UNIVERSITY OF ILORIN

ILORIN, NIGERIA

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY

2018 – 2022

University of Ilorin COMSIT ICT Policy Review Committee

Engr. Dr. J.F. Opadiji

Department of Computer Engineering

University of Ilorin

Engr. O. Bolade-Eyinla

Computer Services and Information Technology Directorate

University of Ilorin

Engr. O.J. Popoola

Computer Services and Information Technology Directorate

University of Ilorin

Ms. A.O. Eletta

Computer Services and Information Technology Directorate

University of Ilorin

Mrs. O. Olasehinde-Williams

Computer Services and Information Technology Directorate

University of Ilorin

Mrs. J. Jimoh-Mohammed

Computer Services and Information Technology Directorate

University of Ilorin

Preface

- **Director, COMSIT**

Table of Contents

1.0 UNIVERSITY OF ILORIN IN BRIEF

1.1 Preamble

The University of Ilorin is one of the second generation universities established by the Federal Government of Nigeria in 1975. From the pioneer undergraduate programmes offered in three faculties (Art, Education and Science), the University now runs over 60 undergraduate and graduate programmes in one college and fifteen Faculties: Agriculture, Arts, Basic Medical Science, Clinical Science, Education, Engineering and Technology, Environmental Sciences, Communication and Information Sciences, Law, Life Sciences, Management Sciences, Pharmaceutical Science, Physical Sciences, Social Sciences and Veterinary Medicine .

From an initial intake of 200 undergraduate foundation students in 1976, the student population as at the 2017/2018 session stood at over 54,000 undergraduate and postgraduate students. From the staff strength of about 200 in 1975, the population of staff as at April, 2018 stood at 4,403 for academic and non-academic staff.

With this growth, a rapidly changing technology and the need to integrate services, systems and databases a robust policy is required to deploy the required ICT infrastructure.

1.2 Current ICT Environment at the University of Ilorin

Like many universities in the developing world, the University of Ilorin acquired its first sets of microcomputers in the mid 1980's. They were used mainly for administrative purposes. The period also witnessed the establishment of the University Computer Centre, a unit for the training of low level computer technicians and delivering computing and data processing services.

In the 1990's giant strides were made with the growth in the acquisition of microcomputers by Units, Departments and individuals. This was complemented with the establishment of the Management Information System (MIS) Unit and the Nigerian Universities Network (NUNet) Office, both in 1992. With the growth in the number of units and individuals using computers it was evident that the University needed a centralized service oriented unit to manage the ICT needs of the University. This led to the establishment of the Computer Services and Information Technology (COMSIT) Directorate in 2001. The Directorate is charged with the responsibilities of deploying ICT infrastructure and services for administrative purposes, teaching, research and learning to the University. It also provides needed services to the University's immediate and larger community.

Before the year 2003, Internet connectivity by some units was mainly through dial-up access or wireless connectivity to private ISPs within the City of Ilorin. A landmark achievement was the commissioning of the Education Trust Fund sponsored VSAT project of the University in 2003. This provided better access to Internet facilities for the University. A VSAT Board was constituted to manage the wireless wide area network (WAN) for the distribution of Internet services. In addition, the University in conjunction with the Joint Komputer Company (JKK) successfully used Computer Based Test (CBT) in August, 2008, for conducting examination of large classes including the Post-JAMB Screening.

The campus computer network is made up of a fibre optic backbone and a wireless distribution centre. There are 3 main layers of the network: the Core, the Distribution and the Access layer. As at March 2013, all the completed buildings on campus were connected to the campus wide fibre optics backbone, new buildings like the Faculty of Arts complex, Unilorin Microfinance Bank and Faculty of Vet Medicine were connected making a total of 99 (ninety nine) building connected to the campus wide fibre optics backbone. All other buildings after March 2013 were either connected to the Network via wireless or are presently not on the network.

The fibre optic backbone is divided into six (6) distribution rings; the Senate, Library, Human Kinetics, COMSIT, CIS, and Agric rings. Only 3 of these rings currently have active equipment (Senate, CIS and Agric). Other rings are looped to the closest ring for Internet connectivity. There is a direct link from each of these distribution rings to the Network Operations Centre and to the closest distribution ring.

Thirty-two (32) buildings have structured LANs on the campus, while others use wireless access points at the access level. About forty percent (40%) of student environment (lecture theatres) has been connected to the network via wireless backbone.

Coverage

The network coverage area includes the Main campus, Institute of Education, School of Preliminary studies, College of Health Sciences , University staff Quarters (senior and junior), and some staff residential houses.

Bandwidth

The University is currently on four (4) STM1 (620 Mbps) bandwidth.

Users

Presently, over forty five thousand (45,000) users are on the network. These include all staff and undergraduate students. Postgraduate students are not yet on the network as registered users. Users have their login credentials to log on to the University hotspot. The login credentials cannot be used simultaneously on more than one device.

Services

The network provides Intranet and internet services, some of these services include: VoIP, surveillance, video conferencing, live streaming and cloud storage. The Network unit runs 24 hours services in three (3) shift duties (morning, afternoon and night).

2.0 ICT POLICY OBJECTIVES

The objectives of the ICT policy are to:

(1) provide a framework for automation of all administrative processes in the University;

(2) provide a template for the provision of adequate and reliable ICT facilities to promote effective teaching, research and scholarship;

(3) draw up standards for ICT capacity building for staff and students;

(4) craft procedures for access to information across the campus;

(5) regulate ICT support for research and development activities in the University;

(6) ensure protection of intellectual property rights for ICT projects developed by members of the University Community;

(7) guarantee efficiency of University operations and services through implementation of relevant information systems;

(8) improve academic reporting facilities at both central and faculty levels through the implementation and upgrade of an integrated staff and students' information management system;

(9) provide a framework for partnership between the University and external organizations on ICT-related projects;

(10) provide regulations on the use of University ICT facilities to prevent abuse among members of the University community and any unlicensed user; and

(11) ensure enforcement of regulations provided for in the University ICT policy.

With proper implementation, the ICT policy would enhance quality in teaching, learning, research, and community service.

3.0 POLICY STATEMENTS

3.1 ICT Procurement Policy

The vista of ICT infrastructure within the University has changed over the past ten years. This is as a result of the deployment of ICT-enabled teaching and research equipments apart of computers in various departments and units within the University. Most of these teaching and research equipment require internet connectivity to maximise their usage, hence the need to provide guidelines for their procurement. These guidelines are to ensure easy integration into the existing University ICT network. Also, the increasing use of microcomputers and mobile devices for various University activities require that the procurement process of these devices be regulated to avoid the purchase of substandard equipment and in more extreme cases the procurement of equipments that can compromise the University ICT network infrastructure.

3.1.1 Objectives

The objectives of the University of Ilorin ICT procurement policy are:

(1) to ensure that teaching, research and administrative electronic equipment procured by the University are ICT-enabled and are internet-ready;
(2) to ensure the purchase of high quality, state-of-the-art and easily upgradable ICT equipment by the University given the increasingly short lifecycle of these equipments;
(3) to protect the University against poor warranty and guaranty conditions during ICT equipment purchases;
(4) to enable the University take advantage of economy of scale during large quantity ICT equipment purchases from Original Equipment Manufacturers (OEMs) or their certified vendors;
(5) to ensure conformity with standardized requirements for ICT equipment connectivity to the University ICT network infrastructure;
(6) to ensure that approved standards are followed in situations when ICT services are to be procured by the university; and
(7) to create a dynamic inventory system for all ICT equipment within the University.

3.1.2 General ICT Procurement Policy

The following shall govern the mode of procurement of ICT equipments and services in the University:

(1) The Computer Services and Information Technology (COMSIT) Directorate shall be notified when ICT-enabled equipment are to be procured by the university for advice on the inter-operability of such equipment with the existing University network infrastructure and conformity with requirements regarding various ICT standards and quality.

(2) In situations where ICT services are to be procured by the University, providers of such services shall be made to consult with the COMSIT Directorate regarding their activities on the ICT network infrastructure.

(3) A User Requirement Specification shall be submitted to COMSIT with details of the requirements; the desired aim and objectives for making the request; and the number of anticipated users.

(4) Acquisition of these goods and services by various units shall be done in a manner that would be in consonance with a procurement advisory document prepared by COMSIT on such procurements.

(5) Off-the-shelf software must be licensed and capable of running under the desired operating system platform(s).

(6) For software to be developed in-house, COMSIT or any other group as determined by the University Administration shall provide for specification, verification, validation, implementation and maintenance.

(7) Where necessary, especially for major ICT projects, an ICT Project Management Committee shall be responsible for planning and monitoring and evaluation of such projects.

(8) No agreements for the supply of ICT equipment, components or services shall be undertaken by the University without collective consultations and agreement with the End user and COMSIT.

(9) Where possible, the University shall consider the option of in-house direct purchase for the purpose of cost minimisation and utility maximisation.

(10) All certified vendors of OEM (Original Equipment Manufacturer's) equipment and off-the shelf software must show evidence of their registration with the Manufacturer.

(11) All warranty and guaranty agreements with OEMs shall be fully explored in cases of equipment defects and/or damage.

(12) In addition to the acquisition process mentioned above, the University may acquire ICT devices through in-house design and production, donations from other agencies such as Government, Institutions and NGOS and through ICT equipment leasing.

(13) COMSIT shall develop and operate an ICT equipment inventory information system that will keep track of all ICT equipment, their location and their present operating conditions within the University.

(14) The Bursary Unit shall have real-time access to the ICT equipment information system.

3.2 Unilorin ICT User Access Policy

Users of the University of Ilorin ICT facilities are primarily staff and students of the institutions. User access may be given to non-members of the University community based on the approval of the University management through the Director of COMSIT or other delegated authorities. All users of the ICT facilities in the University are considered to have given their consent to comply with the terms of the University of Ilorin ICT policy. The University reserves the right to withdraw all or part of any user privileges at any time it deems fit with or without prior notification given to such users.

3.2.1 Objectives

The objectives of the Unilorin ICT user access policy are:

(1) to regulate the activities of ICT users on the University ICT network;

(2) to provide guidelines for the use of private devices on the ICT network;

(3) to deter users from use of the network for nefarious activities;

(4) to protect users on the network against unsolicited access to their personal devices; and

(5) to protect the university ICT network against the activities of vandals.

3.2.2 ICT User Access Policy

Activities of users of the University of Ilorin ICT facilities shall abide by the following guidelines:

(1) All users of equipments on the University ICT network shall be responsible for the safe keeping of all such devices in their care all through the period of usage.

(2) Users connecting to the ICT network using personal devices shall obtain proper authorization from the appropriate authority before accessing the network.

(3) Users shall not engage in nefarious activities which violate the codes of the University and/or the laws of Nigeria using the University of Ilorin ICT network either in-situ or remotely.

(4) Users shall make sure not to deploy any injurious software, such as viruses, malwares, spywares, etc, on the ICT network

(5) Users shall make sure to follow copyright laws when using the University ICT network to access any material online as the University shall not be liable for any such infringements perpetrated by any individual or group of individuals.

(6) Users shall not at any time negotiate or grant access to anyone with regards to the use of the ICT network for any purpose.

(7) Users shall immediately report any suspected security breach of the network noticed on by them either on their devices or the devices of other users.

(8) Users shall not use the University ICT network to connect to devices of other users without prior authorization.

(9) Users shall not access any official material on the University ICT network without appropriate authorization.

(10) The University shall prosecute any unauthorised access to her network.

3.2.3 Bring Your Own Device (BYOD)

(1) Staff or Students who prefer to use their personally-owned IT equipment for work purposes shall secure corporate data to the same extent as on corporate ICT equipment, and must not introduce unacceptable risks (such

as malware) onto the Corporate networks by failing to secure their own equipment

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

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

- Anything classified SECRET or CONFIDENTIAL;
- Other currently unclassified but highly valuable or sensitive corporate information which is likely to be classified as SECRET or above;
- Large volume of corporate data (i.e. greater than 1Gb in aggregate on any one POD or storage device).

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

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

(6) Suitable antivirus software shall be properly installed and running on all devices.

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

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

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

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

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

3.3 User Support and Facilities Management Policy

(1) The ICT services offered to the University community shall be adequately supported through a helpdesk system. Faculty-based ICT officers, Web-ring groups and departmental level advisers shall be well trained to offer various degrees of support on the ICT services pertaining to all ICT infrastructure and services.

(2) COMSIT shall provide helpdesk support for the following services:

- Staff and Student Portals (admission inclusive)
- Email
- Web Sub-domains
- Computer Networks (Internet and Intranet Connectivity)

3.3.1 Password Policy

Computer passwords are used for various purposes at the University. Since very few systems have support for one-time tokens, that is, dynamic passwords that are only

used once, all users shall familiarize themselves with the following information on how to select strong passwords. Poor, weak passwords have the following characteristics:

(1) The password contains less than eight characters

(2) The password is a word found in an English or other dictionary

(3) The password is a common usage word such as:

a) Names of family, pets, friends, co-workers, or fantasy characters.

b) Computer terms and names, commands, site, company, hardware, software.

c) The words "faculty", "ilorin", " nigeria" or any such derivation.

d) Birthdays and other personal information such as addresses and phone numbers.

e) Word or number patterns like aaabbb, qwerty, zyxwvuts, or 123321.

f) Any of the above spelled backwards.

g) Any of the above preceded or followed by a digit such as secret1, 1secret.

Strong passwords have the following characteristics:

- Contain both upper and lower case characters like a-z, A-Z;
- Have digits and punctuation characters as well as letters such as 0-9, !@#$%^&*()_+|~- =\`{}[]:";'<>?, or / ;
- Are at least eight alphanumeric characters long;
- Are not words in any language, slang, dialect, or jargon, among others; and
- Are not based on personal information, or names of family, among others.

(4) The rules governing password use is aimed at reducing the vulnerability of the ICT services provided by the university to internal and external security threats. To this end, the follow rules shall be adhered to by users of these services:

a) All system-level passwords such as root, enable, server administration, Application administration accounts, shall be changed at least once every month.

b) All user-level passwords such as email, web, and desktop computer shall be changed at least once every six (6) months.

c) User accounts that have system-level privileges granted through group memberships or programs such as "sudo" shall have passwords distinct from all other accounts held by such users.

d) Passwords shall not be inserted into email messages or other forms of electronic communication.

e) Passwords for the University accounts shall not be used for other non-University access such as personal ISP accounts, personal email services, and Bank ATMs.

f) All passwords shall be treated as sensitive, confidential University information. Users shall not share the University passwords with anyone, including administrative assistants or secretaries.

g) Users shall not use the "Remember Password" feature of applications based email services like Eudora, Outlook, and Netscape Messenger.

h) Users shall not write passwords down and store them anywhere in public spaces.

i) Where an account or password is suspected to be compromised the affected passwords shall be changed immediately. The COMSIT shall be alerted immediately to investigate the incident, if it affects critical University information systems or processes.

j) As a proactive defence procedure, password cracking or guessing tools may be performed on a periodic or random basis by the relevant staff of the COMSIT or its delegates. If a password is guessed or cracked during one of these scans, the affected user shall be required to change the password immediately. All user-level and system-level passwords shall conform to the guidelines described below.

(5) Software applications developed by and/or for the University shall contain the following security precautions:

a) Shall support authentication of individual users, not groups.

b) Shall not store passwords in clear text or in any easily reversible form.

c) Shall provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
d) Shall support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

3.3.2 ICT Facilities Management

After deployment of ICT infrastructure and services, necessary conditions for safe and convenient usage shall be provided, these include:

a) Training of intending users which must precede the usage of any new ICT facility.
b) Provision of conducive environment for ICT usage.
c) Providing adequate protection for ICT equipment such as burglar proof windows and doors.
d) ICT equipment shall be installed and/or configured to eliminate unauthorized access and use.
e) ICT equipment should be used along with UPS and Automatic Voltage Regulator (AVR) where necessary.

3.3.2.1 Hardware Maintenance Services

(1) Maintenance of hardware shall be taken into consideration from the design stage and point of procurement.

(2) Astute management of the procurement process shall deliver a robust service level agreement-SLA (after sales service inclusive) to maintain the quality of service (QoS) and quality of Experience (QoE) desired.

(3) Except otherwise approved, branded hardware equipment shall be procured to access on demand technical support from vendors; cloned system may be procured in exceptional cases when desired, and in this case shall be subjected to necessary technical approval.

3.3.2.2 Hands-On-Training

The Hands-on-Training on the supplied equipment and software shall assume the practical nature of the subject and shall include use of manuals, workshop training, audio-visual presentations, etc.

3.3.2.3 Specifications for Hardware Deployment

When purchasing hardware, provision shall be made for the following:

(1) Electricity installation and control shall conform to the IEEE regulations.

(2) All cabling shall comply with the relevant sections of the IEEE regulations.

(3) Lightening arrestors should be installed on every building housing ICT equipment.

(4) Fire extinguishers should be displayed at strategic areas of the building where the equipment are installed.

(5) All equipment for ICT use should be of voltage rating 230 / 240 Volt (± 6%); and frequency of 50 Hz (±1%).

(6) New buildings should include cabling for network terminals.

(7) Dynamism in the ICT world necessitates that COMSIT / any other group as determined by the University Administration publishes a list of specifications to guide the University community from time to time.

(8) All procurement must be guided by the published specifications.

3.3.2.4 Installation and Testing

(1) Whether a supply is by an external contractor or internally acquired, COMSIT shall ensure that installation and testing carried out by the supplier complies with the contract specifications and is so confirmed on the certification.

(2) In addition, software supplied shall comply with the manufacturers licensing and Registration requirements. Therefore, certification for off-the-shelf software will be signed only after successful registration and licensing.

(3) Confirmation of manufacturers' or suppliers' documentation shall be part of the certification process. Such documentation include user manuals, circuit diagrams, hardware drivers, installation guide, program source code (for in-house software), users maintenance manual (hard copy or soft), and any other materials that may be deemed necessary for that particular contract.

(4) Adequate lighting arrestors shall be installed on every building housing the server.

3.3.2.5 Maintenance

(1) For adequate maintenance of ICT facilities the items and conditions below shall be in place:

- Original software
- Adequate documentation such as Users manual, Repair or Troubleshooting guide, Circuit diagrams, Installation and Configuration manual, Device drivers
- Compatibility of components (Hardware and Software).
- Upgradeability
- Sufficient and adequate spare parts to ensure spontaneous repair by replacement
- Relevant spare parts must always accompany the purchase of any equipment
- Built-in redundancy especially for Servers

(2) To facilitate maintenance of any type, all ICT equipment shall carry history cards. The history card contains basic information about the equipment and shall include the following:

- Name of equipment.
- Location of equipment.
- University Fixed Asset Number.
- Serial number/Model Number.
- Scheduled preventive maintenance dates.

- Name and Signature of staff that carried out the maintenance.
- A description of job done and parts changed.
- Signature and comments of the user department.
- Signature and comments of the supervising maintenance officer.

(3) To facilitate the maintenance of Software, the policy on software usage shall be practiced.

3.3.2.5.1 Preventive Maintenance

(1) The preventive maintenance option shall be designed to track down degraded or worn out parts which require replacement, in order to increase the life-span and efficiency of the equipment. Under this option, there shall be an agreed period of time when this exercise shall be carried out to locate any faulty component for replacement.

(2) The preventive maintenance service routine shall focus on the following activities – cleaning, inspection, lubrication, replacement and adjustment.

(3) For effective maintenance, Schedule Forms and Maintenance Logbooks shall be used by the maintenance officer for timing the maintenance and to carry out the preventive maintenance. Such maintenance logbooks shall include,

- Name of equipment.
- Location of equipment.
- University Fixed Asset Number.
- Serial number/Model Number.
- Scheduled preventive maintenance dates.
- Name and Signature of staff that carried out the maintenance.
- A description of job done and part changed.
- Signature and comments of the user department.
- Signature and comments of the supervising maintenance officer.

(4) The algorithm (step by step) of preventive maintenance shall be designed and formatted to prevent damage to an otherwise functioning equipment by the maintenance team.

3.3.2.5.2 Breakdown Maintenance

(1) A complaint on breakdowns or faults can occur at any of the University ICT installations. Such complaints shall be made to the officer-in-charge by the following methods:

- Writing an internal memo
- Filling an appropriate report form
- Placing a telephone call, or
- Through the Intranet communication system.

(2) Thereafter, the maintenance logbook described under Preventive Maintenance shall be used for documenting the resolution of the complaint. In the case of a breakdown, repairs which cannot be corrected at the users' site shall be moved to the workshop.

(3) The officer-in-charge should work towards resolving the complaint as quickly as possible. Where this is not feasible, the problem should be brought to the attention of a higher authority.

3.3.2.5.3 Contracted Maintenance

It is envisaged that from time to time situations may arise that require the use of an external maintenance vendor. This may result from a situation where the required expertise is not readily available internally, or where it is desirable to award the maintenance alongside the supplies.

In general, contracted maintenance services for ICT equipment, components or services, shall be undertaken by the University with collective consultations and agreement with the User, COMSIT or any other expert group as the University may wish to set up for such a purpose (i.e. the contract supervisor), in order to draw up the

type of maintenance agreement to be procured. The contract shall comply with the following:

- As part of the conditions of the agreement, the contractor shall include a maintenance training plan for in-house staff.
- For contracted maintenance, a representative of the contract supervisor shall be present as supervisor to certify the work done.
- Payment for contracted maintenance shall be made in line with the agreement and final endorsement of the contract supervisor.

3.3.2.5.4 Hardware Redundancy Policy

Spare parts shall be made available for all high-end network equipment i.e. power supply units, routers, switches and network cable at the heart of the data centre network equipment in the data centre or Network Operation Centre(NOC). This will ensure high availability of the services of the data centre and NOC. Therefore, hardware in this category should be purchased with spares.

3.3.2.5.5 Hardware Replacement Policy

Any ICT system on the University ICT network is expected to be at least ninety-five percent (95%) reliable, therefore spares should be made available for all ITEs (Computing Server and Network Modules) for emergency contingency purposes and in order to ensure availability of service.

3.3.2.5.6 Tools and Maintenance Store in COMSIT

The COMSIT directorate shall have a tools and maintenance equipment store which shall keep inventory of all tools and equipment used by maintenance personnel. The staff in charge of this store shall keep a log of tools and equipment usage with the respective times of release and return to the store. Maintenance staff to whom any equipment is released shall be responsible for the safe-keeping of such equipment.

3.3.2.6 Software Maintenance and Upgrade

The maintainability of Software shall be considered from the design and development stages for bespoke solution and during the request for proposal (RFP) in the case of

off-the-shelf packages. Software maintenance and upgrade shall be performed by designated personnel in COMSIT and ICT Faculties, upon approval from the Director of COMSIT. Such maintenance/upgrade shall be scheduled during off-peak period to prevent denial of services.

3.3.2.6.1 Specifications for Software Deployment

Software includes Firmware, Operating Systems (for Standalone and Network), Utility Software, DBMS, Programming and Application Packages and Mobile apps. To facilitate its usage and maintenance, the following shall be practiced:

(1) Software shall be original and shall be purchased directly from the company or its representatives in Nigeria.

(2) Adequate documentation such as user's manuals, installation and configuration manual shall accompany any software acquired off-shelf or developed by a contractor or consultant or in-house.

(3) Sufficient and adequate training and retraining shall be provided for the assigned Programmers/System Analysts on any new software acquired or developed.

(4) Designated officers shall update all software as new versions are released.

(5) Collaboration on in-house software development by both COMSIT and ICT Faculties shall be encouraged.

3.3.2.7 Hands-On-Training

The Hands-on-Training on the supplied equipment and software must assume a practical nature and should include use of manuals, hands-on practical sessions, audio-visual presentations, etc.

3.3.3 User Support Services

(1) Users of the computer based information system provided on the platforms of web, email, portal and network domains shall be adequately supported by the helpdesk unit in COMSIT.

(2) The helpdesk team shall deploy bespoke and/or off-the-shelf helpdesk multi-level ticket system to enhance service delivery.

3.3.3.1 End-User Support

(1) The University shall establish a centralized End-user Support Centre manned with staff having good working knowledge of latest operating systems, development tools, and application packages on workstations.

(2) A help desk will exist as a point of contact with end-users, staffed by personnel who can give immediate technical support or can refer (escalated) to specialists if the problem cannot be handled. The functions of the End-user Support Centre shall be as follows:

- Assistance for day-to-day end-user computing problems.
- General technical assistance.
- Professional assistance in writing and debugging specific programs.
- Assistance in accessing corporate databases (query language).
- Access to reference material on facilities, databases, etc.

3.3.3.2 Appropriate Use and Responsibility of Users

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

- Are courteous and polite;
- Are consistent with University policies;
- Protect others' right to privacy and confidentiality;
- Do not contain obscene, offensive or slanderous material;
- Are not used for purposes that conflict with the University's interests;
- Do not unnecessarily or frivolously overload the email system (e.g. spam and junk mail);
- Do not carry harmful content, such as Viruses
- Are not for commercial purposes

3.3.4 Decommissioning Policy

ICT devices shall be considered obsolete on the recommendations of COMSIT, ICT related faculties or any other expert group as the University may wish to set up for such purpose. On making final decision, the device(s) shall be decommissioned and disposed of by any of the following means:

- Auction Sales.
- Gift to the University Secondary School or Primary School.
- Gift to charity organizations.
- Users of the equipment or staff.
- Released to ICT-related departments and faculties or COMSIT for training of student or for research purposes.
- Outright scrapping through proper disposal methods for electronic hazardous wastes.

However, arrangement could be made during the procurement process of branded hardware for exchange of seemingly obsolete hardware for later/state-of-the-art versions, with minimal cost implications.

3.4 ICT Network Infrastructure Policy

The computer network infrastructure in the University has evolved into a large, complex network over which the education, research and business activities of the University are conducted. It is envisaged that the network will integrate text, image, voice and video, to form a unified information technology resource for the University community. Such a network shall demand adherence to a centralized, coordinated strategy for planning, implementation, operation and support. This policy applies to any person accessing or using the network infrastructure owned, managed, supported or operated by, or on behalf of the University. These include all university staff and students; any organization accessing services over the University network; persons contracted to repair or maintain the University network, and suppliers of network services.

3.4.1 Objectives

(1) The objective of this policy is to establish a comprehensive and uniform Network development and management policy for administration of the University network infrastructure.

(2) To ensure that engineering technologies and standards are taken into account when designing and implementing network infrastructure in the University.

(3) To define the arrangements and responsibilities for the development, installation, maintenance, use and monitoring of the University's network.

3.4.2 ICT Network Architecture

(1) The University network functions shall be broken down into the following areas:

- Network backbone connections
- External data communication
- Network equipment
- Network expansion
- New buildings/ refurbished buildings/construction of roads
- Network management
- Network security
- Network users
- Contractors
- Network support

(2) This therefore shall require a policy that will secure the future reliability, maintainability of the network.

3.4.3 Network Backbone Connections

(1) Connection to any of the University backbones shall be approved by the Director of COMSIT.

(2) All building on the main campus shall be connected to the fibre optics backbone with fibre active equipment at the access level.

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

(4) All buildings on campus shall be connected to the wireless backbone or fibre backbone depending on the distance to the nearest distribution ring.

(5) Upgrading of the existing wireless backbone on 100Mbs link at lectures theatres to fibre backbone of at least 1Gb link shall be done to make the lecture theatres “e-learning ready” and for better network performance.

(6) Buildings connecting to the University network shall meet overall University network security and management requirements.

(7) A University staff that wants his/her home connected to the University network shall write to the Director of COMSIT for permission and will bear the cost of survey, design, installation and implementation and maintenance on approval.

3.4.4 External Data Communication

(1) All external communications shall be channelled through the University approved links upon prior written consent from the Director of COMSIT.

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

3.4.5 Network Equipment (Servers, Switches, Routers, Access Points, etc)

(1) The purchase and installation of any network equipment shall be approved by the Director of COMSIT and shall follow the policy on procurement of hardware.

(2) All Network equipment are owned by the University though they are in the custody of the units where they are deployed.

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

(4) The University shall migrate from the campus standalone wireless APs deployment to controller based technology that is compatible with the Aps for better performance and efficient management, especially in locations like lecture halls, lecture theatre, auditorium.

(5) The number of deployed radios in a location shall be proportional to the number of targeted concurrent users to follow the standard of the radio's Original Equipment Manufacturer (OEM).

(6) In the event that any equipment is stolen or damaged, the Director COMSIT shall be informed immediately.

(7) Movement of a network equipment shall only be done only with the sole permission of the Director COMSIT.

(8) Only designated members of the staff of COMSIT or ICT-related departments and units shall be authorized to install and maintain active network equipment including hubs, switches and routers connected to the University's networks with the consent and approval from the DCOMSIT.

(9) Replacement of any network equipment shall follow the hardware replacement policy.

3.4.6 Network Expansion

(1) The Director COMSIT must be consulted to give approval for the expansion of the network.

(2) The Director COMSIT shall be consulted in advance where there is need to add or replace a network /power backup equipment.

(3) In the event of network expansion or changes on the network the Director of COMSIT must be consulted for approval who shall give approval for the

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

(4) Any unit or persons who want to extend the network must get a written permission from the Director COMSIT who will give the approval else such a user will be disabled from the network.

3.4.7 New Buildings / Renovated Buildings / Construction Works

(1) The Physical and Planning Unit shall ensure that the network structural design is included in the design of any new building and as such work with the Director of COMSIT for guidance.

(2) All new buildings to be erected in the University (blocks of offices) shall incorporate an appropriate structured cabling system to allow connection into the university Network.

(3) In the event of refurbishing an old building the Director of COMSIT has to be communicated so as to ensure that existing network infrastructures are not damaged else the unit shall be responsible for any damage done on existing network infrastructure.

(4) The Director of COMSIT shall be informed any time a building, road, car park is to be constructed, to identify the path of the fibre optic backbone, to avoid damage. In the course of any damage the contractor shall bear the cost of the damage.

3.4.8 Preventive Maintenance of ICT Network Infrastructure

(1) There shall be periodic review of the earthing system in all buildings where network infrastructure are deployed by the works unit.

(2) There shall be provision of earthing system in any new building where network infrastructure shall be deployed by the Works unit.

(3) There shall be periodic review of existing alternative power backup and provision of alternative power backup at any location where network infrastructure is deployed.

(4) There shall be a periodic maintenance of network and alternative power backup every 2 Months by the officer in charge of a Zone and notice shall be communicated to users by the Director COMSIT.

(5) There shall be extinguisher at every location where network equipment are located.

(6) There shall be a cooling system and proper ventilation where network equipment are deployed.

(7) There shall be periodic review of the cooling systems and the fire extinguisher.

(8) Cooling system of the power Farm shall be permanently on and the door always shut.

(9) All periodic reviews and maintenance shall be approved by the Director COMSIT before commencement.

3.4.9 ICT Network Service Providers

(1) Contractors providing ICT network services must obtain the prior approval of the DCOMSIT and shall obtain the appropriate authorization in compliance with procedures and regulations of the University security system.

(2) Contractors shall observe any specific access conditions which apply within the areas in which they will be working. These access conditions include, in all cases, that contractors working in main server rooms shall be accompanied by appropriate University ICT personnel.

3.4.10 Network Security

(1) Room housing network equipment like switches and alternate power shall be under lock and the unit where such rooms are shall be in charge of the security of such equipment.

(2) The server room of the Data Centre shall always be locked and only authorized officers shall have access to the room.

(3) There shall be a functioning Access control system to restrict unauthorized access to the data centre / server room.

(4) All Standalone Aps at less dense populated areas shall be password with a security key to avoid congestion on the APs.

(5) Physical security like burglary shall be provided for all out door Access points to prevent theft and rooms where network equipment are kept shall have lock to restrict unauthorized access.

(6) Users shall keep passwords secure and shall not share accounts. Shared accounts are prohibited. Authorized users are responsible for the security of their passwords and accounts.

(7) An Intrusion Detection system and Firewall shall be installed at the edge of the network for security, management and control.

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

3.4.11 Network Usage

(1) All network users shall be provided login credentials to the university hotspot to have access to the internet upon payment.

(2) Every new staff member shall write through their unit head to the Director COMSIT to have login credentials.

(3) Students account shall be created at the beginning of the session after the late registration and at the end of the session students account will be disabled.

(4) Staff and students shall be able to change their password themselves without having to calling the helpdesk for assistance.

(5) Abuse of network shall result in disconnecting or disabling such user from the network.

(6) A user account can only be used on a device at a time.

(7) Users who require more than one user account shall direct such applications to the Director (COMSIT)

(8) There shall be an idle timeout of 5 Minutes, after which a user shall be logged out and will have to re-login to have access to the network.

(9) All network user complaints shall be directed to the helpdesk officer for network support.

3.4.12 Network User Support

(1) The University Network shall be divided into Zones for easy management and each zone shall be managed by a staff of the Network Administrative unit and shall be known as a zone officer.

(2) The University through COMSIT shall provide tool kits (multimeter, LAN tester, Crimper, punch down, screw driver etc.) for zone officers to work effectively.

3.5 Software Service Policy

Information Systems have become a vital part in many organizations as they are used to support core functions within organizations. This means that reliability is a key component of these Information Systems. Reliability does not come by coincidence; it shall be planned for and incorporated in the entire development process. In order to achieve this, the University and the users shall employ sound software development techniques and standards that will ensure that the end product can stand the test of time. Once software has been developed and is operational, there is need to ensure that all necessary support and use procedures are adhered to. This will ensure that the information from the system remains relevant, is accurate and will only be available to authorized persons. This will also ensure that the integrity of the system is not compromised at all times. Users shall be supported at all times as stipulated in this policy.

The policy covers the development and support guidelines within University. Moreover, the policy also covers the support required for any operational Information Systems, integrity of data, request for service, and accessibility of Information.

3.5.1 Objectives

(1) The purpose of this policy is to ensure that the process of software development at the COMSIT follows the due process right from the planning phase through to the implementation stage and that all deliverables at every milestone meet the required standards.

(2) This policy also seeks to continually improve on the process of software development at the COMSIT and ensure that the software products produced meet the requirements of the user and are of good quality.

(3) This policy also addresses the need for software support and use of the available information to ensure that the integrity of the system is not compromised at any time. The need for ownership of software by users is also addressed to apportion responsibility and improve access to this information.

3.5.2 Software Development Policy Statements

The Portal unit within COMSIT is responsible for developing, and maintaining university wide administrative and academic software portals. The Portal unit section shall provide systems development and support for university enterprise wide applications. In addition to this,

(1) Departments & faculties may be allowed to buy software or customize software limited to internal usage. Such customization with be a collaborative effort between COMSIT and the department

(2) Departments & faculties planning to buy software will need to acquire pre-approval support for purchase from COMSIT. COMSIT will need to verify if the University already has licenses for the software requested or not. In addition, COMSIT will verify if proposed software is available, compatible and conforms to university standard development software/operating systems.

3.5.2.1 Specifications for Software Deployment

Software includes Firmware, the Operating System (for Standalone and Network), Utility Software, Programming and Application Packages. To facilitate its usage and maintenance, these processes shall be followed:

(1) Software shall be original and must be purchased directly from the company or its representatives in Nigeria.

(2) Adequate documentation such as user's manuals, installation and configuration manual shall accompany any software acquired off-shelf or developed by a contractor or consultant or in-house.

(3) Sufficient and adequate training and re-training shall be provided for the assigned Programmers/System Analysts on any new software acquired.

(4) Designated officers shall update all software as new versions are released.

(5) Collaboration on in-house software development by both COMSIT and other ICT related faculties must be encouraged.

(6) Off-the-shelf software shall be licensed and capable of running under the desired operating system platform(s).

(7) For software to be developed in-house, COMSIT or any other group as determined by the University Administration shall provide for specification, verification, validation, implementation and maintenance.

3.5.3 Web Services ad Domains

The web domain shall consist of the University main website and various subdomain under it. The subdomain will be the web pages of faculties, centers, units, institutes, offices, holdings, recreational facilities, accommodation etc. within the university confines. The web domains information structure shall be such that promotes

- Visibility – Impact
- Activity – Presence, Openness & Excellence and

enhances accessibility to University programmes and activities. However the Confidentiality, Integrity and Availability of web information will be guaranteed with secured onsite and/or offsite hosting of web domains services.

3.5.3.1 Web Management Software

(1) Open sources server operating system such as apache server in Linux Operating System is recommended because of the Open Source Codes, Cooperative Tools and Utilities, Multi-user & Multitasking Abilities, Excellent Networking Environment, Security, Cost-effectiveness and Portability they possess. More so, it aids in capacity building and enhance research and development amongst the Linux development community.

(2) Database management systems such as Oracle, Microsoft SQL Server, PhpMyAdmin, MySQL etc. shall be utilised to developed bespoke application tailored to the specific need of the institution.

(3) Content Management Solution (CMS) with the highest degree of security shall be deployed on the webserver and domains. High degree of security shall be maintained through:

- the choice of the most secured CMS,
- proper configuration of CMS,
- upgrade and backup capability,
- deletion of unwanted and unidentified developer extension,
- usage of security extensions,
- keeping file/folder permission appropriate

(4) Proprietary server OS such as Internet Information Service are expensive to deploy, hence usage of such shall be de-emphasized, except when it is absolutely necessary.

(5) Where software-as-a-service (SaaS) is presented in conjunction with Infrastructure-as-a -service (IaaS) and Platform-as-a-service (PaaS), it shall be duly assessed on the basis of confidentiality, availability, Integrity and cost effectiveness by COMSIT to ascertain the sustainability of such services.

3.5.3.2 Web Cache Provision

(1) The COMSIT Directorate shall be responsible for provision and management of University web cache facilities for incoming web traffic.

(2) All web access shall be set up to ensure use of the University's web cache facility for incoming web traffic under the ICT Internet Usage Policy.

3.5.3.3 Web Filtering

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

3.5.3.4 Web Server Standards Policy

The purpose of this policy is to minimise risks to the University that may arise as a result of incorrect information being made available through unauthorised Unilorin web

sites, and to ensure that Faculties, Schools and other Organisational units have access to reliable web facilities and infrastructure. This policy is applicable to:

- All staff and students.
- All University Associates.
- All users of ICT equipment owned or leased by the University.
- All equipment connected to University data and voice networks.

The Director of COMSIT may approve exemption or partial compliance with this policy where technical or operational reasons preclude full adherence.

(1) Material with Unilorin URLs shall only be published on an Authorised web server. Authorised Web servers shall be managed to present a professional image of the University. Authorised web servers shall conform to COMSIT standards for server equipment, configuration and management.

(2) Any material published electronically at Unilorin that is found to be in breach of any Federal or State legislation, any Unilorin Policy, or that significantly restricts or impacts on resources available to others may be removed without notice by authority of the Director of COMSIT.

(3) Except where approval has been granted by the Director, COMSIT or delegate, no web server shall be accessible via the World Wide Web beyond the Unilorin communications network.

(4) COMSIT shall maintain a register of Authorised web servers. Information contained in the register shall include web servers' physical and network addresses, and details of staff responsible for their maintenance. COMSIT may from time to time use information collected in the registration process to contact staff responsible for the maintenance of Authorised web servers.

(5) Before material with a Unilorin URL may be made accessible beyond the Unilorin communications network, the web server on which the material is stored shall be registered with COMSIT, and the configuration of the server must be compliant with the provisions of this policy. To request registration

of a web server and thus enable it to publish material on the internet, the Web Server Registration form must be completed and provided to COMSIT.

(6) Authorised web servers shall be managed to assure maximum availability for University clients. Down-time shall be scheduled with adherence to COMSIT change management procedures.

3.5.3.5 Web Server Management

(1) Each Authorised web server shall be managed by a designated officer who is part of a recognised ICT team to ensure appropriate levels of technical backup. The officer shall be appropriately experienced to professionally manage the Authorised web server. Such officers must be authorized by their executive manager or delegate to act as the point of contact on matters related to the web server(s) in their charge.

(2) The designated officer's name shall be registered with CITS as part of the web server registration process to ensure that contact may be made promptly as necessary.

(3) COMSIT shall from time to time survey Authorised web servers to determine:

- the hardware in use;
- the server operating system in use;
- the web server software in use;
- the latest systems patch installed;
- the latest server application patch installed.

(4) Where any Authorised web server is found to be being managed in contravention of the provisions of this Policy and Procedures, steps may be taken to restrict access to it from beyond the Unilorin communication network after reasonable consultation with the member of staff responsible.

3.5.3.6 Server Security Policy

(1) Any server deployed on the University ICT network shall have an operational group that shall be responsible for its system administration. Operational

groups shall monitor configuration compliance and shall implement an exception policy tailored to their environment. Each operational group shall establish a process for changing the configuration guides; if the server is executing critical University systems this shall involve a final review and approval by the Director, ICT.

(2) All servers shall be registered with the COMSIT. At a minimum, the following information shall be forwarded:

- Contacts of the System administrator
- Physical location of the server
- Hardware and Operating System version in use
- Description of functions and applications of the server

(3) Configuration changes for servers shall follow the appropriate change management procedures.

3.5.3.7 General Configuration Guidelines

(1) Server Operating Systems shall be configured in line with approved ICT guidelines.

(2) Services, applications and ports that are not used shall be disabled at all times, for instance NFS, Telnet, FTP and SSH Client such as Filezilla, WinSCP and Webmin.

(3) Access to services shall be logged and protected through access-control methods such as TCP Wrappers where possible.

(4) The most recent security patches shall be installed on the systems as soon as
practicable, the only exception being when immediate application would interfere with business requirements.

(5) Antivirus software shall be installed and configured to update regularly.

(6) Trust relationships, such as through NFS, between systems are a security risk, and these use shall be avoided. No trust relationship shall be used where alternative secure methods of communication are available.

(7) User access privileges on a server shall be allocated on “least possible required privilege” terms, just sufficient privilege for one to access or perform the desired function.

(8) Super-user accounts such as “root” shall not be used when a non-privileged account can do.

(9) If a methodology for secure channel connection is available, that is technically
feasible, privileged access shall be performed over secure channels, for instance, encrypted network connections using SSH or IPSec.

(10) Servers shall be physically located in an access-controlled environment.

(11) It shall be prohibited to operate servers from uncontrolled or easily accessible areas.

3.5.4 Email services

(1) The email is still the most used application on the Internet and as such the institutional email shall be the only accepted means of correspondence within and out the university.

(2) Legacy webmail configuration with Unilorin fully qualified domain name (FQDN) shall be the first priority in mail relay and exchanges, while collaborative free webmail consumer services with educational applications such as that of GSuite (Google Apps in Education/Supporting Programs), MS Office 365 Apps for Education etc., could follow using protocols such as LDAP for dual delivery of mails. For legacy and collaborative mail accounts, authentication and authorization shall be through the designated corporate administrator.

(3) Email server configurations i.e. incoming and outgoing server settings will be provided by COMSIT and accessible to users. Email Services shall be hosted independently from the Web Services i.e. separate virtual server, to promote availability, sustainability and in-house capacity building.

3.5.4.1 Email Server and Client Software

(1) Mail Transport Agents such as Sendmail, Postfix, Phpmailer etc. are bundles with apache server, while client such as squirrel mail and roundcube mail are light Mail User Agents.

(2) Proprietary Mailing softwares such as Microsoft Exchange server is proprietary and expensive to deploy, hence usage of such shall be de-emphasized, except in cases where is will be funded by external bodies.

(3) Where software-as-a-service (SaaS) is presented in conjunction with Infrastructure-as-a -service (IaaS) and Platform-as-a-service (PaaS), it shall be duly assessed on the basis of confidentiality, availability, Integrity and cost effectiveness by COMSIT to ascertain the sustainability of such services.

3.5.4.2 Appropriate Use of Electronic Mail

Electronic mail facilities provided by the University are intended for teaching, learning, research, outreach and administrative purposes. Electronic mail may be used for personal communications within appropriate limits. Mailing list with list name shall be made available for announcement and discussion, while groups and forum created for collaboration, teaching and learning.

3.5.4.3 Confidentiality and Security

(1) As the ICT network infrastructure and email services are the properties of the University, the University reserves the right to allow authorized personnel to monitor and examine communications on this platform.

(2) Users shall ensure integrity of their password and abide by University guidelines on passwords.

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

(4) Users shall be aware that incremental backup (on demand inclusive) is carried out on the mail server.

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

(6) Recovery of password for users on other web domain services shall be done via email.

3.5.5 Portal Services

(1) Unilorin Web portal applications shall offer consistent look and feel with access control and procedures for multiple applications and databases for staff and students. A single access portal to all university online applications and services is desirable. SSO shall be implemented for identification and authentication on the Portal services.

(2) Portal services shall include all programmes undertaken by undergraduate and postgraduate students, e-journal system, accommodation services, health care services, library services, recreational services or as deemed fit by the University administration.

(3) Portal services shall be developed by in-house personnel of COMSIT or in collaboration with Academics from ICT-based departments and units, except for cases where off-the-shelf portal application is desired or donated.

3.5.5.1 University Data Farm

(1) The University shall set up a centralized and organized knowledge management unit to manage the growing volume of University databases.

The unit will, organizationally, be placed in COMSIT. The functions of the unit shall include:

- Definition and promotion of database standards.
- Promotion and control of data sharing.
- Analysis of impact of change requests (for example: data definition changes) to applications.
- Maintenance of the data dictionary and other documentation.
- Reduction of redundant data and data processing.
- Improvement of security of data.
- Tuning database management systems.
- Selection and evaluation of database technology (database management software and media).
- Physical placement of databases on specific computers (servers).
- Installation of (new releases of) database management systems.

3.6 Unilorin E-Learning Policy

With the deployment of ICT equipment and services for various didactic activities in the University of Ilorin, the regulation of e-learning processes within the University is of utmost importance. The policy regarding e-learning activities in the University regulate the use of ICT-enabled hardware and software for pedagogy and management of educational resources.

3.6.1 Objectives

The objectives of the University of Ilorin E-Learning policy are

(1) to regulate the deployment of e-learning equipment for within the University;

(2) to regulate the use of open educational resources (OERs) for didactic activities in the University;

(3) to provide guidelines for the implementation of learning management systems (LMS) in the University;

(4) to standardize to production of e-learning resources in the University; and

(5) to control the use of licensed learning resources procured by the University.

3.6.2 E-Learning Policy Statements

The operation of e-learning facilities and processes in the University of Ilorin shall be governed by the following guidelines:

(1) The University shall provide internet-ready smart boards and multimedia projectors in as many lecture venues (classrooms, lecture halls and lecture theatres) as possible.

(2) Adequate security shall be provided for e-learning facilities in all lecture venues.

(3) Vandalising of e-learning facilities by any individual or group of individuals shall be strictly prohibited.

(4) All e-learning equipments in lecture venues shall be provided with internet connectivity.

(5) The university shall provide staff and students with access to open educational resources (OERs) via the university intranet and internet infrastructure.

(6) The university e-library shall have a local repository of electronic resources which are made available to staff and students.

(7) The University shall develop and maintain an open courseware system which is to be populated by lecture resources authored by course lecturers.

(8) Academic departments and units shall be mandated to provide original courseware of courses offered by them.

(9) The University of Ilorin open courseware system shall be periodically updated.

(10) The COMSIT directorate shall implement an in-house learning management system open for use by lecturers and students.

(11) The University of Ilorin shall maintain a strict antiplagiarism policy and shall provide for easy access to antiplagiarism tools for all members of the University community.

(12) The use of open social media software by lecturers shall be allowed provided they are in strict compliance to University policies and guidelines governing interaction between lecturers and students.

(13) Social media platform accounts created by lecturers or student groups for pedagogic purposes should be made open for assessment by authorised University officials.

(14) No staff or student shall deploy any unlicensed proprietary software on the University ICT infrastructure. The University shall not be liable for any such actions due to omission or commission on the part of a member of the University community.

(15) The university shall reserve the right to withdraw access by any member of staff or student to the University e-learning facility due to actions deemed to be deleterious to the ICT network.

3.7 Computer-Based Testing (CBT) Policy

The Unilorin CBT centre is composed of six (6) halls containing 1,450 computers which can accommodate 1,200 students per batch, assuming a maximum redundancy of 7%. The following examinations are regularly conducted using the University of Ilorin CBT infrastructure:

- Post – UTME Screening examination
- Unilorin School of Preliminary Studies
- Institute of Education Examinations
- JAMB - UTME

- Unilorin Undergraduate CA and Examinations
- Unilorin Promotion and other external examinations.

3.7.1 Objectives

The use of CBT is aimed at creating a fair and an unbiased test administration and scoring, where each candidate is treated fairly and without prejudice and the objectives of the policy statements are to

(1) improve the integrity of every examination conducted on the CBT platform;

(2) improve on speed and accuracy of examination feedbacks;

(3) improve mechanism to accommodate Special need candidates;

(4) improve data security by eliminating the possibility of hacking and other online malpractices.

3.7.2 CBT Policy Statements

3.7.2.1 Internal examinations

(1) Departmental time tables shall be structured around the CBT time table to avoid clash of exam time.

(2) The CBT internal examinations shall be for Courses with 200 and above registered students.

(3) Lecturers who intend to use CBT for their course examination shall be proficient in the use of the approved CBT authoring Manager.

(4) The chairman CBT writes to the Deans of Faculties and Heads of Departments at the beginning of every semester, requesting for the list of their courses to be examined by CBT.

(5) All questions brought to CBT shall be vetted and signed by the Departmental Examination board. Questions shall be brought one hour before the commencement of examination.

(6) Students shall be at the CBT venue 30 mins before the start of their examination

(7) Questions shall be brought to CBT by the course lecturer or the HOD exactly 1 hour before the examination commences.

(8) Each course should have at least 4 invigilators per hall.

(9) Students who arrive more than 15 mins after their scheduled time will be dined entry.

(10) The CBT committee shall review all incident report on an individual basis and determine whether action is warranted.

3.7.2.2 External Examinations

(1) Channel of communication shall be maintained as thus: information shall be communicated to the DV Academics, the DVC then relates with the CBT Chairman who then relates with the CBT technical head and CBT Technical partners.

(2) Organizations shall come to CBT with questions in the correct and acceptable format 30 mins before the commencement of their examination.

(3) Organizations and bodies shall come with their invigilators for all CBT examinations.

3.7.2.3 CBT Training

CBT shall organize trainings for new Staff and Students every session to intimate them with the modalities of CBT examination and the appropriate personnel to report issues to.

3.8 Telecommunication Policy

The University of Ilorin is yet to take full advantage of advances in the telecommunication technology sector to facilitate easier communication among

members of the University community. Existing telecommunication infrastructure is limited to very few offices within the University. It is expedient that the University provides telecommunication access in every office within the University to reduce time lag in information flow and also provide for better deployment of human and material resources. It is important to note that due to poor official telecommunication infrastructure, most official assignments and communications are carried out on private telecommunication devices, which lead compromise of classified information and in some cases outright loss of vital official communications. The telecommunication policy is therefore crafted to regulate the deployment and use of telecommunication facilities within the University.

3.8.1 Objectives

The objectives of the University of Ilorin Telecommunication policy are:

(1) to regulate the deployment of telecommunication facilities for official communications within the University;

(2) to provide guidelines for use of telecommunication devices for official communications within the University;

(3) to ensure proper management of official communications over official telecommunication channels within the University;

(4) to provide guidelines for the use of open telecommunication platforms by members of the University community for official communication purposes;

(5) to prohibit unauthorised use of the university name, logo or any other insignia on unapproved telecommunication platforms; and

(6) to ensure proper archiving of official communications done on open telecommunication platforms.

3.8.2 Telecommunication Policy Statements

The following guidelines shall be adhered to in the use of telecommunication facilities within the University:

(1) The university shall provide official telecommunication access to staff of the University.

(2) The University shall keep an updated directory of telecommunication access devices provided for staff members.

(3) All university staff shall have access to the official telecommunication directory of the University.

(4) Official telecommunication channels shall be made available for access during official working hours of the University.

(5) Except as approved by an authorised officer, all official communications shall be done on official devices.

(6) The University shall keep logs of official communications for documentation and reference purposes as deemed necessary by the University management.

(7) Private communications shall be prohibited on official telecommunication channels.

(8) Official communications between staff members and students shall be restricted to official telecommunication channels provided by the University.

(9) The University shall not make public private telecommunication channels of staff members.

(10) Staff members shall have access to telecommunication channels of students directly within their official scope of work.

(11) Where necessary, the University shall provide licensed video communication platforms for official meetings.

(12) All approved official accounts created on open telecommunication platforms in the name of any department, unit or agency of the University shall automatically become the property of the University of Ilorin.

(13) No staff member or student shall create any official account in the name of the University without approval from an authorised officer of the University.

(14) In cases where open telecommunication platforms are used for official meetings, approval shall be given by an authorised officer of the University and a log of communications in such meetings shall be archived by the secretariat.

(15) Official accounts created open telecommunication platforms shall be as approved and communications on such platforms shall be restricted to official transactions.

(16) Use of official telecommunication platforms for private, political, religious and commercial communications by staff members shall be strictly prohibited.

(17) The university shall reserve the right to withdraw access of any staff to any of the official telecommunication channels provided by the University.

3.9 Unilorin ICT Industry and Community Partnership Policy

The synergy between the University of Ilorin and the ICT industry has been forged to facilitate research and development activities, human resources development programmes and community development initiatives. In addition to existing partnerships with companies in the ICT industry and contributions made to the development of ICT infrastructure in communities around the University, it is expected that the University of Ilorin will expand this network of partnerships as part of her contributions to the sustainable development goals of the country. Policies in this area are formulated to construct a framework for interactions between the University and various ICT industry partners and also between the University and beneficiary communities of the University of Ilorin ICT community development efforts.

3.9.1 Objectives

The specific objectives of the University of Ilorin ICT industry and community partnership are:

(1) to implement an information system profiling the various partners and partnerships the University has with the ICT industry and the immediate community;

(2) to provide a guideline for engagement of University of Ilorin ICT manpower in specific ICT research projects commissioned by ICT companies;

(3) to define rules of engagement of University of Ilorin ICT personnel in training people outside the University community;

(4) to outline protocols for ICT product development for industries and surrounding communities; and

(5) to map out procedures for engaging beneficiary communities in ICT-oriented community development initiatives.

3.9.2 ICT Partnership Information System

(1) An information system shall be developed to contain the profiles of all industry partners and beneficiary communities.

(2) The information system shall be a store for memoranda of understanding (MoU) and partnership agreements between the University and partners.

(3) The information system shall keep records of interactions between the University of Ilorin and ICT industry partners as well as communities.

(4) The information system shall incorporate a platform that will serve as a dashboard for partners to monitor up-to-date partnership activities.

(5) Information on various partnerships and ICT-oriented community development efforts are to be sourced from the information system and filtered for use by various publicity units of the University.

3.9.3 ICT Research Partnership

(1) ICT-based research partnerships initiated by an ICT company and involving the engagement of University of Ilorin ICT personnel and researchers shall be addressed to the University management.

(2) The Deputy Vice-chancellor, Research, Technology and Innovation (RTI) shall constitute a team of researchers and ICT experts nominated by the Director (Center for Research, Development and In-house Training (CREDIT)) and Director (Computer Services and Information Technology (COMSIT) Directorate).

(3) The research team shall be led by a qualified academic from an ICT-based department or unit, who shall not be below the rank of a Senior Lecturer.

(4) After the signing of a MoU and partnership agreement between the University of Ilorin management and the prospective industry partners, the University of Ilorin research team shall be commissioned to engage in the research project.

(5) The ICT industry partners shall provide complete financial and material support for the project except otherwise stated in the partnership agreement.

(6) A detailed log of interactions between the research team and industry partners shall be stored on the partnership information system.

(7) Ownership of research outputs and dissemination of research outcomes shall be as agreed upon in the partnership agreement.

3.9.4 ICT Training Partnership

(1) Relevant ICT departments and units within the University shall develop specialized short-term training programmes for professional certification courses for interested members of the public and targeted institutions in the ICT industry.

(2) The University shall have detailed prospectus/handbook for every ICT-based training programme which is to be approved by the University Senate.

(3) Each ICT-based training programme shall be domiciled in an academic department/unit of the University.

(4) Trainers are to be pooled from both academic units and COMSIT directorate.

(5) ICT industry clients seeking specialized training courses by the University shall direct all such requests to the University management and the University management through the Director (COMSIT) and Director (Consultancy unit) shall design a training package for the clients.

(6) ICT Industry partners willing to engage the services of the University ICT personnel in sponsored training programmes are to direct their applications to the University management for approval and outsourcing of the relevant staff members.

(7) Industry partners shall also be given opportunities to sponsor in-house training of University staff members and ICT training for University community development programmes through the provision of financial support, infrastructure support and the participation of certified ICT professionals approved by the University management.

3.9.5 ICT Product Development Partnership

(1) The University management shall commission hardware and software development teams made up of personnel from the COMSIT directorate and ICT professionals from other relevant departments and units within the university to develop bespoke software and hardware products on requests received from industries and as community development initiatives.

(2) ICT hardware products commissioned by the university shall be executed by a team of experts from ICT-based departments and units within the university.

(3) Bespoke software and hardware products developed by the University project development team for industry partners are to be fully sponsored by the clients.

(4) Software and hardware development projects shall be treated as consultancy services by the University and staff members drafted into such projects are to be remunerated accordingly.

(5) Complete documentations of developed ICT products commissioned by the University are to be submitted to the University. The University shall own the copyrights of such documentations.

(6) Staff members who engage in ICT development projects commissioned by the University shall sign a non-disclosure, non-compete agreement before participation in such projects.

(7) The University management shall also give due considerations to the outsourcing of ICT professionals within the university to engage in product development projects on request by industry partners.

3.9.6 Community-based ICT Development Partnership

(1) The University shall engage in ICT-oriented community development efforts that include the provision of ICT infrastructure, off-the-shelf software products, development of bespoke software and training programmes for manpower development in the ICT industry.

(2) The University shall also serve as facilitators in various ICT-based corporate social responsibility (CSR) programmes sponsored by companies to benefit the immediate communities of the companies.

(3) On an annual basis, the COMSIT directorate shall draft proposals for community-based ICT development projects for consideration by the University management.

(4) ICT development proposals shall be in tandem with the sustainable development goals of government and the strategic goals of the University.

3.10 ICT Training for Staff and Students

The rapid technology changes occurring in the ICT industry makes it expedient for personnel managing the University ICT infrastructure to undergo frequent trainings to keep up with the pace of these developmental changes. In addition to these, the continuous computerization of various pedagogic and administrative processes in the University calls for regular in-house trainings of staff and students. The Centre for Research Development and In-house Training (CREDIT) is responsible for all the in-house trainings to be carried out within the University. In addition to in-house training of staff members, the COMSIT directorate is expected to facilitate training of ICT personnel.

3.10.1 Objectives

The specific objectives of the various in-house trainings for staff and students in the University of Ilorin as they relate to ICT literacy are:

(1) to keep the University of Ilorin ICT personnel up-to-date with various ICT technologies and standards;

(2) to facilitate literacy of non-ICT staff with regards to the use of off-the-shelf and bespoke software deployed on the University ICT network;

(3) to train students on the use of the University web services and other software deployed on the University ICT network; and

(4) to keep all members of the University of Ilorin community informed of the terms and regulations in the Unilorin ICT policy.

3.10.2 Training of ICT Personnel

(1) The University management, through the COMSIT directorate and CREDIT, shall organize periodic professional in-house training programmes for ICT personnel in the University.

(2) The COMSIT directorate shall on an annual basis seek approval from the University management for various professional certifications and training programmes for ICT personnel in the University.

(3) In addition to the scheduled training programmes, the COMSIT directorate shall organize training programmes for ICT personnel on new ICT technologies and standards when such technologies are to be deployed in the University.

(4) Relevant ICT personnel in the University shall be the first to be trained on any ICT service deployed in the University.

3.10.3 Training of Other Staff

(1) CREDIT shall organize in-house training for relevant staff member on the use of new ICT services deployed in the University.

(2) For ICT facilities and services that require external training of staff, the University shall sponsor relevant staff members in the respective units and at least one ICT officer to participate in such training programmes.

(3) A training manual shall be developed for all ICT hardware and software developed within the University and circulated to all relevant units for adequate training of staff members.

(4) A training programme shall be organized for all new staff members on the University ICT infrastructure and policy.

3.10.4 Training of Students

(1) All new students shall during their orientation programme participate in a training programme on the University ICT infrastructure and ICT policy.

(2) Periodic training shall be organized for students on the use of various web services and software intended for their use on the University ICT network.

3.11 ICT Policy Enforcement

The provision of an ICT policy for the University of Ilorin is to guarantee an efficient running of the entire ICT installation and administration in the University community. To make sure that the policies instituted are strictly adhered to, there is need for the provision of an enforcement mechanism that will adjudicate adherence to the ICT policy by monitoring, evaluating, reporting and possibly correcting operations related to the University ICT infrastructure and administration. Enforcement of the University ICT policy shall fall under the purview of an ICT audit team within the COMSIT Directorate. This team will be charged with the responsibility of implementing the enforcement mechanism as provided for in the University of Ilorin ICT policy.

3.11.1 Objectives

The objectives of the ICT policy enforcement mechanism are:

(1) to provide a system of monitoring the entire University of Ilorin ICT installation and administration;

(2) to outline a method for auditing all processes within the system and evaluate their conformity to approved policy;

(3) to fashion out a protocol for reporting loopholes and violations in the ICT processes ;

(4) to provide a guideline for recommending corrective measures to authorities when loopholes and violations are detected within the system; and

(5) to ensure the documentation and implementation of approved corrective measures in the ICT system.

3.11.2 ICT Policy Enforcement Mechanism

The following is an outline of activities and protocols mapped as enforcement mechanism for the University of Ilorin ICT policy:

(1) The COMSIT Directorate shall have a system audit unit made up of ICT audit specialists who will be charged with the responsibility of enforcing the ICT policy within the University.

(2) The Unilorin ICT audit team shall have full access to all information system audit trails and shall be able to execute queries on any particular process where necessary.

(3) The ICT audit team will have complete access to ICT equipment inventory system; ICT partnership information system and all other information system created to assist enforcement of the Unilorin ICT policy.

(4) The ICT audit team shall develop a comprehensive list of facilities and processes to be audited and perform both periodic and impromptu audits on the system.

(5) The ICT audit team shall keep full documentations of all audit processes carried out within the system.

(6) The ICT audit team shall query all suspected infringements by carrying out thorough investigations involving all parties involved with such ICT facilities and processes.

(7) All substantiated violations of the ICT policy or loopholes in the system shall be officially documented and reported to the governing board of the COMSIT Directorate through the COMSIT Director.

(8) The ICT audit team shall recommend to the governing board corrective and deterrent actions that should be taken to enforce the ICT policy.

(9) After due consultations with the ICT audit team, the COMSIT Directorate governing board shall be empowered to execute any approved corrective and/or punitive measures to ensure compliance with the ICT policy.