PROPOSED

FEDERAL UNIVERSITY WUKARI
ICT STRATEGIC PLAN AND POLICY DOCUMENT

2019-2023

Version: 1.0
Status: draft
Effective Date: under review
Next Policy Review Due: after successful approval of this version

Table of Content

1.0 DEFINITION OF TERMS

Use of the terms:

- "FUW" refers to Federal University Wukari
- **"The University"** refers to Federal University Wukari and any sites associated with it.
- **"University Community"** refers to everyone (students, academic and non-academic staff) working or residing within the university environment of FUW.
- **"ICT"** refers to any communication devices, applications, network hardware and software and any associated systems.
- **"User"** refers to any persons whether staff or student accessing any ICT system owned or leased by Federal University Wukari.
- **"Service Provider"** refers to any organization or individual(s) supplying ICT products/services to Federal University Wukari.
- **"Shared account"** refers to an ICT account in use by more than one person.
- **"Director"** refers to the Director of ICT Services at Federal University Wukari.
- **"The Executive"** refers to the Vice Chancellor or any delegated authority by the VC of Federal University Wukari.
- **"Management"** refers to members of the university community who have managerial or supervisory responsibilities at Federal University Wukari whether at Faculty, Department or Institute level. This includes, but is not limited to, Deans, Chairpersons, Directors and Departmental Heads.
- **"Faculty"** members of the Academic community of FUW.
- **"TCO"** means total cost of ownership of ICT equipment, accusation, maintenance and management over the life time.
- **"CAB"** refers to change advisory board
- **"NOC"** refers to network operating centre

2.0 VISION AND MISSION OF ICT

University's ICT Vision

To provide the students, staff, and other stakeholders with the information and communication technology infrastructure and services to help achieve the university vision.

University's ICT Mission

To build and embed culture of innovation and learning, and best practices through the use of information and communication technology to establish the most hospitable environment for learning, teaching, research, and service to community.

3.0 EXECUTIVE SUMMARY

This document is the Federal University Wukari Information and Communication Technology (ICT) Strategic Plan and policies. It is a response to the evolving operational challenges and emerging ICT needs of the University.

This document recognizes the importance of ICT in the achievement of the University's vision and missions.

The ICT strategic policy is meant to leap frog the University in the implementation of its objectives is contained in the 4-year (2019-2023) strategic plan of the University (Digital Era Plan). The ICT policy, if approved, will form the basis for a 4-year implementation-planning period of the ICT for the University.

The ICT policy would place quality in teaching, learning, research, and community service. ICT requires careful planning, implementation, monitoring, management, staffing (recruitment) and capacity building. The planning process must be integrated with the organizational structure, administration, teaching and long-term goals of the University.

The document will be reviewed annually to accommodate emerging needs and technology. This document is therefore, recommended for consideration by the University administration.

This policy abides by the relevant laws and legislation of Nigeria applicable to data security and retention, copyright, and use of communication media.

4.0 INTRODUCTION

4.1 Historical Background

As a way of addressing the critical problem of qualitative access to tertiary education, the Federal Ministry of Education decided to implement the extant government policy of equitable educational development of Nigeria, by establishing federal tertiary institutions in every State of the Federation, where they do not currently exist. To this end, a memorandum was presented by the Minister of State, Education to the Federal Executive Council, at its 39th Meeting held on Wednesday, 10th November, 2010, requesting for the establishment of 44 additional tertiary institutions nationwide, to address the twin challenges of access and equitable educational development of States in the Federation.

Council in its wisdom however, approved the establishment of twelve new universities on the basis of equity and access. Nine universities were approved for take-off under Phase I of this initiative. Sequel to the above approval, a twelve-member Committee, under the chairmanship of Prof. Julius A. Okojie, Executive Secretary, National Universities Commission, was inaugurated by the Honourable Minister of State, Education, Olorogun Kenneth O. Gbagi on Thursday, 11th November 2010, to among other assignments, develop the modalities for the location and take-off of these universities.

VISION

To be leader among world class public Universities by: advancing knowledge through high quality ICT centric educational experiences for students; encouraging entrepreneurship; conducting leading edge research and scholarship in all areas that promoting an intellectual environment that is anchored on the tenets of open dialogue and inquiry, and a deep and abiding appreciation of the entire spectrum of human experience.

MISSION

To be a student's centered and community engaged institution by providing an enabling environment that enhances intellectual growth, a strong commitment to academic excellence, integrity and entrepreneurship; creating new knowledge and using ICT and other enabling technologies to solve practical problems that benefit humanity; preparing our students as well as professionals in our community for ethical leadership; and promoting service to community and enduring sense of global citizenship.

4.2Current ICT Environment at the Federal University Wukari

The Federal University Wukari commenced operation in the year 2011 with the adoption of the ICT equipment procured by the university and grants of VSAT, micro-computers and laptops from Nigerian communication commission (NCC) and the Nigeria Information Technology Development Agency(NITDA).

Since inception, the universities setup the information and communication directorate (ICT). The ICT directorate is charged with the responsibilities identifying and deploying ICT infrastructure and services for administrative, teaching, research and learning in the university. It also provides support and guidance on ICT to the university immediate and larger community.

Before the advent of the current administration, the VSATs supplied by NCC and NITDA provided slow access and low coverage of internet services within the university campus. Presently the university has upgraded its ICT facilities which provideefficient, fast internet facilities in the campus.

Wide internet linkup of radio backbone, Internet access to academic staff and key management staff is provided, but there are currently plans to extend access to students and other staff on a pay per use basis to ensure sustainability. The university also has an E-library facility that is fully automated, language laboratory for the use of its student and staff. Also the university has a functional website, student portal and a student examination facility, a computerized payroll and an on-going staff records managing software project that the university MIS unit is handling.

5.0 FUW STRATEGIC PLAN FOR INFORMATION AND COMMUNICATION TECHNOLOGY.

Information and communication technology is crucial in the seamless operation of every part of human endeavor. For the university to achieve its vision and mission, the use of information and communication technology tools is not debatable.
It is in realization of this role that the management of the ICT centre after approval of the Vice-chancellor decided to develop a strategic plan and ICT policy for the university. To be able to effectively accomplish this task, the team working on the plan undertook the analysis of the strength, challenges, opportunities and threat in the ICT sphere in the university. Identified strength are the presence of the leadership with broad perspective of ICT, available systems, learning edge infrastructure and facilities In place, communication, a staff pool that is aware of the significance of ICT, a climate that is receptive to new ICT technologies and availabilities of highly trained ICT middle level personnel and technicians. Challenges identified include poor/inadequate power supply, lack of cohesive ICT plan, non-coordination of service/effort, lack of digital classrooms, non-functional e-learning platform, poor usage of university email by staff and students.
Frequent conversion of ICT staff to other departments, inadequate funding, duplication of data, lack of ICT policy, procedure and guidelines.

Also the opportunities identified include grant and research opportunities, access to expert via internet, enhancement of student learning and assessment, distance education, access to research recourses, improvement and refinement of administrative process, promotion of student self-directed learning, partnership with other institutions and corporations, increase in internally generated revenue/ICT services and fraud control, increase access to graduate scholarship funding for local and international sources .
Finally, the threat identify include shortfall in resources accruing from government, low remuneration of ICT personnel compare to private sector, limited knowledge of ICT by ICT personnel, rapidly changing ICT technology, attaching and re-training of ICT staff, lack of coordination between ICT academic and Non-academic staff. This document present a blueprint upon which, we believe may help the university leverage the potentials of ICT to achieve its vision, mission, goals and objective.

5.1SCOPE OF THE ICT STRATEGIC PLAN

The universities ICT strategic plans include all major information and communication technology planning, requirement and investment of the university. It will cover the strategic direction, implementation and management of ICT related current and emerging technology and devices. The strategic plan and policy will serves as a framework for all stakeholders to leverage ICT in the delivery of the university's services.
The major principles which will guide the success of the strategic plan are as follows:-
While the plan is intended to be a four years view of FUW ICT strategic plan, it should be seen as an on-going process. Thus, it can be revisited and revised in reaction to new trends and emerging technologies, new business requirements or changing objectives and directions.

Also project success and failure are to be used to help fine tune the plan and policy to make it up to date.
Secondly, the strategic document should be seen as university's plan and not the administration plan. University wide discussion and acceptance of the document will ensure wide spreads ownership of the document.
The plan envisages that the following key attribute will guide the design, development and implementation of the university's ICT infrastructure.

- Security: Ensure data and services are not compromised.
- Scalability: ICT infrastructures designed to allow for growth and expansion.
- Resilience: Infrastructure and services can tolerate a degree of failure.
- Recoverability: Services can be made available as soon as possible after failure.
- Manageability: ICT infrastructures and services can be managed cost effectively. The total cost of ownership is a key consideration when selecting and recommending ICT systems for adoption
- Interoperability: System and software will be built or designed in a manner that they can interoperate seamlessly.

Finally, Planning, Implementation, Review and improvement will be a key principle in all ICT projects in the university.

5.2POLICIES APPLICATION

This policy document applies to all users and service providers of ICT services.

- The **Equipment Use Policy** applies to staff, students or guests of the University who make use of any ICT equipment owned or leased by the University.
- The **Internet/Email User Policy** apply to staff and students who access the University's Internet and mail facilities.
- The **Password Policy** applies to all users of the University's ICT services.
- The **Hardware Acquisition and Maintenance Policy** applies to all staff responsible for acquiring hardware on behalf of the University and those responsible for maintenance and repairs of this hardware.
- The **Software Policy** applies to staff responsible for acquisition and maintenance of software.
- The **Change Management Policy** applies to managers of departments and ICT staff responsible for acquisition and maintenance of systems which support the corporate functions of the University.
- The **Information Security Policy** applies to all users of the University's ICT services.
- The **Use of Social Networking Sites Policy** applies to all users who access social networking sites using the University ICT resources, including but not limited to Facebook, Skype, and Google Talk.
- The **Bring Your Own Device Policy** applies to all members of the University community, staff and students included who will use their own personal electronic devices, which include but are not limited to laptops and smart-phones to access University ICT resources or to do official University business.

- The Information Security Policy applies to all users of ICT in the University and those responsible for the setting up and maintenance of ICT infrastructure.
- The Service Provider Policy applies to all organizations or individuals who are external to the University but provide ICT services to the University.
- The E-Learning Policy applies to staff providing learning materials and those accessing learning materials on the E-learning platform.
- The Network and Infrastructure policy applies to all users of ICT and personnel responsible the maintenance of the network.

6.0 ICT LAWS AND LEGISLATION in Nigeria

This policy abides by the relevant laws and legislation of Nigeria applicable to data security and retention, copyright, and use of communication media.

7. 0 PRINCIPLES, GOALS AND STRATEGIES

Guiding Principles

The idea of information technology/digital development is based on the hypothesis that the communities we are working for actually use ICT tools and that these instruments can create new opportunities for change and transformation of the socio-economic context. A project has to be thought, structured and implemented for and with the beneficiaries of the new product or the service provided. The following principles will provide a cohesive approach to information technology.

1. ICT is a vital service.
2. ICT is an essential resource for learning, teaching, research, and community partnership.
3. ICT is essential for data and information management
4. ICT TCO and security should be a major consideration in all ICT investment
5. ICT is a strategic University asset, capital intensive and must be effectively and efficiently funded.
6. ICT is essential for communication, partnership, and collaboration
7. ICT is capital intensive, thus an effective mechanism must be evolved to fund and appraise ICT funded provisions.

Principle 1: ICT is a vital service

ICT is central for the achievement of the vision and mission of the University. It is provide infrastructure and tools for ensuring quality learning, teaching, research and service delivery to the university community.

The following goals and strategies are vital.

Goal 1.1.: Develop and implement systematic process for need assessment of information technology architecture, standards, and support.

Strategies:

1. Map existing infrastructure and identify inequities among units, sub-unit, and develop short and long range plan.
2. Survey academic and non-academic staff and students to determine their information and communication technology needs.
3. Assess, recommend, and implement a University wide infrastructure to further provide opportunities for University to leverage on ICT potentials.
4. Providing uninterrupted power supply for effective use of ICT.

Goal 1.2.: Develop, implement and continuously update University-wide architecture and standards to optimize efficiency, effectiveness and support.

Strategies:

1. Create working team to monitor and upgrade ICT architecture and standards on regular basis.
2. Develop proactive research and development unit for evaluation and application of new technologies for the University community.
3. Develop standard operating procedure to optimize the use of site licensing for software acquisition.
4. EstablishNetwork Operating Centre
5. Develop and implement fibre and wirelesscampus-wide fiber-optic cable system.
6. Develop and implement internet backbone (fibre) i.e. Internet bandwidth.
7. Develop central software licensing service together with remote software update service.

Goal 1.3.: Provide access to ICT to Staff and Students from all University Locations and off Campus.

Strategies:

1. Use leading-edge technology to provide reliable and high speed intranet access for University staff, students, and other stakeholders.
2. Connect all buildings (office), lecture theatres, classrooms, etc., to ICT infrastructural resources.
3. Provide wireless environment and appropriate use policy for internet.
4. Provide flexible access options to ICT services on campus and within the University precincts for University and privately owned devices.
5. Provide Intranet and Internet connectivity off campus for staff and students.

Goal 1.4.: Provide seamless, integrated support-from a financial and human resources for ICT related issues across campuses, college, faculties, and departments.

Strategies:

1. Establish synergistic relationship among academic units, Departments, administrative units.
2. Develop and maintain an online, shared database of ICT issues and solutions, that is, bulletin board, workgroup, and discussion group.
3. Provide support services that are easy to use and readily responsive to user needs.
4. Establish and conduct a user-forum for leveraging and maximizing ICT support on campus.
5. Develop and maintain an online reference for common information technology issues, that is, frequently Asked Questions (FAQ).
6. Provide appropriate learning opportunities for staff and students to develop and improve on basic level of ICT knowledge, skills, and abilities.

7. Provide online form for user feedback that is directed at the higher level of the Faculties and Directorate.

Principle 2: ICT is an essential resource for learning, teaching, research, and community partnership.

Goal 2.1.: Use ICT to improve the learning environment.
Strategies:

1. Provide opportunities and support for the creative use of information and communication technology to improve learning
2. Establish an ICT based instructional development centre for direct support of academic and non-academic staff.
3. Continue to equip and systematically upgrade appropriate campus locations (lecture theaters, classrooms, conference rooms, board rooms, laboratories) with necessary hardware and software for instructional delivery.
4. Provide opportunities for staff training and certification to develop knowledge, skills, and abilities related to e-learning and learning management system.

Goal 2.2.: Extend the University Reach through Distance Education.
Strategies:

1. Evaluate online delivery trend of distance education and implement as appropriate.
2. Provide necessary training and support for academic staff who seek to integrate distance education methods in their courses and other instructional activities.

Goal 2.3.: Support discipline specific ICT need for Research.
Strategies:

1. Enable enhancement of research technique and collaboration through improvement of infrastructure.
2. Establish and maintain computationally-intensive/high end computing for support of research and instructional activities.
3. Provide specifically-trained personnel to support high end applications for University community.

Goal 2.4.: Facilitate technological partnership with the educational community, businesses and other organizations.
Strategies:

1. Develop appropriate partnership with commercial vendor for proprietary products.
2. Develop appropriate partnership for leveraging on ICT using open source products.
3. Maximize collaborative external grants efforts
4. Share equipment and expertise with technology partners and Higher Educational Institutions (HEIs).

5. Evaluate the potentials of FUW to serve as resource to external organization and institutions and leverage such potentials.

Goal 2.5.: Use ICT to automate library services.
Strategies:

1. Computerize library archiving system.
2. Provide computerized services for library users. .
3. Provide essential access to electronic versions of books and journals, and digital instructional multimedia. .
4. Provide virtual library services through Intranet and Internet access. (E-library)

Goal 2.6.: Use ICT to support students with diverse learning needs.
Strategies:

1. Evaluate ICT needs of students with disability.
2. Provide assistive ICT facilities and infrastructure for students with disabilities.
3. Provide necessary software for the needs of students with disability.

Principle 3: ICT is essential for data and information management

Goal 3.1.: Provide effective administrative systems.
Strategies:

1. Evaluate the functionality of existing administrative systems and upgrade/replace as necessary.(Enterprise resources management)
2. Provide training for administrative applications.
3. Expedite the implementation of an integrated student information system.
4. Implement staff integrated information system.

Goal 3.2.: **Standardize, integrate and maintain integrity of institutional data**.
Strategies:

1. Incorporate best practices in database technology.
2. Build logical links to minimize frequency of data collection.
3. Provide transaction data with effective dating, where necessary, and maintain on-line history.
4. Build standard data definition across multiple applications.
5. Develop process to validate data on a regular and consistent basis to ensure accuracy.
6. Develop standards by application, for purging an archiving data.
7. Develop federated, shared, managed, archived, and back-up file store of data on students, staff, and administrative issues.

Goal 3.3.: **Expand access to institutional data as appropriate**.
Strategies:

1. Develop and use electronic forms where applicable.
2. Provide expanded reporting tools and report dissemination methods.
3. Implement electronic document management system for institutional distribution of documents.

Principle 4: ICT TCO and security should be a major consideration in all ICT investment

Goal 4.1.: Implement and maintain data administration and security policies and procedures.
Strategies:

1. Comply with laws and regulations (Nigeria), policies and procedures governing the confidentiality and protection of privacy.
2. Protect information through effective University security policies and procedures through the development of a campus-wide use agreement for all individuals with access to the University data.
3. Develop agreement and awareness of what constitute institutional data; addressing the concerns about departmental ownership of data.
4. Train users on awareness of good security practices
5. To ensure adequate TCO of all ICT investment are undertaking before adoption

Goal 4.2.: **Prevent unauthorized access to University network. (Firewall)**
Strategies:

1. Provide technology to protect against ICT security risk and unauthorized access.

Principle 5: ICT is a strategic University asset, capital intensive and must be effectively and Goal efficiently funded.

Goal 5.1.: Establish and maintain competitive edge through the effective and innovative se of ICT resources.

Strategies:

1. Provide leadership to encourage effective use of ICT.
2. Develop and implement a system of assessing and improving ICT processes and services with input from the University community.
3. Use ICT to attract and retain students.
4. Use ICT to help place students in jobs upon graduation.
5. Provide staff with space for personal web pages.(blogs, wiki and Google Apps)

Goal 5.2.: Attract and retain technology savvy staff.

Strategies:

1. Provide necessary ICT resources for technology savvy staff (ICT hardware, peripherals, and software application).
2. Provide professional recognition for teaching, learning, research, and administrative initiatives using ICT.
3. Tenure and promotion criteria to include innovative use of ICT.
4. Strengthen the ICT Management Unit.

Goal 5.2.: Establish exemplary web presence that showcases FUW as a foremost student-centered teaching and research institution.

Strategies:

1. Research opportunities for leveraging the Internet to better serve University goals.
2. Develop the image FUW wants to portray and develop standards to assure consistency of that image.
3. Hire and retain qualified staff who can create and maintain an active web site.
4. Implement a procedure to integrate and update data via the web site.
5. Develop a system to serve customized pages to a variety of users.
6. Encourage academic staff to develop web based learning materials using various ICT tools.

Goal 5.3 Develop measures to access the funding needs of users across the University.

Strategies:

1. Evaluate priority of users for central ICT investment.
2. Provide a breakdown of on-going operational expenditure and a descriptive and prioritized list of new ICT investment.
3. Develop a five-year development budget plan on ICT expenditure

4. Invest in central ICT which provide users with needed ICT environment.

5. Ensure adequate funding of ICT to ensure high priority ICT services are resilient, robust, scalable and reliable.

6. Develop voluntary purchasing mechanism for staff and students to make purchases from a set of companies within an overall framework, and can be shared with other institutions.

Goal 5.4. Ensure mechanism for regular appraisal of expenditure on ICT.

Strategies:

1. Develop mechanism to ensure that the University receives favourable ICT investment conditions from vendors.

2. Establishing a process for appraising central expenditure on ICT in teaching, learning, research, and administration.

3. Appraising expenditure on ICT at unit levels.

Goal 5.5.: Consider alternative sources of funding for ICT development, apart from government funding.(Google, multilateral organization and international donors)

Strategies:

1. Development of proposals for potential donors for acquisition of hardware and development of ICT projects

2. Introduction of ICT levy on students (undergraduate and graduate) for ICT use and access

3. Running of ICT related workshops, short programmes, and training.

4. Providing consultancy ICT services.

5. Engagement in joint ventures with software development organizations, husbanding the library fund for the development of e-library.

6. Dedicating a certain percentage of IGR into institutional ICT development.

7. Source for corporate and governmental agencies (e.g. TETFUND, NITDA, NCC and PTDF) funding of major ICT projects.

8. Pursuance of vendor "In Kind" for technology purchases and upgrade across the University.

9. **Principle 6:** ICT is essential for communication, partnership, and collaboration.

Goal 6.1.: Develop and provide systems and tools to enable units, department and individuals to collaborate across disciplines and institutions. .

Strategies:

1. Analysis of current collaboration practices, within and outside the University.
2. Provide the platform for researchers to collaborate with groups external to University.
3. Provide desktop audio and video conferencing capabilities and collaborative technology.
4. Develop central depository for digital objects for research output.
5. Develop interoperability between institutional, national, and infrastructure to support collaboration and partnership. i.eNgREN

Ensure seamless interoperability with ICT delivered services by units (ICT, Library, facility and Department etc)

8.0 Key Action Programme

KEY STRATEGIC INITIATIVES

Quality Assurance Framework based on Planning, Implementation, Review, and Improvement methodology should be adopted for the Strategic Plan and to accommodate executed projects and on-going ICT activities.

Principle 1: ICT is a vital service

Goal 1.1.: Develop and implement systematic process for need assessment of information and communication technology architecture, standards, and support.

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
1. Map existing infrastructure and identify inequities among units, sub-unit, and develop short and long range plan.	Develop assessment and evaluation instrument on ICT infrastructure Develop short and long range plan for ICT infrastructural development	i. ICT steering Committee ii. ICT Centre i. ICT steering Committee ii. ICT Centre iii. University Administration	2019 to 2020	Planning
2. Survey academic and non-academic staff and students to determine their information and communication technology needs.	i. Develop assessment and evaluation instrument on staff and students' ICT needs ii. Develop the curriculum on staff and students' ICT needs. ii. Develop	i. ICT steering Committee ii. ICT Centre	2019 to 2020	Planning
3. Assess, recommend, and implement a University wide infrastructure to further provide opportunities for University to leverage on ICT potentials	i. Based on 1 and 2 strategies above develop a working plan for development of ICT infrastructure	i. ICT steering Committee ii. ICT Centre iii PPU and Works iv. University Administration	2019 to 2020	Planning

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
4. Providing uninterrupted Power Supply for effective use of ICT.	i. Provision of alternative electricity through generating sets, solar power, wind power, etc. ii. Explore and deploy solar powered hardware (laptops and projectors).	APU/Works/ University Management/ Council/Works Dept./APU APU/PPU/Works/ DVC(MS)	2019 to 2020	Planning Planning

Goal 1.2.: Develop, implement and continuously update University-wide architecture and standards to optimize efficiency, effectiveness and support.

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
7. Create working team to monitor and upgrade ICT architecture and standards on regular basis.	i. Establishment of Unit based ICT Committees ii. Establishment of University wide ICT steering committee	i. Dean of Faculty and Heads of non-academic Units i. University Administration	2019 to 2020	Planning
8. Develop proactive research and development unit for evaluation and application of new technologies for the University community.	i. Constitute core experts to develop and implement researches and evaluate the application of new technologies	University Administration	2019 to 2020	Planning
9. Develop standard operating procedure to optimize the use of site licensing for software acquisition.	i. Develop the standard document for University wide application	i. ICT steering Committee ii. ICT Centre	2019 to 2020	Planning
10. Establishing a Network Operating Centre	i. Construct a state- of- the- art- Network Centre ii. Install state- of- the- art servers, including back-up	 i. ICT steering Committee	2019 to 2020	Planning

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
	servers Install communication base stations to facilitate effective telephone access.	ii. ICT Centre iii. PPU and works iii. University Administration iv. Council		
11. Develop an optical intranet through a campus-wide fiber-optic cable system.	i. Lay fibre optic cables to cover the built-up part of the University. ii. Full networking of the academic and administrative building campus wide.	i. ICT steering Committee ii. ICT Centre iii. PPU and works iii. University Administration iv. Council i. ICT steering Committee ii. ICT Centre iii. PPU and works iii. University Administration iv. Council	2019 to 2020 2019 to 2020	Planning Planning
12. Install a robust internet backbone.	i. Install appropriate V-Sat ii Increase Internet bandwidth (minimum 10GB upload/ download) iii. Ensure affordable internet access to the University community iv. Increase Internet bandwidth (minimum 10GB upload/download)	 i. ICT steering Committee ii. ICT Centre iii. PPU and works iii. University Administration iv. Council	2019 to 2020 2019 to 2020 2019 to 2020 2019 to 2020	(On going) Planning Planning

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
13. Develop central software licensing service together with remote software update service.	i. Develop the standard document for University wide application ii. Initiate Central software licensing	i. ICT steering Committee ii. ICT Centre iii. PPU and works iii. University Administration iv. Council	2019 to 2020	Planning

Goal 1.3.: Provide ICT access to Staff and Students within the University Campus.

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
1. Use leading-edge technology to provide reliable and high speed intranet access for University staff, students, and other stakeholders.	i. Development of core University Intranet Services	i. ICT steering Committee ii. ICT Centre iii. University Administration	2019 to 2020	Planning
2. Connect all buildings (office), lecture theatres, classrooms, etc., to ICT infrastructural resources.	i. Ensure cabled/wireless connection to offices, lecture theatres, classrooms, etc.	i. ICT Steering Committee ii. ICT Centre iii. PPU and works iii. University Administration iv. Council	2019 to 2020	Planning
3. Provide wireless environment and appropriate use policy for internet.	i. Deploy wireless infrastructure for on-campus roaming for staff, students and authorized guests	i. ICT Steering Committee ii. ICT Centre iii. PPU and works iii. University Administration iv. Council	2019 to 2020	Planning

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
4. Provide flexible access options to ICT services on campus and within the University precincts for University and privately owned devices.	i. Develop spaces to support approaches to students-centered learning, that is, Flexible Learning Spaces	i. ICT Steering Committee ii. ICT Centre, iii. PPU and works iii. University Administration iv. Council	2019 to 2020	Planning
5. Provide Intranet and Internet connectivity off campus for staff and students.	i. Deploy wireless infrastructure for off campus access Intranet and Internet connectivity off campus for staff and students.	i. ICT Steering Committee ii. ICT Centre, iii. PPU and works iii. University Administration iv. Council	2019 to 2022	Planning

Goal 1.4.: Provide seamless, integrated support-from a financial and human resources for ICT related issues across campus, college, faculties, and departments.

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
1. Establish synergistic relationship among academic units, Departments, ICT Centre, administrative units, and Department of computer Sciences.	i. Establish central coordinating committee for synergistic relationship. ii. Develop areas of collaboration among the Units.	i. ICT Steering Committee ii. ICT Centre	2019 to 2022	Planning
2. Develop and maintain an online, shared database of ICT issues and solutions, that is, bulletin board, workgroup, and discussion group.	i. Development of online shared database	i. ICT steering Committee ii. ICT Centre	2019 to 2020	Planning

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
3. Provide support services that are easy to use and readily responsive to user needs.	i. Provide support bases across the Faculties, Units, and campuses	i. ICT steering Committee ii. ICT Centre	2019 to 2020	Planning
4. Establish and conduct a user-forum for leveraging and maximizing ICT support on campus.	i. Establish of the user-forum for stakeholders support	ICT Steering Committee ii. ICT Centre	2019 to 2020	Planning
5. Develop and maintain an online reference for common information technology issues, that is, frequently Asked Questions (FAQ).	i. Development of FAQ by ICT units ii. Consideration and editing of FAQ	i. ICT Steering Committee ii. ICT Centre iii. Department of Computer Sciences	2019 to 2020	Planning
6. Provide appropriate learning opportunities for staff and students to develop and improve on basic level of ICT knowledge, skills, and abilities.	i. Development of curriculum for staff and students. ii. Implementation of developed staff curriculum. iii. Implementation of specific user ICT programme based on discipline needs.	i. ICT Steering Committee ii. ICT Centre iii. Department of Computer Sciences	2019 to 2020	Planning
7. Provide online form for user feedback that is directed at the higher level of the ICT Directorate.	i. Development of online form for user feedback. ii. Analysis of user feedback for improved service delivery	i. ICT Steering Committee ii. ICT Centre	2019 to 2020	Planning

Principle 2: ICT is an essential resource for learning, teaching, research, and community partnership.

Goal 2.1.: Use ICT to improve the learning environment.

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
1. Provide opportunities and support for the creative use of information and communication technology to improve learning.	i. Encourage blended teaching where ICT supplement traditional instruction. ii. Provide necessary tools, hardware, and software for course development. iii. Lecturers to be encouraged to produce their lecture for web	i. ICT Steering Committee ii. ICT Centre, iii. PPU and works iii. University Administration iv. Council i. ICT Steering Committee ii. ICT Centre, iii. University Administration	2019 to 2020 2019 to 2020 2019 to 2020	Planning Planning Planning
2. Establish an ICT based instructional development centre for direct support of lecturers and other staff ICT project.	i. Establishment of ICT based instructional development centre	i. ICT Steering Committee ii. ICT Centre, iii. University Administration	2019 to 2020 2019 to 2020	Planning Planning
3. Continue to equip and systematically upgrade appropriate campus locations (lecture theaters, classrooms, conference rooms, board rooms, laboratories) with necessary hardware and software for	i. Provision of ICT hardware and software in lecture theaters, classrooms, conference rooms, board rooms, laboratories for instructional purposes. ii. Provision of support staff for ICT hardware in instructional settings	i. ICT Steering Committee ii. ICT Centre, iii. University Administration i.ICT Steering committee ii. ICT Centre,	2019 to 2020 2019 to 2020	Planning Planning

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
instructional delivery.				
4. Provide opportunities for staff training and certification to develop knowledge, skills, and abilities related to e-learning and learning management system.	i. Organization of workshops on ICT based instructional material development.	i.ICT Steering Committee ii. ICT Centre.	2019 to 2020	Planning

Goal 2.2.: Extend the University Reach through Distance Education.

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
1. Evaluate online delivery trend of distance education and implement as appropriate.	i. Encourage the development of e-learning packages for blended teaching where ICT supplement traditional instruction. ii. Organization of workshop on distance education.	i. ICT Centre, ii. University Administration	2019 to 2020 2019 to 2020	Planning Planning
2. Provide necessary training and support for academic staff who seek to integrate distance education methods in their courses and other instructional activities.	i. Organization of workshops on ICT based instructional material development for distance education. ii. Commencement of ICT based distance education programme.	i. ICT steering Committee ii. ICT Centre, i. ICT Steering Committee ii. ICT Centre, iii. University Administration	2019 to 2020 2019 to 2020	Planning Planning

Goal 2.3.: Support discipline specific ICT need for Research.

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
1. Enable enhancement of research technique and collaboration through improvement of infrastructure.	i. Survey of existing ICT research infrastructure across the University ii. Development of ICT research infrastructure	i. ICT steering Committee ii. ICT Centre iii. University Administration. i. ICT steering Committee ii. ICT Centre iii. University Administration.	2019 to 2020 2019 to 2020	Planning Planning
2. Establish and maintain computationally-intensive/high end computing centre for support of research and instructional activities.	i. Establish FUW e-Research Centre (eFUWRC) as facilitator for e-Research. ii. Develop a Virtual Research Environment to offer interoperability between data resources, computer facilities, research repositories, and applications. Explore simulated research Laboratory collaboration with international reputable Global universities.	i. University Administration. i. ICT steering Committee ii. ICT Centre iii. Department of computer Sciences. iv. University Administration.	2019 to 2020 2019 to 2020	Planning Planning
3. Provide specifically-trained personnel to support high end applications for University community.	i. Train core ICT professionals to support ICT application in research.	i. ICT steering Committee ii. ICT Centre iii. Department of computer science iii. University Administration.	2019 to 2020	Planning

Goal 2.4.: Facilitate technological partnership with the educational community, businesses and other organizations.

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
1. Develop appropriate partnership with commercial vendor for proprietary products.	i. Identification of appropriate vendors for partnership.	i. ICT steering Committee ii. ICT Centre iii. Department of computer Sciences. iii. University Administration.	2019 to 20202 2019 to 2020	Planning Planning
	ii. Establishing framework with identified research institutions using necessary MOU	i. ICT steering Committee ii. ICT Centre iii. University Administration.		
2. Develop appropriate partnership for leveraging on ICT using open source products.	i. Identification of appropriate open source for institutional application.	i. ICT steering Committee ii. ICT Centre iii. Department of computer Sciences.	2019 to 2020 2019 to 2020	Planning Planning
	ii. Training of ICT professionals' in the development and application of open source materials.	i. ICT steering Committee ii. ICT Centre iii. Department Computer Sciences.	2019 to 2020	Planning
	iii. ICT professionals' participation in open source projects.	i. ICT steering Committee ii. ICT Centre iii. Department of Computer Sciences.		
3. Maximize collaborative external grants efforts	i. Organisation of workshop on grantmanship and proposal writing	i. ICT steering Committee ii. ICT Centre	2019 to 2020	Planning
4. Share equipment and expertise with technology partners and Higher	i. Collaborate and share equipment with HEIs	i. ICT Steering Committee ii. ICT Centre iii. University	2019 to 2020	Planning

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
Educational Institutions (HEIs).	ii. Enhance participation in ngNOG and other ICT related organizations in Nigeria	Administration. i. ICT Steering Committee ii. ICT Centre iii. University Administration.	2019 to 2020	Planning
5. Evaluate the potentials of FUW to serve as resource to external organization and institutions and leverage such potentials.	i. Identify potential areas the University personnel can serve as resources for other institutions	ICT Steering Committee ii. ICT Centre iii. University Administration.	2019 to 2020	Planning

Goal 2.5.: Use ICT to automate library services.

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
1. Computerize library archiving system.	i. Implement the computerization of the library activities iii. Optimize the use of university e-library iv. Develop and implement the university e-library for the use of student and staff within the campus.	i. ICT Centre, ii. FUW Library. iii. University Administration	2019 to 2020	planning
2. Provide computerized services for library users.	i. Provided an automated library management system ii. Provide needed training for library staff on ICT	i. ICT Centre, ii. FUW Library. iii. University Administration	2019 to 2020	Planning

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
	integration in Library iii. Implement new Library Management System			
ICT Strategies	**Initiatives**	**Responsibility**	**Time Frame**	**Phase**
3. Provide essential access to electronic versions of books and journals, and digital instructional multimedia.	i. Survey staff and students e-books, journals, and digital learning materials. i. e-books, journals, and digital learning materials.	i.ICTCentre, ii. FUW Library. iii. University Administration i. ICT Centre, ii. FUW Library. iii. University Administration	2019 to 2020 2019 to 2020	Planning Planning
4. Provide virtual library services through Intranet and Internet access.	i. Plan 24x7 access to library and information services. ii. Develop interoperability standards for close collaboration with other ICT units in the University, and other libraries	i. ICT Centre, ii. FUW Library. iii. University Administration i. ICT Centre, ii. FUW Library. iii. University Administration	2019 to 2020 2019 to 2020	Planning Planning

Goal 2.6.: Use ICT to support the learning of students with diverse learning needs.

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
1. Evaluate ICT needs of students' with disability.	i. Survey the number and categories of students with disabilities. ii. Develop assessment and evaluation instrument on ICT infrastructural, hardware, software needs of students with disabilities.	i. ICT Centre, ii. University Administration i. ICT Centre, ii. University Administration	2019 to 2020 2019 to 2020	Planning Planning

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
2. Provide assistive ICT facilities and infrastructure for students' with disabilities.	i. Implement the provision of assistive ICT facilities and infrastructure for students' with disabilities	i. ICT Centre, ii. University Administration	2019 to 2020	Planning
3. Provide necessary software for the needs of students' with disability.	i. Train staff assisting the students with disabilities on the use of assistive ICT. ii. Implement the provision of assistive ICT software for students with disability.	i. ICT Centre, ii. University Administration	2019 to 2020	Planning

Principle 3: ICT is essential for data and information management

.

Goal 3.1.: Provide effective administrative systems.

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
1. Evaluate the functionality of existing administrative systems and upgrade/replace as necessary.	i. Survey existing application of ICT in information management. ii. Upgrade/replace existing systems with a view to have seamlessly integrated management information system(enterprise resources system)	i. ICT steering Committee ii. ICT Centre, i. ICT steering Committee, ii. ICT Centre iii. University Administration	2019 to 2020 2019 to 2020	Planning
2. Provide training for administrative applications.	i. Organization of training and workshops n ICT application for administrative purposes.	i. ICT Centre, ii. ICT steering Committee iii. University Administration	2019 to 2020	Planning
3. Expedite the implementation of an integrated student information system (Student Portal)	i. Improvement on students' information system	i. ICT Centre, ii. ICT steering Committee iii. University Administration	2019 to 2020	Done
4. Implement integrated staff information system (Staff Portal)	i. Implementation of integrated staff information system	i. ICT Centre, ii ICT steering Committee iii. University Administration	2019 to 2020	planning

Goal 3.2.: Standardize, integrate and maintain integrity of institutional data.

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
1. Incorporate best practices in database technology.	i. Develop database technology based on best practices	i. ICT Centre, ii. ICT steering Committee iii. University Administration	2019 to 2020	Planning
2. Build logical links to minimize frequency of data collection.	i. Develop platform for the integration of students and staff management information systems	i. ICT Centre, ii. ICT steering Committee iii. University Administration	2019 to 2020	Planning
3. Provide transaction data with effective dating, where necessary, and maintain on-line history.	i. Implement data transaction standards.	i. ICT Centre, ii. ICT steering Committee iii. University Administration	2019 to 2020	Planning
4. Build standard data definition across multiple applications.	i. Implement the building of standard data definition across multiple applications.	i. ICT Centre, ii. ICT steering Committee iii. University Administration	2019 to 2020	Planning
5. Develop process to validate data on a regular and consistent basis to ensure accuracy.	i. Implement the process to validate data on a regular and consistent basis to ensure accuracy	i. ICT Centre, ii. ICT steering Committee	2019 to 2020	Planning
6. Develop standards by application, for purging and archiving data.	i. Implement the process to develop standards by application, for purging and archiving data	i. ICT Centre, ii. ICT steering Committee	2019 to 2020	Planning
7. Develop federated, shared, managed, archived, and back-up file store of data on	i. Implement the acquisition of servers and back-up file store of data.	i. ICT Centre, ii. ICT steering Committee iii. University Administration	2019 to 2020	Planning

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
students, staff, and administrative issues.				

Goal 3.3.: Expand access to institutional data as appropriate.

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
1. Develop and use electronic forms where applicable.	i. Develop appropriate electronic forms for staff and students information management system, admission, transfer, awards, etc.	i. ICT Centre, iii. University Administration	2019 to 2020	Planning
2. Provide expanded reporting tools and report dissemination methods.	i. Implement e-feedback for students on performance in courses and annual performance. ii. Implement digital provision of academic transcript and confirmation of results. iii. Develop digital centralized computation of students' results.	i ICT Centre, ii. Academic Office iii. University Administration	2019 to 2020	Implementation Implementation implementation
3. Provide electronic document management system for institutional distribution of documents.	i. Implement electronic document management system for institutional distribution of documents (minutes of meetings, senate proceedings, circulars, bulletins, pay-slip, etc.).	i. ICT Centre ii. ICT steering Committee iii. University Administration i. ICT Centre ii. Information Directorate	2019 to 2020	planning planning

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
	ii. Disseminate information via the University web site (authorized access for classified documents)	iii. University Administration		

Principle 4: ICT TCO and security should be a major consideration in all ICT investment

Goal 4.1.: Implement and maintain data administration and security policies and procedures.

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
1. Comply with laws and regulations, policies and procedures governing the confidentiality and protection of privacy.	i. Implement laws and regulations, policies and procedures governing the confidentiality and protection of privacy	i. ICT Centre ii. Legal Unit iii. University Administration	2019 to 2020	Planning
2. Protect information through effective University security policies and procedures through the development of a campus-wide use agreement for all individuals with access to the University data.	i. Development of laws and regulations for individuals with access to University data. ii. Implementation of international, national, and institutional confidentiality and protection of privacy	i. ICT Centre ii. Legal Unit iii. University Administration i. ICT Centre ii. Legal Unit iii. University Administration	2019 to 2020 2019 to 2020	Planning
3. Develop agreement and awareness of what constitute institutional data; addressing the concerns about	i. Implement agreement and awareness of what constitute institutional data. ii. Define individual and institutional ownership of	i. ICT Centre ii. Legal Unit iii. University Administration	2019 to 2020 2019 to 2020	Planning

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
departmental ownership of data.	data			
4. Train users on awareness of good ICT security practices.	i. Organize workshop to train users on good security practices and issues. ii. Continuously maintain an active education programme with all ICT users(bulletin boards)	i. ICT steering Committee ii. ICT Centre iii. Legal Unit iv. University Administration	2019 to 2020 2019 to 2020	Planning

Goal 4.2.: Prevent unauthorized access to University network.

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
1. Provide technology to protect against ICT security risk and unauthorized access.	i. Provide leading edge anti-virus product for individual users.	i. ICT Centre ii. University Administration	2019 to 2020	Implementation
	ii. Install bandwidth manager to prevent unauthorized access to network.	i. ICT Centre ii. University Administration	2019 to 2020	Planning
	iii. Provide firewall to allow appropriate traffic and block inappropriate traffic.	i. ICT Centre ii. University Administration	2019 to 2020	Planning
	iv. Provide Intrusion Prevention Systems which detect and stops attacks in real time.	i. ICT Centre ii. University Administration	2019 to 2020	Planning
	v. Put in place necessary Network Admission Control, which ensures network devices are safe before they are allowed access in the University network resources.			

Principle 5: ICT is a strategic University asset capital intensive and must be effectively and efficiently funded.

Goal 5.1.: Establish and maintain competitive edge through the effective and innovative use of ICT resources.

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
1. Provide leadership to encourage effective use of ICT.	i. Develop core ICT users across Faculties, Departments, and Units, who can model good use of ICT	i. ICT Centre ii. ICT steering Committee ii. University Administration	2019 to 2020	Planning
2. Develop and implement a system of assessing and improving ICT processes and services with input from the University community.	i. Design assessment instrument that is administered regularly to harvest input from University community	i. ICT Centre ii. steering Committee ii. University Administration	2019 to 2020	Planning
3. Use ICT to attract and retain students.	i. Development of robust ICT environment and maintenance for attracting. ii. Introduce more ICT related courses (e.g. Computer Engineering, Computer Education) and computer application contents in courses.	i. ICT Centre ii. ICT steering Committee ii. University Administration i. Computer Science Department ii. Academic planning iii. University Administration	2019 to 2020 2019 to 2020	Implementation Planning
4. Use ICT to help place students in jobs upon graduation	i. Track job market and assist graduating students to access job information. ii. Provide students with job relevant skills	i. Academic planning ii. University Administration	2019 to 2020	Planning

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
5. Provide staff with space for personal web pages.	i. Encourage staff to develop and host personal web pages attached to the University web site.	i. ICT Centre ii. ICT steering Committee ii. University Administration	2019 to 2020	Planning

Goal 5.2.: Attract and retain technology savvy staff.

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
1. Provide necessary ICT resources for technology savvy staff (ICT hardware, peripherals, and software application).	i. Improve ICT resources for technology savvy staff.	i. ICT Centre ii. ICT steering Committee ii. University Administration	2019 to 2020	Planning
2. Provide professional recognition for teaching, learning, research, and administrative initiatives using ICT.	i. Encourage staff development in the area of ICT use for teaching, learning, research, and administrative purposes. ii. Provide necessary ICT resources for teaching, learning, research, and administrative purposes.	i. ICT Centre ii. ICT steering Committee ii. University Administration i. ICT Centre ii. ICT steering Committee ii. University Administration	2019 to 2020 2019 to 2020	Planning Planning
3. Tenure and promotion criteria to include innovative use of ICT.	i. Develop criteria for including innovative use of ICT in staff promotion.	i. ICT Centre ii. ICT steering Committee iii. University Administration iv. Council	2019 to 2020	Planning

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
4. Strengthening the ICT Management Unit	i. Provide appropriate infrastructure for operations of the ICT Centre	i. ICT Centre ii. ICT steering Committee iii. University Administration iv. Council	2019 to 2020 2019 to 2020	planning
	ii. Employ staff with demonstrable capacity for the various functions expected of the ICT Centre.	i. ICT Centre ii. ICT steering Committee iii. University Administration iv. Council	2019 to 2020	Review and Improvement
	iii. Provide in-house and external continuous professional training for ICT Centre staff	i. ICT Centre ii. ICT steering Committee iii. University Administration iv. Council		Improvement

Goal 5.3.: Establish exemplary web presence that showcases FUW as a foremost student-centered teaching and research institution.

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
1. Research opportunities for leveraging the Internet to better serve the University goals.	i. Encourage lecturers to leverage internet potentials in their research. ii. Host all lecturers' publications and research briefs (on-going, mimeographs, unpublished) on University site.	i. Individual lecturers ii. Faculties iii. University administration i. ICT Centre ii. University administration	2019 to 2020	Implementation planning
2. Develop the image Unilorin wants to portray and develop standards to assure consistency of that image.	i Redesign the university web page towards meeting the global international institutional standards	i. ICT Centre ii. University Administration	2019 to 2020	planning
3. Hire and retain qualified staff who can create and maintain an active web site.	i. Employ staff with demonstrable capacity for creating and maintaining robust University web presence.	i. ICT Centre ii. University Administration iii. Council	2019 to 2020	Planning
4. Implement a procedure to integrate and update data via the web site.	i. Develop federated approach to web content development, via Faculty web rings. ii. Develop Wiki approach to web development.	i. ICT Centre ii. University Administration i. ICT Centre ii. ICT steering Committee iii. University Administration	2019 to 2020 2019 to 2020	Planning Planning

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
5. Develop a system to serve customized pages to a variety of users.	i. Separating the University web content into public (external facing) and intranet (internal facing), focusing on users needs and activities. ii. Developing a single login for students' and staff access to seamlessly navigate through the internet and intranet.	i. ICT Centre ii. ICT steering Committee iii. University Administration i. ICT Centre ii. ICT Committee iii. University Administration	2019 to 2020 2019 to 2020	
6. Encourage academic staff to develop web based learning materials using various ICT.	i. Encourage staff developed e-learning packages for hosting on the University web site.	i. ICT Centre ii. ICT steering Committee	2019 to 2020	

Principle 6: ICT is essential for communication, partnership, and collaboration.

Goal 6.1.: Develop and provide systems and tools to enable units and individuals to collaborate across disciplines and institutions.

ICT Strategies	**Initiatives**	**Responsibility**	**Time Frame**	**Phase**
1. Analysis of current collaboration practices, within and outside the University.	i. Assess the current collaboration practices in the University	i. ICT Centre ii. Faculties ii. University administration	2019 to 2020	Planning
2. Provide the platform for researchers to collaborate with groups external to University.	i. Provide University wide platform to promote collaboration and encourage external collaboration. ii. Establish grid middleware suite (software environment) to support research collaboration and harnessing of distributed ICT facilities and databases.	i. ICT Centre ii. Faculties iii. University administration i. ICT Centre ii. University administration	2019 to 2020 2019 to 2020	Planning
3. Provide desktop audio and video conferencing capabilities and collaborative technology.	i. Establish infrastructural facilities for audio and video conferencing. ii. Increase Internet bandwidth to minimum of 10 gig. for instructional podcasting	i. ICT Centre ii. PPU and works iii. University administration i. ICT Centre ii. PPU and works iii. University administration	2019 to 2020 2019 to 2020	Planning

ICT Strategies	**Initiatives**	**Responsibility**	**Time Frame**	**Phase**
	(internet audio publishing method) and video podcasting (internet video publishing method).			
4. Develop central depository for digital objects for research output.	i. Provide University wide central depository for digital objects.	i. ICT Centre ii. University administration	2019 to 2020	Planning
5. Develop interoperability between institutional, national, and infrastructure to support collaboration and partnership.	i. Provide infrastructural facilities and resources for interoperability between institutional, national, and other ICT centre	i. ICT Centre ii. University administration	2019 to 2020	Planning
6. Ensure seamless interoperability with ICT delivered services by units (ICT centre, Library, Faculties, etc).	i. Provide University wide interoperability platform for University ICT units.	i. ICT Centre ii. University administration	2019 to 2020	Planning

Principle 7: ICT is capital intensive, thus an effective mechanism must be evolved to fund and appraise ICT funded provisions.

Goal 7.1.: Develop measures to access the funding needs of users across the University.

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
1. Evaluate priority of users for central ICT investment.	i. Assess users' needs and cost implication of such needs. ii. Determine the budgetary need based on users' needs.	i. ICT Centre, ii. University Administration	2019 to 2020	Planning
2. Provide a breakdown of ongoing operational expenditure and a descriptive and prioritized list of new ICT investment.	i. Evaluate the operational expenditure on existing and on-going ICT investment.	i. ICT Centre ii. University Administration	2019 to 2020	Planning
3. Plan a five-year development budget plan on ICT expenditure	i. Develop a five-year development budget plan on ICT expenditure for the University.	i. ICT Centre ii. Bursary ii. University Administration	2019 to 2020	Planning
4. Invest in central ICT which provide users with needed ICT environment.	i. Implement the five-year development budget plan on ICT expenditure	i. ICT Centre ii. Bursary ii. University Administration	2019 to 2020	Planning
5. Ensure adequate funding of ICT to ensure high priority ICT services are resilient, robust and reliable.	i. Implement budget plan as specified and ensure adequate funding as may be necessary. ii. Develop and implement	i. ICT Centre, ii. Bursary ii. University Administration	2019 to 2020 2019 to 2020	Planning Planning

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
	supplementary budget as may be required.			
6. Develop voluntary purchasing mechanism for staff and students to make purchases from a set of companies within an overall framework.	i. Facilitate staff and students' ICT hardware acquisition through repayment initiatives.	i. ICT Centre ii. Bursary Iii. University Administration	2019 to 2020	Planning

Goal 7.2.: Ensure mechanism for regular appraisal of expenditure on ICT.

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
Develop mechanism to ensure that the University receives favourable ICT investment conditions from vendors.	i. Implement mechanism to ensure that the University receives favourable ICT	i. ICT Centre ii. Bursary Iii. University Administration	2019 to 2020	Planning
Establishing a process for appraising central expenditure on ICT in teaching, learning, research, and administration.	i. Appraise current central expenditure on ICT for teaching, research, learning, and administration.	i. ICT Centre ii. Bursary Iii. University Administration	2019 to 2020	Planning
Appraising expenditure on ICT at unit levels.	i. Appraise current expenditure on ICT for teaching, research, learning, and administration at units' level.	i. ICT Centre ii. Bursary Iii. University Administration	2019 to 2020	Planning

Goal 7.3.: Consider alternative sources of funding for ICT development, apart from government funding.

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
1. Development of proposals for potential donors for acquisition of hardware and development of ICT projects.	i. Encourage staff development of proposals.	i. Faculties ii. Academic Planning ii. University Administration	2019 to 2020	Planning
2. Introduction of ICT levy on students (undergraduate and graduate) for ICT use and access.	i. Implementation of students' payment of ICT levy	i. Bursary ii. University Administration	2019 to 2020	Planning
3. Introduction of ICT staff levy for ICT training, use, and access.	i. Implementation of staff's payment of ICT levy	i. Bursary ii. University Administration	2019 to 2020	Planning
4. Running of ICT related workshops, short programmes, training, and professional certification on ICT.	i. Design and implement short programmes and training on ICT. ii. Run certified ICT professional programmes (Microsoft, CISCO, Oracle, etc.)	i. ICT Centre i. ICT Centre ii. University Administration	2019 to 2020 2019 to 2020	Planning Planning
5. Providing consultancy ICT services	i. Engage in consultancy services on ICT	i. ICT Centre ii. Department of computer Sciences iii. University Administration	2019 to 2020	Planning
6. Engagement in joint ventures with software	i. Explore joint venture with software	i. ICT Centre ii. Department of computer	2019 to 2020	Planning

ICT Strategies	Initiatives	Responsibility	Time Frame	Phase
development organizations	development organizations.	Sciences iii. University Administration		
7. Husbanding the library fund for the development of e-library.	i. Use part of the Library fund to fund digitization of library activities.	i.ICTCentre ii. Library iii. University Administration	2019 to 2020	planning
8. Dedicating a certain percentage of IGR and ICT based revenue for institutional ICT development.	i. Determine and fund ICT development using IGR	i. Bursary ii. University Administration	2019 to 2020	Planning
9. Source for corporate and governmental agencies (e.g. ETF) funding of major ICT projects.	i. Explore corporate sponsorship of ICT funding	i. ICT Centre ii. Faculties iii. University Administration	2019 to 2020	planning
10. Pursuance of vendor "In Kind" for technology purchases and upgrade across the University.	i. Leverage the use of vendor "In Kind" for technology purchases and upgrade	i. ICT Centre ii. Faculties iii. University Administration	2019 to 2020	Planning

APPENDIX 1 - HARDWARE ACQUISITION AND MAINTENANCE POLICY

1.0 Introduction

This policy sets out the requirements for acquiring hardware by the various departments of the University. Proper computer hardware resources should be available in Faculties, departments, offices and teaching labs to support the University's mission and vision. It is desirable at all times for users to have hardware with sufficient specifications to support their job-related requirements or learning needs. This policy is meant for management and any personnel who are responsible for hardware acquisition.

1.1 Hardware Acquisition

All hardware must be procured in accordance with the following:

- Minimum standard specifications for computer hardware will be regularly determined and updated by the ICT Centre in liaison with the various user departments. This information will be provided on the ICT Centre web site.
- Any department intending to procure hardware must submit their specifications to ICT Centre for approval before their order can be processed by the Procurement Unit.
- Wherever possible, uniform hardware should be procured throughout the University in order to make repairs and parts replacement easier and less expensive.
- Suppliers of hardware must be vetted to ascertain their ability to supply proper equipment and provide subsequent maintenance and repairs on the equipment if such need should arise. Hardware should be sourced only from approved vendors, in accordance with the University's procurement regulations/procurement law.
- Warranty certificates should be issued and signed for all hardware purchased.
- On delivery, all equipment should go through an acceptance test by ICT centre
- The hardware inventory register should be updated whenever new hardware is acquired, the inventory details should also be added to the main University asset register**.**

1.2 Hardware Maintenance

- A hardware maintenance contract should be drawn up with the suppliers of hardware requiring specialist maintenance. This includes, but is not limited to UPS systems, Laptops, printer, servers and photocopiers and all ICT related equipment.
- During the warranty period, no attempt should be made to repair faulty hardware as this renders the warranty invalid. Such hardware should be sent for repairs to the supplier in its original packaging.
- Only authorized university technicians may undertake maintenance or repairs on University hardware.

- Only service providers who are licensed by hardware manufacturers to maintain or service hardware should be contracted to carry out repair or maintenance work on hardware.
- Service Level Agreements should be drawn up with service providers responsible for maintenance of hardware equipment. All service level agreements should be recommended by the Director ICT Centre for management's approval.

1.3 Hardware Replacement and Disposal

When hardware no longer allows a user to carry out the functions for which it was procured, it should be replaced. This may happen when software required for business activities, teaching or service provision cannot run on existing hardware effectively or when there is malfunctioning of hardware which cannot be rectified.

1.3.1 Needs Assessment

A replacement needs assessment should be carried out in departments by relevant ICT staff in liaison with department heads to identify hardware that needs replacement. This information is useful for budgetary purposes.

1.3.2 Cascading Hardware

Hardware which becomes obsolete for high end users is usually useful for lower end users not requiring high specifications.

All users will be dealt with in accordance to their hardware and software needs.

1.3.3 Hardware Disposal

Hardware must be disposed in accordance with the University equipment disposal policy. **(See 1.4)**

1.4 Hardware Life Span

The life span of hardware should be determined. This is useful for auditing purposes and valuation of computer equipment. Scheduled replacement may also be possible after the lifespan has been determined. The following hardware life spans should be recommended:

- Desktop Life Span: 5/6 years
- Laptop Life Span: 3/5 years
- Servers Life Span: 5/6 years

APPENDIX 2 -SOFTWARE ACQUISITION & USAGE POLICY

2.0 Introduction

The purpose of this policy is to define the acceptable acquisition and use of software licenses. The central management of licenses aids the university in taking advantage of bulk software procurement pricing and reduces the possibility of redundant software. It is the responsibility of the university to prevent the installation of unlicensed software on its computers as this may lead to legal action by the developers of such software's.

2.1 Software Licenses Acquisition and Use

The Federal University Wukari uses computer software under license from software companies. The university does not own most of the software or its documentation and does not have the authority to copy it unless authorized.

It is the policy of the Federal University Wukari to adhere to software copyrights and the terms and conditions governing their use. The University does not allow the use of software without the proper licenses.

For cost effectiveness, duplicating software acquisition should as much as possible be avoided.

2.2 Responsibility for Software

- This policy is the main responsibility of the Director ICT Centre who is the custodian of software licenses.
- Management in the various Units should ensure that all software installation done on computers in their departments is in accordance with specifications in the license agreement. Any queries regarding the terms of software licensing should be referred to the Director ICT Centre.

Software	License No.	Version	Expiry Date	License Deployment	User Limit

Sample of software license management form

- An inventory of software in use should be kept, which specifies the details of the software, license, version and how many users are permitted per license. (See table above)

2.3 Software Installations End-users may not make software installations on the University computers. Personnel appointed from ICT Centre will carry out installations unless otherwise clearly instructed. Proper installation procedures must be followed in all instances.

2.4 Acceptable use of University Software

- All software must be used according to the terms of the license agreement for the particular software. All commonly used software licenses must be purchased through the ICT Centre. Software such as antivirus updates may be downloaded from the University website.
- University staff may not make copies of licensed software to use on other University sites or outside the University without proper authorization. Anyone found using software illegally will be personally held liable for any penalties which may arise from such use.
- Software on local networks or multiple machines may be used only in compliance with the license conditions.

Where a need for particular software is identified, whether for teaching, research or administration, a request should be made with the head of department who will send the request to Director ICT Centre or his representative for the acquisition of the software license.

Appendix 3 - Network Management Policy

3.0 Introduction

The FUW communicates both internally and externally through the use of its network infrastructure and network management software. The requirement for the availability of communication channels at all times and the need to protect the integrity of data that travels through the network dictates the need for the proper management of the University's networks.

This policy aims to ensure that the network system is properly designed and managed. The requirements in the policy aim to ensure that:

- The network is designed to a capacity which adequately caters for communication and data transmission requirements of the University.
- Access to the University network is through properly authorized and authenticated methods. Data, which is transmitted through the University network, is secure.
- The University's network is not used to transmit illegal, defamatory or offensive material.
- The university network is not used as a means to illegally gain access to or tamper with other networks outside of the university.

3.1 Definition of terms

Availability: The network is accessible and usable upon demand by an authorized person.

Integrity: Network settings have not been altered in an unauthorized manner.

Local Area Network (LAN): A computer network which covers a small area, for example a building.

Wide Area Network (WAN): A computer network which covers a larger geographical area than a single building.

Virtual Local Area Network (VLAN): A logical computer network segment within a single physical LAN.

Virtual Private Network (VPN) A logical private network tunnel within a public physical network

3.2 Responsibility for policy

This policy is the responsibility of the Director ICT Centre who will ensure that only authorized and qualified personnel are responsible for managing the network and its resources.

3.3 Network Configuration

The network must be designed and configured for optimal and secure performance, with minimum disruption and downtime.

Devices used for network setup and configuration must conform to a set standard and to industry best practices.

All devices that make up the network infrastructure must be logged and regularly maintained to ensure the integrity of the network.

Bandwidth requirements must be constantly reviewed to cater for the business needs of the University community Bandwidth management strategies must be implemented to ensure priority for bandwidth is given to the University's core business

All network configurations and designs must be documented and the documentation must be updated whenever a change to either design or configuration has been made.

All network points must be clearly labeled according to a set standard both in the network cabinet and the point in the offices.

3.4 Network Security

3.4.1Physical Security

- The network infrastructure must be protected from unauthorized access
- Wireless access points must be properly secured to prevent tampering
- The area in and around server rooms or data centers and Network cabinets must provide protection against fire, water damage, and any other environmental hazards
- All physical network points in public places must be secured to prevent unauthorized access to network resources. Primary network points in public places must be always disabled and only enabled when there is a need and the relevant authority has authorized this need.
- Network access by third parties must be through written authority from the Network Manager for performing specific tasks assigned to them for a duration limited to the particular tasks.
-

3.4.2 Logical Security

Procedures must be put in place to implement and maintain the network's logical security.

- The network must be segregated according to logical domains and access control levels must be according to the sensitivity and business nature of the domain.
- Firewalls must be properly configured to protect the domains.
- Identification and authentication methods must be enforced to prevent unauthorized access to network devices.
- All devices accessing the network must be authorized and identifiable.
- Network activity must always be monitored for performance and intrusion detection.
- Penetration tests must be periodically performed on the network to test its resilience.

3.5 Business Continuity

Network management should include the backing up of network devices configurations to be used for recovery in the event of a disaster as specified in the Information Security Policy. **(See Appendix 8).**Any upgrade to the network must be done by qualified personnel and should follow the proper change management procedures as specified in the Change Management Policy. **(See Appendix 7)**

Appendix 4 - ACCEPTABLE USER POLICY

4.0 INTRODUCTION

This policy applies to all users of FUW ICT facilities, be they owned or leased by the university. It is meant to guide users in the general accepted use of ICT services within the University. This policy should be read together with the relevant detailed individual policies outlined in this document.

4.1 Authorized Use of Facilities

The use of ICT services is available to staff, registered students, visiting lecturers, retired academic staff (subject to approval by the Director ICTcentre) and service providers currently working for the University e.g. external auditors (subject to approval by the Director ICT centre), occasional users e.g., use of facilities during workshops and seminars by attendees.

The use of facilities is subject to registration and issuing of a username and password. Only authorized personnel in the faculty or department can carry out registration. Thus, the use of facilities has to be traceable to the user (Audit log file, log file).

4.2 Acceptable Use of Hardware and Software

Users are required to use all hardware and software in a responsible manner that does not cause damage to equipment, software, networks or the rooms housing the equipment, and other users. Because of the resources required to put back systems to their original state, unauthorized modification to hardware or software constitutes damage. Any costs incurred in restoring hardware/software to its original state will be charged to the user responsible for the damage. One's use of the University hardware or software must not interfere with the ability of others to make use of it or its proper functioning.

4.3 Introduction of Viruses onto Systems

Users must not introduce any viruses, malware, Trojans or any software which may compromise any ICT equipment. It is the responsibility of users to report any virus attacks on computers in their use.

4.4 Licensing Requirements

Users must comply with all licensing requirements for hardware, software or any ICT facility they may use. Where a user is unsure, they should seek clarification with personnel managing ICT services in their department or faculty or the ICT Centre. It is an offence to install or use any software without satisfying its license requirements

4.5 User Rights

Users accessing ICT services in Computer Lab or within the university must respect the right of other users when using ICT facilities, conducting themselves in a quiet and respectable manner, respecting the time limit allocated to them, bearing in mind that such facilities are shared. The ICT Director reserves the right to withdraw ICT facilities to any user found in violation of any or all of the above laws.

4.6 Ethical Use

Users must use facilities in a responsible manner in order not to tarnish the university image. It is an offence to download or distribute offensive materials using the University's ICT facilities. Any user found to be using ICT facilities in an unethical manner will be liable to disciplinary measures or prosecution if they are in violation of the Nigerian Laws.

4.7 Profit Use

Use of ICT facilities for personal profit is strongly not permitted. ICT facilities shall be used to satisfy the roles and responsibilities assigned to users in their line of work/duty or study.

4.8 Legal Compliance

All ICT services should be used in compliance with the rules, regulation, laws governing ICT at the FUW and in Nigeria.

APPENDIX 5- Internet and Email use Policy

5.0 Introduction

Federal University Wukari provides electronic mail resources to support its work of teaching, scholarly research, and administrative services. This policy statement sets forth the University's policy with regard to use of, access to, and disclosure of electronic mail to assist in ensuring that the University's resources serve those purposes.

5.1 Privacy, Confidentiality and Public Records Considerations

FUW will make reasonable efforts to maintain the integrity and effective operation of its electronic mail systems, but users are advised that those systems should in no way, be regarded as a secure medium for the communication of sensitive or confidential information. Because of the nature and technology of electronic communication, the University can assure neither the privacy of an individual user's use of the University's electronic mail resources nor the confidentiality of particular messages that may be created, transmitted, received, or stored thereby. The University owns all e-mail accounts created under chosen platform (Google) and has the right to take reasonable steps to ensure that its email facility is not being used for illegal or offensive purposes.

5.2 Permissible Uses of Electronic Mail

5.2.1 Authorized Users

The only authorized users of the University's electronic mail systems and resources are University staff, students and other persons who have received permission under the appropriate University authority (ICT Director).

5.2.2 Purpose of Use

The use of any University resources for electronic mail must be related to University business, including academic pursuits Incidental and occasional personal use of electronic mail may occur when such use does not generate a direct cost for the University. Any such incidental and occasional use of University electronic mail resources for personal purposes is subject to the following provisions:

- Such use must not cause significant additional cost to the University;
- Such use must not interfere with employment or other obligations to the University;
- All relevant University policies must be observed;
- Personal views transmitted or published using the facilities must be clearly identified as personal views and not those of the University.
- Such use must not directly or indirectly interfere with the University's operation of the electronic facilities;
- The purposes are of a purely personal and private nature, and not for financial gain;

5.3 Prohibited Uses of Electronic Mail

FUW resources may not be used to:

- Engage in illegal activities.
- Perpetuate chain e-mail letters or their equivalents. This includes letters that require the recipient to forward an e-mail to a specified number of addresses in order to achieve some monetary, political, superstitious, or other goals.
- Create and/or send "spam." (Spam is defined as any unsolicited electronic communication that is sent to any number of recipients who did not specifically request or express an interest in the material advertised in the communication). It will be considered a greater offense if the University electronic communications resources are exploited to amplify the range of distribution of these communications.
- Send or encourage "letter bombs." Letter bombs are extremely large or numerous e-mail messages that are intended to annoy, interfere, or deny e-mail use by one or more recipients.
- Practice an activity designed to deny the availability of electronic communications resources to others. Also called "denial of service attacks," these activities deny or limit services through mail bombing, malicious executable such as viruses, threatening to transmit a virus, or pretending to have sent a virus to others or opening a large number of mail connections to a mail host without authorization or permission.
- Sending and soliciting to receive pornographic material by electronic means or storing of such material on a university computer. These activities are both illegal and will constitute serious University disciplinary offences.

5.3.1 Other Prohibited Uses

- Other prohibited uses of electronic mail include, but are not limited to
- Use of electronic mail systems for any purpose restricted or prohibited by laws or regulations.
- Sending copies of documents in violation of copyright laws.
- Inclusion of the work of others in electronic mail communications in violation of copyright laws.
- Capture and "opening" of electronic mail except as required in order for authorized employees to diagnose and correct delivery problems or as authorized by law to obtain evidence of illegal activities.
- Use of electronic mail to harass or intimidate others or to interfere with the ability of others to conduct university business.
- "Spoofing," i.e., constructing an electronic mail communication so it appears to be from someone else.

- "Snooping," i.e., obtaining access to the files or electronic mail of others for the purpose of satisfying idle curiosity.
- Attempting unauthorized access to electronic mail or attempting to breach any security measures on any electronic mail system, or attempting to intercept any electronic mail transmissions without proper authorization.

5.4 University Access and Disclosure

5.4.1General Provisions

- To the extent permitted by law, the University reserves the right to access and disclose the contents of faculty, staff, students', and other users' electronic mail without the consent of the user. The University will do so when it believes it has a legitimate reason including, but not limited to, those listed in paragraph 3 (below), and only after explicit authorization is obtained from the appropriate University authority.

- Faculty, staff, and other non-student users are advised that the University's electronic mail systems should be treated like a shared filing system, i.e., with the expectation that communications sent or received on University business or with the use of University resources may be made available for review by any authorized University official for purposes related to University business.

- Electronic mail of students in connection with their university studies may constitute "education records" and the University may access, inspect, and disclose such records.

- Any user of the University's electronic mail resources who makes use of an encryption device to restrict or inhibit access to his or her electronic mail must provide access to such encrypted communications when requested to do so under appropriate University authority.

5.4.2 Monitoring of Communications

The University will not monitor electronic mail as a routine matter but it may do so to the extent permitted by law, as the University deems necessary for purposes of maintaining the integrity and effective operation of the University's electronic mail systems and to detect the carrying out of illegal and impermissible activities through the E-mail system.

5.4.3 Inspection and Disclosure of Communications

The University reserves the right to inspect and disclose the Contents of electronic mail. The executive may authorize tracking of its student or employee e-mail use in a number of circumstances including, but not limited to:

- ❖ Investigations by law enforcement agencies where there are reasonable grounds for believing that there have been violations of the laws of Nigeria.
- ❖ Suspected violations of University Codes of Conduct, regulations or policies;
- ❖ In situations involving possible threats to the health or safety of people or property;
- ❖ In order to fulfill other legal responsibilities or obligations of the University;
- ❖ When necessary to prevent interference with academic activities;
- ❖ As needed to locate substantive information required for University business that is not more readily available by some other means.

5.4.4 Limitations on Disclosure and Use of Information Obtained by Means of Access or Monitoring

The contents of electronic mail communications, properly obtained for University purposes, may be disclosed without permission of the user. The University will attempt to refrain from disclosure of particular communications if disclosure appears likely to create personal embarrassment, unless such disclosure is required to serve a business purpose or satisfy a legal obligation.

5.4.5 Special Procedures

Individuals needing to access the electronic mail communications of others, to use information gained from such access, and/or to disclose information from such access and who do not have the prior consent of the user must obtain approval in advance of such activity from the appropriate University authority. The Registrar will issue a written statement of the procedure to be followed to request such approval. The prescribed procedure will:

- Seek to minimize the time and effort required to submit and respond to requests; and
- Seek to minimize interference with University business; and
- Seek to afford protection of the rights of individuals.

5.5 Disciplinary Action

Appropriate disciplinary action will be taken against individuals found to have engaged in prohibited use of the University's electronic mail resources.

5.6 Public Inspection, Retention, and Archiving

Communications of University employees in the form of electronic mail may constitute "correspondence" and therefore may be a public record subject to public inspection under Nigerian Law.

5.7 Expiration of Accounts

5.7.1 Employees retiring from the University: - Accounts for faculty and staff retiring from the University will be maintained indefinitely.

5.7.2 Employees resigning from the University:-Accounts for faculty and staff leaving on good terms will expire 90 days after the last day of employment.

5.7.3 Employees Dismissed from the University: - Accounts for faculty and staff dismissed from the University will expire immediately. Email will not be forwarded after the account expires.

5.7.4 Students Graduating:-

Accounts for students graduating from the University will expire 60 days after the last day of the semester during which they wrote their final year examinations.

5.7.5 Expelled Students:-

Accounts of expelled students expire immediately upon their expulsion.

5.8 Use of Mailing Lists

5.8.1 Use of University Maintained Mailing Lists

The use of University Maintained Mailing lists should be restricted to Official University business. These lists will be for the distribution of official communications, unless approved by the ICT Director. Some official lists may require mandatory participation by all faculty and/or staff employees.

5.8.2 Use of Personal Mailing Lists

Faculty and Staff may create and maintain their own personal mailing lists. The individual creating and maintaining the list and any users using the list must ensure that members of the list agree to participate in the list. When an individual requests that their name be removed from a mailing list, the list maintainer must remove any such individual from the list. As these lists originate from FUW and carry its name, correspondence on these personal lists must still comply with the acceptable user policy of the University.

Appendix 6 - Password Policy

6.0 Introduction

This policy governs the use of usernames and passwords by users of ICT facilities at the Federal University Wukari.

6.1 Responsibility for Policy

The Director ICT Centre is responsible for this policy.

All ICT users at FUW must familiarize themselves and comply with the requirements for this policy.

Students and staff are required to apply for permission to access relevant ICT facilities from the management of such facilities in departments or faculties. When approval is granted, the user is allocated a user name, usually a combination of initials and surname in the case of staff and Registration number in the case of students. The user will be provided with username and default password which must be changed (Password) at first log-in.

Workstations should not be left unattended to or with unrestricted access as this may result in others accessing a user's account and viewing private information or sending messages from the same account. A password screensaver should be used to minimize unauthorized access.

6.2 Rules governing Username/Password Use

- Users may only use their own username and are not permitted to use other peoples' usernames.
- Passwords associated with any username must be kept private. If a user suspects that their password may be known by other users, they should immediately change it. If any unauthorized acts are done using one's username, they will be held responsible unless they prove that they were not responsible for the act.
- No account shall be shared; each user accessing a system should have their own account created for them.
- In the event that a user is assigned responsibilities which enable them to access high level usernames and passwords, it is an offence to pass that information on to others unless written permission is given by management. Adequate preparation should be made to ensure that passwords are store in encrypted form to protected those with access from deciphering them. In situations where periodic password changes are required, users should comply with instructions to change passwords at the appropriate times. Failure to adhere to requirements will result in user lockout.

6.3 User name Expiry/Account Deletion

- Staff: When staff employment with the University ceases or are transferred to another unit, access to systems must be suspended and their account is deleted from all systems they had access to. However, in the event that an employee leaves the employment of the university not through dismissal they may still access their E-Mail account for a period not exceeding 60 days.(See Appendix 2 – E-Mail Use Policy)
- Students: When a student graduates, they may have access to their E-Mail account for a period not exceeding 90 days. A student who is suspended from the University will have their E-Mail account deleted immediately upon suspension and any other facilities they had access to.
- Visiting Staff: A visiting staff's account is only valid for the duration of their visit. The account should be deleted at the end of the visit. Automatic dates of expiry should be set on such accounts.

Appendix 7- Change Management Policy

7.0 Introduction

The University's reliance on ICT systems and services to perform its roles and functions is on an upward trend. Such changes to critical systems and infrastructure, if not implemented in an organized manner may pose risks to the University.

This policy aims to achieve the following:

- To establish the process of controlling modification to hardware, software and documentation to ensure the protection of ICT services against unapproved and undocumented modifications.
- To communicate with relevant personnel changes that may negatively affect provision of ICT services.
- To ensure the use of a standard framework of procedures (SOPs) in handling changes to ICT systems at the FUW.

This policy applies to all individuals who install, operate or maintain ICT resources. Heads of department, Units and other functional services who use the university ICT systems must also familiarize with the requirements of this policy.

It is important that change is properly managed to avoid inconveniences to system users as it may affect the stability and security of systems. It is critical that all change are planned, tested, approved and publicized. A detailed change management procedure manual must be kept for all ICT systems.

7.1 Responsibility for policy

- This policy is the responsibility of the Director ICT Centre.
- Staff responsible for system changes must familiarize with the requirements of this policy.
- Stakeholders in the various functional process units must also familiarize with requirements of this policy.

7.2 Types of Change

Change refers to any additions, deletions or modifications to an Information Technology resource that is operating in a live environment. This resource may be any of the following:

- The infrastructure, which includes the network, hardware, operating system, data and voice networks
- The databases and data

- Environmental facilities including but not limited to air conditioning units and power/electricity supplies.

Change is classified in terms of the following:
Minor: Minimal modifications to a live system which has very limited impact on business and its potential disruption to services should be minimal.

Major/Significant: Significant changes to a live system with the potential to have a major impact on business and disruption to services.

Emergency/Unscheduled: Such change may involve repairs to sudden breakages or a system malfunction, which are impacting negatively on service delivery. Such change does not have forward planning but nevertheless should be documented.

7.3 The Change Management Framework

The management of change to ICT systems shall be done according to the ICT Infrastructure Library framework.

- Faculty, Department, Unit and directorate or system owner **(ICT)** will make a formal request for change onto the Help Desk or the relevant ICT Unit. If request is made through the ICT Centre, it is the responsibility of ICT to log the request.
- A Change Advisory Board **(CAB**), which consists of the ICT staff responsible for implementing the change and representatives of the business owners (stakeholder), in cases where the change is not an emergency will sit to discuss the requested changes, assign levels of criticality and approve or deny the change request.
- Emergency change requests shall be approved by the ICT Director
- A change manager will chair the **CAB** and will be responsible for ensuring that all changes are documented and a log is kept for any change that is undertaken. All change, whether planned or emergency, successful or not shall be documented. Change reviews shall be regularly performed and completed changes closed
- A business continuity plan should be in place to mitigate in case of unsuccessful change implementation.

- Prior to a change, a copy of the system/database/data shall be made and archived before the change is effected. These archives shall be logged and filed by the Change Manager.

Details of the change management procedures are found in the Change Management Procedure Manual

APPENDIX 8 - Information Security Policy

8.0 Introduction

The FUW possesses information that is both sensitive and valuable; this includes but is not limited to student records, financial data and research information. If such information is exposed to unauthorized individuals, this could cause harm to the university. If information is tampered with or is made unavailable, the university's ability to do business effectively will be compromised. Incidents, which involve loss of data integrity, availability or confidentiality, can be costly to the University. In determining its Information Security Policy, the University has adopted principles, policies and practices which maximize protection against risks so that the security of its information and systems is assured.

This policy aims to ensure that all information and information systems are adequately protected. To achieve this, it is of importance that all staff and students abide by the requirements stated in the policy guidelines. The requirements in the policy aim to ensure that:

Information deemed to be confidential is protected from unauthorized access.

All Information, which the University avails to staff and students, or any relevant third parties is complete and accurate at all times.

The university's ICT infrastructure, hardware and network systems are protected from risk through application of information security industry best practices.

University information is correctly categorized to ensure access is on a need to know basis

8.1 Definition of terms

Availability: Data or information is accessible and usable upon demand by an authorized person.

Confidentiality: Data or information is not made available or disclosed to unauthorized persons or processes.

Integrity: Data or information has not been altered or destroyed in an unauthorized manner.

Risk: The probability of a loss of confidentiality, integrity, or availability of information resources.

Information Owner: The manager responsible for the creation of information or the primary user of that information.

Custodian: The custodian of information is responsible for the processing and storage of the information. The custodian is responsible for the administration of system controls as specified by the information owner.

Management: Staff who perform managerial or supervisory functions and are responsible for overseeing employees' use of information including reviewing and approving employees access authorizations.

8.2 Responsibility for policy

This policy is the responsibility of the Director, ICT Centre FUW.

8.2.1 General Staff Responsibilities

An individual may only access information, which they require to perform University duties allocated to them according to their roles and responsibilities

Information obtained during the course of one's duties may not be divulged, copied, altered, sold or destroyed except when authority has been granted

Every staff member should be aware of the level of sensitivity of the information they have access to and should manage such information according to its security requirements

An individual must ensure that a computer allocated to them to conduct University business is adequately protected

The confidentiality, integrity and availability of information, be it on physical documents, computer storage media or in Email communications must be protected

Confidential information must be destroyed before it is discarded.

Confidential information must not be divulged even after a member of staff leaves University employment

8.2.2 Management Responsibilities

In addition to the general staff responsibilities, it is management's responsibility to ensure that

Procedures are put in place in departments to support the university's need for confidentiality, integrity and availability of information.

Each staff member understands their security related responsibilities

Restrictions to information are communicated to all staff who use, capture, store process or transfer information in any form, physical or electronic

Management is responsible for authorization of access to University systems by their staff and communicating with the relevant ICT unit in the case that staff is no longer allowed access to information.
Management is also responsible for development of the university information security manual (rules and regulations) and the training of staff on these procedures.
Management is also expected to create an information security unit that will oversee the information security issues in the university.

8.2.3 ICT/information security Personnel Responsibilities

In addition to the general staff and management responsibilities, ICT staff being the custodians who manage Information systems and network infrastructure that is used to capture, store, and process transmit information must ensure that the university requirements for integrity, availability and confidentiality of information are implemented in all ICT environments. They must also ensure that:

- They understand the levels of sensitivity of information to be captured and stored by the university
- All systems implemented satisfy the required level of security based on the sensitivity of information they handle
- All technology in use at the university operates in a secure environment
- Effective standards and strategies are developed to protect information against threats
- Staff are educated on threats to information(creation of bulletin board, information security training)

8.2.4Information Owners Responsibilities

In addition to complying with the general staff and management responsibilities information owners must ensure that:

- Information they are responsible for is classified according to the level of sensitivity and confidentiality. **(See appendix7.1 - procedures manual for classifying information)**
- The requirements for availability of the different classes of information are specified
- Staff's authorizations to access information through their roles or job functions are specified according to their roles and responsibilities.

8.3 Securing Information

8.3.1 Physical Security

Access to areas in which information processing is carried out must be restricted to only appropriately authorized individuals.

File servers hosting confidential and/or Internal Information must be installed in a secure area to prevent theft, destruction, or access by unauthorized individuals. Documented procedures to control and validate a person's access to server rooms or data centers based on their roles or function, including visitor control, must be developed.
The area in and around server rooms or data centers must provide protection against fire, water damage and any other environmental hazards.

8.3.2 Data Security/Information Handling

Procedures must be put in place to ensure data integrity is maintained at all times

- Electronic transmission of data must be done using secure means, with properly documented procedures
- Confidential paper documents must be disposed of by shredding
- Security mechanisms must be put in place to protect data from viewing by unauthorized individuals
- Electronic data must be securely deleted when removable media or computers containing hard drives are being destroyed

8.3.3 Network Security

The university network must be protected from both external and internal risk. Technical security mechanisms must be put in place to guard against unauthorized access to data that is transmitted over a communications network, including wireless networks. **(The details on network security are found in Appendix 3 – Network & Infrastructure Policy).**

8.3.4 Computers Security

Access to the use of university computers must be restricted only to authorized individuals. Access to servers must also be restricted only to authorized ICT personnel. Each department must have written down procedures for access authorizations for computers they use. The following guidelines must be followed:
With the exception of computers used in public places like the library and computer labs, wherever more than one individual uses a computer, accounts must be created for each individual user who should provide a password for their account. Sharing of accounts is strongly discouraged.

Procedures must be put in place to make user accounts activities traceable.
Use of strong passwords must always be enforced on user accounts (Refer to Appendix 6- Password Policy for details on password use)

8.4 Business Continuity

Hardware or network failure may occur during normal business operations of the university. It is important that minimum loss is experienced as a result of such failure. As such, controls must ensure that the university can recover from any damage to computer equipment or files within a period of time in which university operations are not negatively impacted. Each department is required to develop and maintain a plan for responding to a system emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages systems that manage student information, confidential, or any Internal Information. This will include developing policies and procedures to address the following:

8.4.1 Data Backup Plan

- A data backup plan must be documented and routinely updated to create and maintain, for a specific period of time, retrievable exact copies of information.
- Backup data must be stored in an off-site location and protected from physical damage.
- Backup data must be afforded the same level of protection as the original data.
- Periodic restore of data must be performed to ensure the availability of data in an emergency

8.4.2 *Disaster Recovery Plan:*

A plan must be developed, documented and tested which will be used to restore operations in the event of data loss due to a disaster or any other cause. Such a plan must document the following:

- Classification of data in terms of its criticality and recovery priorities
- The various roles and responsibilities of personnel involved in disaster recovery and the contact persons in the event of a disaster
- All resources required for a successful disaster recovery
- Refer to Appendix 7B- Disaster Recovery Guidelines for details

8.4.3 *Change Management*

Proper procedures must be followed when changes are implemented on live information systems. If not implemented properly, data loss may occur or previously operating systems may fail to function after updates or upgrades have been performed on systems. All personnel involved in managing systems must familiarize and comply with requirements for change management.

Appendix 9 - Use of Social Networking Sites Policy

9.0 Introduction

The use of social networking has become very useful for collaboration, both for personal and business use. This policy sets out the requirements for using social networking sites on University facilities. Social networking sites include, but are not limited to Facebook, Skype, Twitter, LinkedIn and G-talk. This policy must be read in conjunction with Appendix 5 – Internet and Email policy.

All staff and students must comply with the requirements of this policy.

9.1 Personal use of Social Networking Sites

Where an individual uses social networking sites in a personal capacity, they must desist from the following:

- Disclosing confidential information relating to one's employment at the University. Such action will result in disciplinary action being taken against the individual;
- Use of abusive language when communicating. University facilities must not be used to abuse other members of staff, students or members of the community near or far away. Any use of social networking sites to abuse others makes one liable to prosecution according to the laws of Nigeria;
- Tarnishing the image of the University is never tolerated. Any communication which tarnishes the image of the University must be avoided, as this may lead to disciplinary action against the individual;
- Expressing one's personal views as those of the University. The University has formal means of communication and only authorized individuals may post information on its behalf;
- Using University time to do personal business on social networks;
- Sharing personal views about or on a particular Religion – both positive and negative, as the University was not meant for propagating one religion over another.

9.2 Use of Networking sites for University business

Departments may set up networking sites for collaboration amongst staff members, the University community and various stakeholders. The following must be adhered to:

- Networking sites must conform to standards set by the University through Director ICT Centre.
- The head of department is responsible and accountable for its networking site
- The Head of department must always ascertain the accuracy and credibility of information before it is posted on sites
- Information posted on networking sites must portray the University in a positive manner.
- Official networking sites may not be used to post information of a personal nature.

- ❖ The privacy and feelings of others must always be respected when posting information on networking sites
- ❖ Social networking sites must not be used to distribute illegal or defamatory content, any such use may lead to disciplinary measures in accordance with University regulations

Appendix 10 - E-learning Policy

10.0 Introduction

This policy governs the use of E-learning facilities by the user of ICT resources at the Federal University Wukari they are:

I. The Director, Information & Communication Technology, Centre is responsible for this policy.
II. All ICT users at the FUW must familiarize themselves and comply with the requirements for this policy
III. The central system for E-learning is found at www.fuwukari.edu.ngLecturers are responsible for creating and maintaining the course site for the courses they are currently teaching. Students are responsible for enrolling in the courses that are offered on the E-learning platform. Only registered students can enroll in E-learning courses.

10.1 Rules governing E-learning use

- ❖ Only courses that are on the FUW course list or courses that have been approved by the university senate can be loaded on the platform.
- ❖ All courses have to be associated with a department in the university
- ❖ Instructors are responsible for creating course site and uploading course materials
- ❖ Instructors are responsible for the course settings.
- ❖ Instructors should upload content that is copyrighted
- ❖ Though the system maintains a backup, ultimately instructors are responsible for the backing up of the material they have uploaded
- ❖ At the end of the academic semester instructors are responsible for archiving their courses
- ❖ Students are responsible for enrolling into the courses that they are currently taking
- ❖ Students are responsible for backing-up any material they would have uploaded on the platform

Appendix 11- Service Provider Policy

11.0 Introduction

The University depends on external providers to supply hardware, software and maintenance services for its ICT investments. Service providers include but are not limited to supply of the following:

- Internet service provision
- Hardware Supply, Servicing and repairs
- Application Software supply and Maintenance
- Infrastructure setup and maintenance
- Telecommunication services
- Information Systems Auditing

This policy sets out the requirements for appointment of ICT service providers and the quality of service the University must receive from the appointed providers and the supervision of service providers who service sensitive applications.

11.1 Appointment of Service Providers

I. Service providers must be appointed according to the procurement regulations of the University and Nigerian procurement Law.
II. A service provider may only be appointed if they have proven competence and the capacity to perform the service they wish to be appointed to do
III. Where equipment repair services are required, the premises of the provider must be inspected to ensure they have adequate resources to repair the equipment

11.2 Service Guarantee

- All goods and services received on Warranty must be issued with a warranty certificate from the supplier which must be honored by the service provider, if there is need, and the warranty conditions are met
- A valid contract must be signed for all services which are provided for extended periods. It is the responsibility of the appointed ICT personnel to ensure the service provider services do not disadvantage the University
- Service Level Agreements must be signed between the University and Service provider to determine the quality of service the University must expect to get and any penalties which may be incurred for non-compliance.
- All work done by service providers must be tested for quality before it is approved for payment so that the University gets value for money

- ❖ A provision must be made for termination of contract if any contract terms are not met or the level of service does not meet the set standard

11.3 Systems Security

I Access to University systems by service providers must only be on a "need to know " basis

II Any access to the University network or systems must be approved by the Director ICT Centre or his appointee

III Access to systems must only be for the duration of the service, which must be disabled as soon as the task is completed

IV All system access accounts given to service providers must be reset as soon as they complete work on the systems in order to protect the system from unauthorized access

V The service provider must provide guarantee for security of University data, which they may take off-site to work on.

VI The service provider must be liable for any loss or damage which may occur when they work on University systems

VII Service providers must not disclose any information they handle while they work on the University systems. A Non-disclosure agreement where the service provider must sign necessary before they commence work on University systems.

Appendix 12 - Bring Your Own Device (BYOD) Policy

12.0 Introduction

Advances in ICT have resulted in a shift from the traditional approach where access to ICT resources could only be through equipment owned by the Federal University Wukari. The BYOD policy seeks to address security concerns brought about by the use of personal devices like smart phones, tablet computers, laptops for work purposes. Personal devices are ICT devices owned either by staff of the University or by service providers who do business with the University. Personal devices may be used to do University business, which includes but is not limited to the sending and receiving of official communication, accessing the University network and distribution of corporate information through the network.

This policy aims to ensure that all University resources accessed through personal devices are adequately protected. Security risks which arise through the use of personal devices include the following:

- Access of University data by unauthorized persons who may not be employees of the University. This leads to loss of data confidentiality when a device is used by persons other than the employee of the University.
- Compromise of network security through attacks from malware or hacking through connection of external devices to the University network
- Breach of Intellectual property rights for University information that is created, stored or communicated on personal devices
- Personal devices connected onto the network being used for piracy

This policy must be read together with Appendix 7 – Information Security policy.

12.1 Responsibility for policy

This policy is relevant to all members of staff or students who wish to use their own personal devices during the course of their duties or studies. Third parties who include, but are not limited to service providers and visitors to the FUW who wish to connect to the University resources using their own devices must abide by the requirements of this policy. The Director ICT Centre reserves the right to limit the use of personal devices on the University network.

12.1.1 ***General Responsibilities***

- An individual must seek approval to connect their device on the University network. When such access is granted it is the responsibility of the owner to have their device registered on the network
- It is the responsibility of a device owner to make sure that their device has up to date antivirus software installed on their device. Failure to comply may mean the device is disconnected from the network
- Personal devices connected on the University network may not be used for sending offensive communication as such communication may be deemed to be coming from the University. Owners of personal devices should also read Social networking and Internet and Email Policies together with this policy
- Only personal devices belonging to University staff and students may be connected on the University network. Visitors to the University and service providers must apply to the Director ICT Centre through the department they are attached to

12.1.2 ***Using personal devices for University business***

- When a personal device is used for University business, it is the device owner's responsibility to ensure that any official Information residing on the device is protected and kept separate from personal information residing on the same device.
- University information residing on personal devices remains the property of the University and such information may not be shared with third parties, copied, altered, sold or destroyed except when authority has been granted
- Every staff member should be aware of the level of sensitivity of the information they store on their device and should manage such information according to its security requirements
- Confidential information on personal devices must be permanently destroyed before the device is discarded
- Confidential information must not be divulged even after a member of staff leaves University employment
- In the event that a device containing sensitive University information is lost the device owner must communicate to the relevant authority
- When an employee leaves the University, the device is deregistered from the network. Any University information stored on the device should be permanently deleted.