that disrupts or damage computer systems.

11.3 Electronic Mail (E-mail) Services

E-mail services provide users with the means to exchange digital messages using a store and forward mechanism. E-mail systems accept, forward, deliver and store messages on behalf of users who only need to connect to the e-mail infrastructure for the duration of message submission to, or retrieval from their designated server.

The e-mail facility has been provided by the tertiary institution to enhance faster communication and interaction among the staff and students.

The following shall be considered for the tertiary institution's e-mail services:

a. Tertiary institution e-mail account;

b. Closure of tertiary institution e-mail account;

c. Mailing lists.

11.3.1 Tertiary Institution E-mail Account

Tertiary institution e-mail service is available for all staff and students under the official tertiary institution domain name (tertiary-institution.edu.ng) governed by the tertiary institution's mail policy. The e-mail account is divided into two groups:

a. Personal e-mail account: for the personal and professional use of the staff or students (tied to the name of the user);

b. Official e-mail account: strictly for official correspondence (tied to an office/post).

   i. Users shall be required to have a tertiary institution e-mail account which will be issued after approval by the authorized officer.

ii. The e-mail addresses (personal and official) shall have a standard format which all users must comply with.

iii. Only staff and students shall hold a tertiary institution e-mail accounts.

iv. E-mail shall be an acceptable means of disseminating official information (memos, notices) to the tertiary institution community.

v. Official internal information (as in iv) disseminated through e-mail shall be through tertiary institution's e-mail account.

vi. All official correspondences and public interaction shall be via the tertiary institution's e-mail account.

vii. Staff shall be expected to check and reply to official e-mail message within 24-hours.

viii. Students shall be expected to check and reply to all official e-mail messages within 48-hours.

ix. Users are not allowed to:

- Use tertiary institution's e-mail account for spamming;
- Use unethical languages in e-mails;
- Falsely represent the tertiary institution, assert or imply that personal views or opinions are the institutional view or opinion of the tertiary institution;
- Use the e-mail account for any commercial purpose;
- Send mass e-mail to a wide sub-set of users in the tertiary institution without appropriate privilege or permission;
- Use the e-mail account for disseminating offensive materials relating to ethnicity, religion or gender;
- Use the e-mail account for propagating negative impressions against the tertiary institution’s management;

x. Users shall be expected to ensure:

- Their access information (username and password) are kept private and promptly report in case compromise is suspected. Users are held accountable for any e-mail sent using their account;

- Confidentiality and privacy of official information is upheld: official information is not circulated beyond the boundary of the tertiary institution e-mail domain;
- Attachments sent are virus-free.

11.3.2 Closure of Tertiary Institution E-mail Account

i. The tertiary institution e-mail account of staff shall be deactivated or disabled as soon as feasible in the following categories:
   i. *Dismissal:* The e-mail account shall be deactivated immediately;
   ii. *Resignation:* The e-mail account shall be deactivated within 6 months;
   iii. *Retirement:* The e-mail account shall be deactivated based on extant rules of that institution;
   iv. *Death:* The e-mail account shall be deactivated based on extant rules of that institution;

ii. The tertiary institution e-mail account of students shall be deactivated or disabled in the following categories:
   i. *Expulsion:* The e-mail account shall be deactivated immediately;
   ii. *Rustication:* E-mail account shall be deactivated for the period of rustication;
   iii. *Graduation:* The e-mail accounts of graduating students shall be migrated to the alumni's mailing list after graduation;
   iv. *Death:* The e-mail account shall be deactivated based on extant rules of that institution.

11.3.3 Mailing Lists

i. Mailing lists shall be created to facilitate communications and dissemination of information in the tertiary institution;

ii. The tertiary institution staff Mailing List shall be used to disseminate information to and among staff;

iii. Postings to the tertiary institution Staff Mailing List shall be restricted to messages from the Head of Institution, Registrar, statutory boards, committees and others as approved by the Head of Institution or Registrar.

11.4 Tertiary Institution's Website

It is the policy of the tertiary institution to have an official website (tertiary-institution.edu.ng) that showcases the tertiary institution to the rest of the world for the purpose of disseminating up-to-date information from all organs of the tertiary institution (Faculties, Colleges, Departments, Directorates, Centres, Institutes and Units). The purpose of this website is to provide the staff and students of tertiary institution with the necessary information about the functionality of the tertiary institution website as an effective communication medium for the benefit of the tertiary institution community and the world at large. The website will amongst other things:

a. Enhance the tertiary institution's presence on the internet and broaden recognition for the tertiary institution, while strengthening its image;
b. Publishing of current and informative content in an acceptable manner;
c. Support a sustainable information and communication infrastructure that supports the tertiary institution's mission, goals and objectives through an on-line presence;
d. Help in optimizing resources to streamline, and automate the development and maintenance of a quick and easily accessible means of communication with the tertiary institution's target audience.

Some other considerations are listed below:

i. Tertiary institution web pages are the primary entrance points to the tertiary institution's website and the appearance and content shall be the responsibility of the ICT Directorate;
ii. The ICT Directorate shall always review the web pages to ensure that they reflect the same high level of quality and consistency as the tertiary institution's print publication;
iii. The ICT Directorate shall ensure that the content of the site conforms to the mission and mandate of the tertiary institution;
iv. Each Unit/Department/Directorate/College shall setup a committee to provide information to the Directorate of ICT for update of their web pages.
v. No Unit/Department/Directorate/Colleges shall be allowed to host their website or web-pages outside the tertiary institution's web server. Where this is deemed necessary, permission shall be sought from the Head of Institution.

11.5 Disclaimer

The tertiary institution shall not be responsible for the impact of materials viewed, downloaded or scanned by users from the Internet.

12.0 E-LEARNING AND DIGITAL RESOURCES

This refers to any technologically mediated learning using computers and other digital devices whether from a distance or in face-to-face classroom setting as in computer assisted learning.

In this section, policies on the following shall be considered:

a. E-learning Resources;

b. Digital Resources;

c. Digital Preservative/Archiving;

d. Education, Research Development and Copyright;

e. Tertiary institution Library;

f. Capacity Building/ End-User Skills Development.

12.1 E-Learning Resources

i. The tertiary institution shall acquire a versatile e-learning platform (open source or propriety) for use with e-learning activities. All tertiary institution faculties and teaching units should be enabled to effectively utilize the platform for content delivery learning and information exchange.

ii. The tertiary institution shall promote the integration of e-learning to improve the effectiveness of teaching, research and learning.

iii. The tertiary institution shall promote the development of e-content to address the educational needs of the tertiary institution.

iv. The ICT Directorate shall develop tertiary institution wide and global e-learning networks based on academic interest groups and research collaborations.

v. The tertiary institution shall ensure continuous training and promotion of in-house e-learning training capabilities for all students and staff on a continuous basis to equip them with the requisite skills to fully exploit the e-learning tools in the various disciplines.

vi. The tertiary institution shall collaborate and form global e-learning networks with other academic and research interest groups to facilitate the sharing of e-learning resources.

vii. The tertiary institution shall establish the appropriate common e-learning platform responsive to academic needs.

viii. The tertiary institution shall provide greater access to tertiary institution education through the development of ICT-based distance learning.

ix. The tertiary institutions should be encouraged to use plagiarism detection software for academic and research activities.

12.2 Digital Resources

Digital resources contribute to the commitment of the tertiary institution to support research activities and are intended primarily as a repository for previously-published work, and not as an independent publishing platform for new research articles.

Institutions are encouraged to provide access to reputable online databases, e-journals/conference proceedings, e-book, etc. Students and staff can access these databases and e-journals while on the institution's network or use some access login while off campus.

The tertiary institution community should note the following:

i. Researchers, authors, departments/units shall submit work for which they are the sole rights holders, or for which they have obtained permission to submit from all co-authors to the library;

ii. Work that may be submitted shall include; Theses and Dissertations, Journal articles, working papers, Conference papers, Inaugural lectures and published books. The work will receive increased visibility while raising the profile of the tertiary institution;

iii. All graduate Theses/Dissertations, Research Publications, Inaugural Lectures, and Conference Proceedings etc., approved by the appropriate Board shall be submitted to the Library in soft copies;

iv. Minutes of all meetings and reports of statutory boards, committees and others shall be deposited at the office of the Registrar;

v. All relevant hard copies of documents e.g. Minutes, CVs etc., shall be digitized and archived at the designated (Electronic Document Management System-EDMS Unit) of the ICT Directorates.

12.3 Digital Preservation/Archiving

The rapid growth in the number of digital resources and the tertiary institution's budget used to obtain them has made it necessary for proactive steps be taken to preserve these materials. As such:

i. Digital preservation activities shall ensure that Departments/Units, Faculties, Staff, Students, and other users have ongoing access to the tertiary institution Library's expanding digital collections;

ii. Tertiary institution library shall be committed to providing access to digital materials while respecting and upholding the intellectual property rights of authors and obtaining prior consent when the creator's identity is known;

iii. The tertiary institution library shall observe current standards and best practices related to the creation, maintenance, storage, and delivery of digital objects and metadata, as determined by international, national, consortia, and local institutions and governing bodies;

iv. The tertiary institution library shall commit to on-going training and development of staff in areas related to digital preservation, as well as outreach to inform units/departments, faculties, students, and staff of the best practices for creating and maintaining digital objects;

v. Tertiary institution library shall fulfill the digital preservation objectives by developing and maintaining the necessary hardware, software, expertise, and protocols to ensure long term access;

vi. The specific preservation actions used for the tertiary institution library's digital resources shall be significantly dependent on the source and type of content, as well as the existing technology, expertise, and ongoing support;

vii. Digital objects shall be managed using the life-cycle model, which is a framework describing the stages that digital resources go through during their existence;

viii. All digital resources created by the tertiary institution library shall adhere to the library's pending metadata policy;

ix. Digital resources shall be stored in a manner that is consistent with accepted best practices in the digital preservation community. This will include both technical infrastructure (hardware, software, network access, data backup, facilities, maintenance, etc.) and ongoing preservation management activities;

x. Best practices in digital preservation require duplicating digital objects in both local systems and geographically removed systems and shall in due course institutions should pursue this by working with the ICT Directorate to host redundant/remote local storage.

xi. This policy and the actions that flow from it shall be evaluated regularly to ensure that implemented strategies continue to support the Library's mission and policies to provide up-to-date resources, use resources in a cost-effective manner, and adapt appropriately to address evolving technologies. This evaluation shall be completed at least once every 3 years.

12.4 Education, Research Development and Copyright

Education, research and development constitute the major arm of any tertiary institution system. They represent where inventions, copyrightable works and other creative products of scholarship that have the potential to benefit the public through practical application may result from the activities of tertiary institution employees. This is in the course of their employment or through the use, by the students or by any person, of tertiary institution resources such as facilities, equipment, or funds. As such:

i. Those participating in scientific or scholarly research shall maintain careful research records, to establish and follow well-defined protocols consistent with all State, Federal, and tertiary institution guidelines, and to report discoveries, observations, and scholarly and artistic activities accurately and fairly;

ii. The tertiary institution owns all rights, titles, and interest in tangible research property and research data developed with support from tertiary institution resources;

iii. The tertiary institution shall own all rights, title and interest in Trademarks that relate to tertiary institution Intellectual Property or relate to a program of education, service, public relations, research or training by the tertiary institution;

iv. An author of an instructional or scholarly copyrightable work that is not tertiary institution-owned shall be free to publish it, register the copyright in the author's name, and retain any revenues which may result therefrom;

v. The tertiary institution shall require a written agreement from independent contractors that ownership of copyrightable works made in the course of a tertiary institution retention will be assigned to the tertiary institution;

vi. Each instructional or scholarly copyrightable work shall, by the operation of this policy, be subject to a perpetual non-exclusive, royalty-free license from the author to the tertiary institution to use, duplicate, and internally distribute such;

vii. Inventors shall promptly in writing disclose and assign each invention to the tertiary institution and/or its designee and shall not disclose any invention to any third-party except as specifically authorized by the tertiary institution or its designee;

viii. The tertiary institution Intellectual Property Office shall facilitate institutional practices that support research, education and development in the tertiary institution. This office shall also provide guidance regarding a fair use and other copyright compliance issues and will advise the Head of Institution on issues regarding the application of copyright law by tertiary institution staff. It will also implement a systematic, ongoing programme of copyright education and awareness suited to the rapidly changing technological and legal environments of higher education;

ix. Tertiary institution staff who desire to use copyrighted materials will be responsible for ensuring compliance with the applicable copyright law, including making an initial good faith determination as to whether or not the desired use falls within the fair use exemption;

x. In the event of genuine doubt regarding the application of copyright law, the tertiary institution staff shall have to consult with the appropriate office regarding such matters;

xi. The tertiary institution shall preserve valuable and intellectual materials by converting them into digital forms.

12.5 Tertiary Institution's Library

i. In terms of ICT services, the tertiary institutions Library will be responsible for creating and making available electronic-based library information resources under the supervision of the ICT Directorate. These resources will be for the purpose of teaching, learning and

research. They will include e-books, Online Public Access Catalogue (OPAC), digital repository, e-journals, information literacy, audio-visual services and CD-ROMs.

ii. The tertiary institutions shall improve both the efficiency and effectiveness of library operations and services through the implementation of an Integrated Library System (ILS). The ILS will be accessible within and outside the tertiary institution's network.

iii. The tertiary institutions will support the integration of its library information resources with other interested academic and research groups to share and gain access to more information resources.

v. The tertiary institutions shall continue to improve the infrastructure that will ensure easy access to the ILS.

12.6 Capacity Building/ End-User Skills Development

Use of ICT-supported and ICT-driven business processes invariably requires training in order to ensure effective and efficient utilization of resources. The effectiveness of training programs will depend on informed identification of training needs, which in turn, can be achieved through adequate ICT policy provisions. Such provisions include:

i. Mandatory training in basic and essential ICT skills for all cadres of staff and students;

ii. Programs for the continuous training for ICT personnel, as informed by periodic skills assessment to identify knowledge gaps;

iii. Regular programs for training and ICT-driven skills acquisition and improvement for teaching staff and facilitators at all levels;

iv. Development of capacity building modules for use with training programs and designed to address specific ICT skills gaps;

v. Building a pool of instructors (in-house and external experts) for training programs;

vi. Facilitating the ability of the ICT Directorate to conduct skills assessments and consequently recommend ICT training as may be indicated by skills assessment outcomes;

vii. Capacity building and collaboration programs designed to enable significant self-reliance;

viii. Essentially engender lifelong learning in ICT knowledge.

13.0 ENFORCEMENTS

Abuse of ICT privileges is subject to disciplinary action, which may include the loss of these privileges and other disciplinary actions. The ICT Directorate should:

i. Make appropriate recommendations on infringement to the institution's management for necessary action;

ii. Document and audit user compliance from time to time for the purpose of enforcing this policy;

iii. Monitor and respond to network breaches as they occur;

iv. Temporarily suspend network access if an incident is determined to be interfering with the operations of the tertiary institutions network;

v. Determine the impact of any alleged violation of this policy and take, without notice, any necessary action if tertiary institutions resources and services are adversely affected to prevent immediate and further damage to the tertiary institutions network. Such actions may include:

- Suspension of an account;
- Disconnection of systems or disabling network ports;
- Termination of running processes and programs;
- Any other actions deemed necessary to restore network services.

vi. Let users know that they shall be responsible for any financial loss to the tertiary institutions that results from inappropriate use of ICT resources;

vii. Immediately reset the user's password to a one-time only password in the event that a user password is compromised. Such actions are necessary to mitigate the risks from unauthorized access to tertiary institutions systems.

THIS INSTRUMENT IS HEREBY ISSUED ON THE 2ND DAY OF AUGUST, 2019

BY THE NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY (NITDA)

…..……

Dr Isa Ali Ibrahim (Pantami), PhD, FNCS, FBCS, FIIM

Director General/ CEO
Chief Information Technology of Nigeria.

Bibliography

Sources of these materials utilized include the following:

a) Federal Republic of Nigeria: "*National Information and Communication Technology (ICT) Policy*" by the Ministry of Communication Technology. June 2012. Available from https://www.researchictafrica.net/countries/nigeria/Nigeria_National_ICT_Policy_(draft)_2012.pdf

b) The Council of Computer Professionals Registration Council of Nigeria, in accordance with the Statutory Provisions of Section 17; see https://lawsofnigeria.placng.org/print.php?sn=78

c) Computer Professionals Registration Council of Nigeria Act Cap C22 LFN 2004 "*Report on the GAP Analysis of the ICT Needs in Nigerian universities*" by National Information Technology Development Agency (November 2017)

d) UNIYO: "*Information and Communication Technology (ICT) Policy*" December, 2015. Available from https://www.uniuyo.edu.ng/phpfiles/download.php?pc=%27.aC9WNHRvL3dVYUFvNUh3QW1Cb21ydz09

e) Makerere university "*Information & Communication Technology Policy: April 2016 to 2020"* https://policies.mak.ac.ug/sites/default/files/policies/ICT%20POLICY%20%28APRIL%202016-2020%29.pdf