UNIVERSITY OF ILORIN

ICT POLICY

(2023-2028)

In alignment with her commitment in fostering a connected and technologically-enabled 21st-century institution, the University of Ilorin presents this Information and Communication Technology (ICT) Policy. This policy serves as a foundational framework to guide the sustainable, secure, and integrated use of Digital Infrastructures, and ICT services throughout the University community focused on technology enabled teaching, research and community services.

https://www.unilorin.edu.ng/
PMB. 1515, Ilorin, Nigeria
dcomsit@unilorin.edu.ng

Table of Contents

SCOPE

This policy is applicable to the University Community with regards to the design, integration, deployment, usage, management, monitoring and security of digital infrastructures and ICT services.

POLICY FRAMEWORK

The University of Ilorin ICT policy contains setailed guidelines and principles governing various aspects of ICT within the university, including but not limited to:

- ✧ Acceptable Use: Expectations regarding responsible and ethical use of university ICT resources.
- ✧ Data Management: Policies related to data classification, storage, backup, and retention.
- ✧ Security Measures: Information on cybersecurity, access controls, and incident reporting.
- ✧ Network and Infrastructure: Guidelines for network usage, hardware, and software standards.
- ✧ Privacy and Compliance: Information on data privacy regulations and compliance requirements.
- ✧ User Responsibilities: The roles and responsibilities of faculty, staff, students, and administrators.
- ✧ Training and Awareness: Promoting ICT literacy and awareness through training and education.
- ✧ Incident Response: Procedures for handling security incidents, data breaches, and violations.
- ✧ External Collaboration: Policies for engaging with external collaborators and sharing resources.

1.0 UNIVERSITY OF ILORIN IN BRIEF

1.1 Introduction

The University of Ilorin is one of the second generation universities established by the Federal Government of Nigeria in 1975. From the pioneer undergraduate programmes offered in three faculties (Art, Education and Science), the University now runs over 125 undergraduate programmes in 16 Faculties: Agriculture, Arts, Basic Clinical Sciences, Basic Medical Sciences, Clinical Sciences, Education, Engineering and Technology, Environmental Sciences, Communication and Information Sciences, Law, Life Sciences, Management Sciences, Pharmaceutical Sciences, Physical Sciences, Social Sciences and Veterinary Medicine. Furthermore, the University currently runs over 440 graduate programmes under the postgraduate school across various disciplines.

From an initial intake of 200 undergraduate foundation students in 1976, the student population as at the 2022/2023 session stood at over 46,000 undergraduate and over 6,000 postgraduate students. From the staff strength of about 200 in 1975, the population of staff as at September, 2023 is 3,536.

With this growth, coupled with the evolving ICT landscape, this policy would drive the expected sustainable, scalable and integrated ICT ecosystem.

1.2 University of Ilorin ICT Environment

1.2.1Evolution

The University of Ilorin's journey in embracing ICT began in the mid-1980s when the university acquired its first microcomputers primarily for administrative use. During this period, the University Computer Centre was established to provide training for low-level computer technicians for the delivery of computing and data processing services.

1.2.2Growth and Milestones

In the 1990s, there was exponential growth in ICT development, marked by key milestones such as the formation of the Management Information System (MIS) Unit and the Nigerian Universities Network (NUNet) Office in 1992.

Recognising the increasing demands for ICT services, the Directorate of Computer Services and Information Technology (COMSIT) was founded in 2001, becoming the University's comprehensive ICT unit.

Founded on the principle of progressive learning, the University of Ilorin has continually embraced the rapid advancement of ICT. This showcases the University's commitment to fostering a connected and technologically-enabled institution.

1.2.3Infrastructure and Connectivity

The University's network is structured into three critical layers: Core, Distribution, and Access. At its core is the Network Operations Centre (NOC), ensuring uninterrupted network services. In 2003, the Education Trust Fund sponsored the University's landmark VSAT project, which evolved and culminated in the establishment of the Network Operations Centre (NOC) in 2011. This significantly enhanced the University's internet connectivity. Today, the University is confident of a state-of-the-art fiber optic backbone segmented into thirteen distribution rings, providing seamless connectivity to approximately 65 percent of the campus as at September 2023.

1.2.4Bandwidth

The University is currently on 2 Gbps bandwidth subscription from two Internet Service Providers (ISPs) with equitable distribution across the network to facilitate seamless internet connectivity. This caters for the University community for the advancement of teaching, learning and research in tandem with 21st century digital infrastructure and services requirement. Users have their login credentials to log on to the University hotspot which cannot be used simultaneously on more than one device.

1.2.5Services

The University NOC provides Intranet and internet services which include and not limited to: VoIP, surveillance, video conferencing, live streaming and cloud storage, running 24 hours. The ICT support landscape leverage a proactive approach to technology management, diligently focusing on user needs, and consistently evolving with the disruptive tendencies of the current advancements in the ICT ecosystem. This plays a vital role in enhancing the overall educational and administrative experience within the University.

2.0 ICT POLICY OBJECTIVES

The objectives of the ICT policy are to:

1. Provide a framework for digital infrastructure-provisioning, deployment, management/maintenance and recycling;
2. provide a template for measuring the adequacy, reliability and sustainability of digital infrastructure and services;
3. provide a framework for automation of all University's core processes to enhance effective teaching, research and community development;
4. set consistent benchmarks and standards for ICT training for both staff and students;
5. develop framework for ICT support to foster innovative research and development;
6. provide a framework for Cybersecurity measures to safeguard the University's digital infrastructures and assets;
7. Provide a framework for the implementation of the campus wide security intelligence gathering;
8. Develop a consortium model for digital infrastructure and e-resources sharing with external collaborators;
9. provide guidelines for the acquisition and renewal of relevant software and other ICT resources licenses;
10. establish clear regulations for the ethical use of ICT facilities, focusing on preventing misuse and safeguarding resources;

11. ensure protection of intellectual property rights for ICT projects developed by members of the University Community; and
12. provide awareness and ensure enforcement of regulations provided for in the University's ICT policy.

3.0 POLICY STATEMENT

3.1 Digital infrastructure and ICT services provisioning, deployment, management/maintenance and recycling policy

In achieving sustainable integration of digital infrastructure and ICT services into the University system, the following guidelines should be strictly adhered to:

a) Effective planning driven by users' needs assessment should be a precondition in making provision for digital infrastructure and ICT services;
b) COMSIT Directorate shall be consulted for recommendation when digital infrastructure and ICT services are to be procured by the University for conformity with requirements regarding various ICT standards and quality;
c) Acquisition of digital infrastructure and ICT services shall be in consonance with a procurement procedure manual prepared by the Directorate of procurement;
d) For the deployment of software, University Administration through COMSIT, shall provide a detailed specification, verification, validation, implementation and maintenance through an architectural document;
e) University ICT Project Management Committee shall be constituted by the University management to be chaired by the Director of COMSIT (DCOMSIT), with relevant heads of units in COMSIT and other ICT related Departments, for planning, deployment, monitoring and evaluation of all ICT projects;
f) ICT based consultancy shall be sourced in-house where available through University Consultancy unit to aid efficient ICT service delivery;
g) Vendors shall provide evidence of registration with Original Equipment Manufacturers (OEM) with necessary financial, technical and legal requirements;
h) Comprehensive warranty agreement shall be required from vendors to safeguard the University's interests against defect or damages;

i) The University shall also acquire Digital Infrastructure and ICT services through in-house design and production, leasing and donations from individuals, private firms, Government agencies and Non-Governmental Organisations (NGOs);

j) The University shall drive expected synergy between COMSIT and central store with regards to automation of digital infrastructure inventory;

k) Prior to deployment, all digital infrastructure and ICT services shall be uniquely identified by COMSIT; Suggested fields shall include:

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

l) The University through COMSIT shall maintain an inventory system for the movement of ICT equipment, in ensuring standardised process to effectively track, manage, and optimise the allocation, utilisation and maintenance of all digital infrastructure in accordance with established standards and best practices;

m) Digital infrastructure maintenance and repair unit of COMSIT shall be reactivated and empowered to provide required in-house proactive support, maintenance, repair and upkeep of all digital infrastructure and ICT services;

n) The University ICT policy shall support a balanced approach that encompasses robust local hosting, leveraging on cloud solutions for scalability, flexibility and data protection;

o) For contracted maintenance of digital infrastructure and ICT services, there shall be a clear and precise Service Level Agreement (SLA) between the University and the Contractor with clear and measurable performance metrics;
p) All unserviceable digital infrastructure within the University shall be recommended by COMSIT to be reduced, reused and recycled in promoting Green Computing;
q) Digital infrastructure shall be considered obsolete on the recommendations of COMSIT, and be decommissioned and disposed in accordance with established University boarding regulation;
r) The adequacy, reliability and sustainability of deployed digital infrastructure and ICT services shall be measured based on standard metrics as defined by COMSIT before signing off;
s) All University buildings housing network infrastructure shall have an appropriate earthing system;
t) There shall be provision and bi-annual review of alternative power backup solutions for all digital infrastructure control units;
u) Dedicated security proof network equipment control rooms across the University shall be equipped with effective cooling/ventilation system and accessible to Zonal Officers to provide required services;
v) The University shall periodically review the policy on payment for network access, ensuring it aligns with its commitment to open and equitable digital access;
w) The University shall define the bandwidth requirement on the recommendation of COMSIT based on Staff and Student population considering the core digital infrastructure and ICT services;
x) The Physical Planning Unit shall integrate the network structural design at the initial stages of new buildings;
y) Regular consultation and joint meetings with the Director of COMSIT should be scheduled to ensure ICT requirements are adequately addressed before erecting a new structure in the University;
z) All newly erected buildings within the University shall incorporate a structured cabling system in compliance with global best practices to facilitate seamless connection into the university network;

aa) Before building renovations, Works and Physical Planning Units shall consult with COMSIT to safeguard existing network infrastructures;

bb) Prior to constructing any building, road, or car park, the Director of COMSIT shall be duly consulted to identify and map out the path of fibre optic backbones to avoid the destruction of existing fiber layout;

cc) All ICT network service providers shall seek authorisation in line with the University's security and operational guidelines;

dd) Service providers shall strictly adhere to specified access conditions within their operational areas;

3.2 Automation policy

In line with global best practices, automation of all university's core processes shall strictly adhere to the following:

a) The University shall automate all her core processes to achieve the desired digital transformation and effective decision making through big data analytic and Artificial Intelligence;

b) The relevant units of the University whose processes are to be automated shall be involved in requirement gathering and validation;

c) All automations within the University shall strictly adhere to the policy statement as contained in section 3.1 (d) above;

d) Considering the dynamism and evolving nature of digital solutions, all automations within the University shall be constantly reviewed to keep abreast with current trend; and

e) All automated systems shall be signed-off by the respective units.

3.3 ICT Training Policy

This Training Policy reflects our commitment to providing comprehensive, equitable, and accessible ICT training opportunities to all members of the university community. Thus, the following guidelines are provided:

a) The University shall continually engage in training and retraining (local and International) of staff across all cadres in line with the evolving technological innovations;

b) All digital infrastructure projects shall have a training component with Hands-on-training on the supplied equipment and software;

c) Students across all ICT related disciplines shall be trained to support digital infrastructure deployment and ICT services within the University through student intern-ship and work study;

d) Clients seeking specialised ICT training from the University shall direct such requests to the University management through Consultancy unit to be designed and delivered by COMSIT;

e) Partners shall be given opportunities to sponsor in-house training of University staff and ICT training for University community development programmes through the provision of financial support, infrastructure support and the participation of certified ICT professionals approved by the University management;

f) The University shall continually encourage ICT related professional certifications of interested Staff on recommendation of COMSIT;

g) User training manuals shall be developed for all ICT hardware and software deployed within the University and circulated to all relevant units for seamless usage experience;

h) A training programme shall be organised for all new staff on the University's digital infrastructure, ICT services and policy;

i) All new students during their orientation shall participate in a training programme on the University digital infrastructure, ICT services and policy;

j) Periodic training shall be organised for students on University digital infrastructure, ICT services and policy as the need arises;

k) There shall be continuous training and retraining of all role players (Deans, Sub-Deans, HODs, Faculty IT Officers, Faculty Officers, Level Advisers, Course Lecturers), in the delivery of ICT support services; and

l) Regular training sessions and workshops shall be conducted to educate users about best practices, security protocols, and basic troubleshooting steps.

3.4 ICT Support Policy

To achieve efficient ICT service delivery towards innovative teaching, research and Community development, the following shall be strictly adhered to:

a) Robust automated Helpdesk management system shall be developed towards real time escalation and resolution of users oriented enquires and issues;

b) Towards achieving a decentralised ICT support services, Faculty/Unit IT officers shall be empowered with required privileges to resolve some routine update requests on the portal with due approval of the Deputy Vice-Chancellor (Academic);

c) Towards achieving regular updates on the University Website, Faculty/Unit Web-ring officers shall be empowered with necessary privileges to update staff personnel records;

d) The University Network shall be segmented into strategic zones, based on factors like user density, data traffic, and infrastructure complexity with each zone overseen by a designated staff (Zone Officer);

e) Zone officer shall be responsible for daily monitoring, routine maintenance, and immediate troubleshooting within their designated zone;

f) Zone Officers shall be equipped with both physical and digital toolkits;

g) The University, through COMSIT, shall provide proactive solutions for real time digital infrastructure monitoring;

h) Knowledge based expert systems shall be integrated into the planned automated helpdesk management solution leveraging on ethical Artificial Intelligence;

3.5 Cybersecurity Policy

The University is strategic in her mission to protect sensitive information, uphold privacy, fortify her digital infrastructure and ICT services. The University aims at mitigating risks, educating the community, and ensuring the resilience to cyber threats through proactive measures and vigilance. The following shall be adhered to:

a) The Director of COMSIT shall be the custodian of all super privileges with regard to the University's Digital infrastructure and ICT services;

b) The outgoing Director shall as part of handing over procedures, securely transfer ***ALL CLASSIFIED*** information and privileges to the incoming Director;

c) The Data Centre shall have a state-of-the-art access control for strict accessibility to designated personnels with activity logs maintained for all entries;

d) The University shall adopt a comprehensive authentication procedure that securely restrict access to unauthorised and non-academic resources on the network;

e) All outdoor access points shall be fortified against theft;

f) All official communications shall be carried out using the University's email addresses;

g) There shall be stringent data privacy measures to safeguard user information and digital assets, in accordance with relevant data protection regulations;

h) Sharing of portal/web credentials shall be strictly prohibited, with users held accountable for any security breaches originating from their accounts;

i) The University shall develop a plan for data-backup, disaster recovery and business continuity to ensure data Confidentiality, Integrity and Availability in case of unexpected events;

j) A dedicated Cybersecurity Unit in COMSIT shall be created to provide a roadmap for the security threat and attacks mitigation;

k) The University shall categorise all her digital infrastructure to determine level of accessibility and confidentiality;

l) Contractors and digital service providers shall comply with the University's Cybersecurity protocols.

m) Regular security audits and checks shall be conducted to ensure compliance with cybersecurity ethics; and

n) All service providers with access to the University's data shall sign a confidentiality and non-disclosure agreement.

3.6 Campus Wide Security Intelligence Gathering Policy

The campus wide security intelligence gathering policy shall enhance the university's situational awareness, assess potential threats, and proactively address security concerns, through the following guidelines:

a) The University shall drive expected synergy between COMSIT and Security Unit leveraging on technology-driven security intelligence system;

b) The University shall establish Digital Security command Centre to achieve real time escalation and security intelligence gathering;

c) There shall be accurate digital mapping of the University's locations for seamless deployment and management of digital security infrastructure; and

d) A staff of the University, a Cybersecurity expert, shall be responsible for data collection and analysis of security intelligence gathered.

3.7 Digital Infrastructure and E-Resources Sharing Policy

In order to foster a dynamic exchange of digital infrastructure, ICT services and e-resources to promote innovation and enhanced teaching, research and community development, the University shall:

a) encourage collaborative sharing of digital infrastructure, licensed e- resources among partners subject to a valid Memorandum of Understanding (MOU), copyright and licensing agreement;

a) promote strict adherence to copyright laws and licensing agreements when reproducing, sharing, or distributing digital contents;

b) establish principles of responsible use, emphasising ethical and legal responsibilities among collaborative partners with regards to the sharing of digital infrastructure and e-resources; and

c) outline strategies for the preservation and long-term storage of digital assets.

3.8 Acquisition and Renewal of Relevant Software Policy

To ensure globally competitive standards in software usage and maintenance, the following refined guidelines shall be instituted:

a) The University shall provide proprietary and licensed Integrated Development Environment (IDE) packages to support software development, deployment and soft skill acquisition;

b) The Academic Planning Unit shall collate all software needs of the University and provide same annually to COMSIT for suitable implementation;

c) Open Source Software deployment shall be given first priority while licensed software shall only be considered provided there is a sustainability plan in place;

d) Open Source Software deployment culture of consistent security update shall be adhered to;

e) The university shall maintain an up-to-date inventory system of all software to effectively track expiration dates and renewal requirements;

f) Review the usage and necessity of each software application and ICT resources to determine if renewal is warranted while working with Procurement Unit for timely renewal;

g) All software deployed shall conform with internationally recognised standards of quality and security with primary focus on its capability and compatibility;

h) There shall be a comprehensive documentation provided by the vendor of all software tools to include user manuals, installation guides, configuration manuals, and troubleshooting documentation;

i) Software vendors shall be selected based on reputation, training, support offered and cost effectiveness

3.9 Intellectual Property Protection Policy

This policy underscores University's commitment in fostering an environment where the intellectual contributions of her academic community deployed via her digital infrastructures and ICT services are respected, protected, and ethically utilised. The University shall:

a) be committed to safeguarding intellectual property rights and promote a culture of respect for creative and innovative work while prohibiting unauthorised distribution, reproduction or sharing of copyright materials;

b) establish clear guidelines for the protection of intellectual property assets;

c) clarify the ownership rights of intellectual property created by staff, students, and external collaborators in various contexts, including sponsored research, individual initiatives, and collaborative projects;

d) ensure that all intellectual properties are timely disclosed and reported to the designated office responsible for intellectual property management;

e) define the processes for protecting, commercializing, and licensing intellectual property assets in accordance with relevant laws and regulations of the University;

f) ensure that patent and research breakthrough products are visible on the University website;

g) specify the distribution of revenues generated from the commercialisation of university-owned intellectual property, ensuring fair and equitable participation of the creators;

h) approve all multimedia contents in line with the University established procedure prior to upload; and

i) establish mechanisms for enforcing intellectual property rights and resolving disputes among creators, collaborators, and the university.

3.10 Portal / Web Policy

For a 21st Century University, Portal and Web services are pivotal to achieving and sustaining global competitive advantage. Thus, the following guidelines are recommended. The University shall:

a) ensure that the portals are hosted with a reputable host provider that will guarantee availability, scalability, and security;
b) engage a reputable agent for seamless subscription fulfilment and management of cloud resources hosting;
c) imbibe the culture of regular vulnerability assessment of the portal and web solutions;
d) ensure that proprietary software (database client and IDE) is used in the development, deployment and management of Portal and Web solutions; and
e) adopt an integrated, enterprise, and scalable Portal solution architecture.

3.11 Enforcement Mechanism Policy

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

a) COMSIT in collaboration with Corporate Affairs Directorate, shall ensure a wide awareness and dissemination of the ICT policy;

b) The COMSIT Directorate shall have a system audit unit made up of ICT audit specialists who will be charged with the responsibility of compliance with the ICT policy within the University and where necessary take appropriate remedial measures;

c) Unilorin ICT audit team shall have full access to all information system audit trails and be able to execute queries on any particular process where necessary to assist the enforcement of the Unilorin ICT policy; and

d) All substantiated violations of the ICT policy in the system shall be officially documented and reported to the Vice Chancellor through Director COMSIT.

For the sustainability of the newly reviewed ICT policy, the following recommendations are made:

a) The University shall develop a clear organogram for the Directorate of COMSIT for seamless implementation of the policy;
b) The University shall put in place strategy to achieve stakeholder adoption;
c) The University shall remit 5 percent of contract sum for all ICT related project to COMSIT for seamless support and maintenance;
d) Directors of COMSIT shall be appointed from ICT related Departments/Units; and
e) Appointed Directors of COMSIT shall abide by the University approved ICT policy.

REFERENCE

This policy was drafted taking into consideration the University's rules and regulations.

Approval and Acknowledgement

The reviewed ICT policy after due consideration shall be processed for the approval of Senate and subsequently acknowledged by all Staff.

Revision History

This is the first review of the initial University ICT policy (2018-2023). The implementation of the newly reviewed ICT policy shall span between 2023-2028.

MEMBERSHIP OF ICT POLICY REVIEW COMMITTEE

Contact details for individuals or departments responsible for policy administration and support.

1. Prof. R. A. Jimoh, Director, COMSIT
2. Mrs. Falilat F. Sheriff, Director, Legal Unit
3. Dr. A. A Oloyede, Director, CREDIT
4. Mr. K. A. Saadu, University Procurement Officer
5. Mr. K. A. Adewoyin, Rep. Registrar
6. Mr. G. O. Eromosele, Rep. University Librarian
7. Prof. Oluwakemi C. Abikoye, Rep. Computer Science Department
8. Dr. A. T. Ajiboye, Rep. Computer Engineering Department
9. Dr. M. O. Oloyede, Rep. Information Technology Department
10. Dr. A. O. Otuoze, Rep. Electrical/ Electronic Engineering Department
11. Engr. H. O. Akande, Head, Network Operations Centre
12. Dr. R. A. Tomori, Deputy Director, COMSIT
13. Mr. Y. Suleiman, Deputy Director, COMSIT
14. Mr. A. B. Yusuf, Deputy Director, COMSIT
15. Engr. J. A. Adesina, - Secretary

APPENDIX- DEFINITION OF UNIVERSITY OF ILORIN ICT POLICY KEY TERMS

Acceptable Use: This term refers to the guidelines and expectations regarding the responsible and ethical use of university ICT resources, often outlining what is permitted and prohibited.

Access Control for Data Centre: Access control for a data centre refers to the measures and protocols in place to regulate and restrict physical and digital access to the data centre facility. It includes authentication, authorization, and security mechanisms to ensure only authorized personnel can enter and access the data centre.

Access to Audit Trails: Access to audit trails refers to the ability to view and analyze records of events and activities within an information system or network. These audit trails provide a chronological record of actions and can be accessed for security monitoring and analysis.

Acquisition and Procurement: Acquisition and procurement involve the processes of acquiring goods, services, or assets for an organisation. It includes activities such as sourcing, purchasing, and contract management.

Adherence to Copyright Laws: Adherence to copyright laws means complying with legal regulations that govern the use, reproduction, and distribution of copyrighted materials. It involves respecting the intellectual property rights of creators and authors.

Alternative Power Backup Solutions: Alternative power backup solutions refer to backup power sources, such as renewable energy systems, that can provide electricity in case of primary power source failures.

Authentication Procedures: Authentication procedures are the methods and processes used to verify the identity of users or entities attempting to access a system, network, or application. Authentication typically involves username and password verification, biometrics, or multi-factor authentication.

Automation of Core Processes: Automation of core processes involves the use of technology and software to streamline and execute essential organisational processes with minimal manual intervention. It aims to improve efficiency and reduce human error.

Awareness and Dissemination: Awareness and dissemination refer to the activities of creating awareness and distributing information or policies within an organisation. It ensures that stakeholders are informed about important matters or changes.

Balanced Approach to Local Hosting and Cloud Solutions: A balanced approach to local hosting and cloud solutions means adopting a strategy that combines both on-premises (local) hosting and cloud-based solutions to meet an organisation's computing and storage needs effectively.

Bandwidth: The capacity or speed of an internet connection, typically measured in bits per second (bps) or gigabits per second (Gbps).

Campus-Wide Security Intelligence Gathering: Campus-wide security intelligence gathering involves collecting and analyzing security-related information and data across an entire campus or organisation to assess potential threats, vulnerabilities, and security risks.

Cloud Storage: A service that allows data to be stored, managed, and accessed over the internet from remote servers, providing scalability and accessibility.

Collaborative Sharing: Collaborative sharing refers to the practice of sharing digital infrastructure, resources, or information among partners or collaborators to foster cooperation, innovation, and efficient use of resources.

Collation of Software Needs: Collation of software needs involves the process of gathering and compiling a comprehensive list of software requirements and preferences within an organisation to inform software acquisition and deployment.

Commercialization and Licensing: Commercialization and licensing refer to the process of turning intellectual property or innovations into commercial products or services. Licensing involves granting permission to use, distribute, or sell these products or services under specific terms and conditions.

Comprehensive Documentation: Comprehensive documentation includes detailed and thorough records, manuals, guides, or reports that provide comprehensive information about a particular subject, process, or system.

Confidentiality and Non-Disclosure Agreements: Confidentiality and non-disclosure agreements are legally binding contracts that stipulate the terms and conditions under which parties agree to protect and not disclose confidential information shared between them.

Constant Review of Automations: Constant review of automations involves regularly evaluating and reassessing automated processes and systems to ensure they remain effective, efficient, and aligned with current needs and standards.

Copyright: A legal protection granted to the creators of original works, giving them exclusive rights to reproduce, distribute, and display their work.

Custodian of Super Privileges: The custodian of super privileges is an individual or entity responsible for managing and safeguarding highly privileged access rights and permissions within an organisation's systems and networks.

Cybersecurity: The practice of protecting computer systems, networks, and data from theft, damage, or unauthorized access.

Cybersecurity Measures: Cybersecurity measures encompass the policies, practices, and technologies implemented to protect an organisation's digital assets and information from cyber threats, including unauthorized access, data breaches, and malicious activities.

Cybersecurity Unit: A cybersecurity unit is a specialized department or team within an organisation dedicated to managing and enhancing cybersecurity efforts, including threat detection, incident response, and security strategy development.

Data Backup and Disaster Recovery: Data backup and disaster recovery refer to the processes and strategies for creating and maintaining copies of data to ensure its availability and rapid restoration in the event of data loss or disasters.

Data Centre: A facility used to house computer systems and associated components, such as servers, storage systems, and networking equipment, often used for data processing and storage.

Data Collection and Analysis: Data collection and analysis involve gathering and examining data to extract meaningful insights, patterns, or trends. It is essential for informed decision-making and problem-solving.

Data Management: Data management involves policies and practices related to the classification, storage, backup, retention, and handling of data within an organisation.

Decommissioning of Obsolete Infrastructure: Decommissioning of obsolete infrastructure involves the retirement and removal of outdated or no longer needed physical or digital assets, such as hardware or software.

Deployment of Software: Deployment of software involves the installation, configuration, and implementation of software applications or solutions within an organisation's computing environment.

Digital Infrastructure and E-Resources Sharing: Digital infrastructure and e-resources sharing entail collaborating and sharing digital infrastructure components, services, and electronic resources (e.g., databases, documents) with partners or stakeholders.

Digital Infrastructure Inventory: A digital infrastructure inventory is a record or database containing details of all digital assets, equipment, and components within an organisation's IT infrastructure.

Digital Infrastructure Provisioning: Digital infrastructure provisioning includes the planning, acquisition, and deployment of digital resources and technology infrastructure to support organisational needs.

Digital Infrastructure Reduction, Reuse, and Recycling: This term refers to the practice of minimizing the environmental impact of digital infrastructure by reducing resource consumption, reusing components, and recycling electronic equipment responsibly.

Digital Infrastructures: Digital infrastructures encompass the hardware, software, networks, and systems that enable digital communication, data processing, and information sharing within an organisation.

Digital Mapping: Digital mapping involves creating electronic representations of geographic areas or locations, often using geographic information systems (GIS) technology.

Digital Security Command Centre: A digital security command Centre is a centralised facility equipped with technology and personnel responsible for monitoring and responding to security threats and incidents in real-time.

Disclosure and Reporting: Disclosure and reporting refer to the act of revealing or making known information, incidents, or events, often in compliance with organisational or legal requirements.

Distribution of Revenues: Distribution of revenues involves allocating income or profits generated from various sources, such as commercialization or licensing, among relevant stakeholders or entities.

Documentation of Violations: Documentation of violations entails recording instances where policies or regulations have been breached or where non-compliance has occurred.

Enforcement Mechanism: An enforcement mechanism is a structured approach or system for ensuring compliance with policies, rules, or regulations within an organisation.

Enterprise: In the context of software or solutions, "enterprise" typically refers to systems designed for large organisations with complex needs.

External Collaboration: Policies and guidelines for engaging with external collaborators, sharing resources, and collaborating with organisations outside the university.

ICT Services: Information and Communication Technology (ICT) services encompass various technology-related services such as network connectivity, software applications, support, and other digital services provided by an organisation.

Incident Response: Procedures and protocols for how the organisation handles security incidents, data breaches, and policy violations.

Integrated Development Environment (IDE): A software application that provides comprehensive tools for software development, including code editing, debugging, and testing.

Intellectual Property: Creative work or ideas, such as inventions, and software that can be legally protected through patents, copyrights, or trademarks.

Knowledge-Based Expert Systems: Knowledge-based expert systems are computer programs or software that use a knowledge base of facts and rules to solve complex problems or provide expert-level advice and decision-making in specific domains. These systems simulate the decision-making abilities of human experts.

Maintenance and Repair: Maintenance and repair refer to the activities and processes involved in keeping equipment, machinery, systems, or infrastructure in working order. Maintenance focuses on preventative measures to ensure proper functioning, while repair addresses the restoration of functionality when something malfunctions or breaks.

Measurement of Adequacy, Reliability, and Sustainability: This term indicates the assessment and evaluation of how sufficient, dependable, and sustainable digital

infrastructure and ICT services are within an organisation. It involves measuring whether the systems meet the required standards and can be maintained over time.

Network and Infrastructure: Network and infrastructure encompass the physical and digital components that enable data transmission, communication, and information sharing within an organisation. This includes hardware (e.g., servers, routers) and software (e.g., applications, protocols).

Network Earthing System: A network earthing system refers to the grounding or earthing arrangements in a network infrastructure. It ensures that electrical systems are properly grounded to prevent electrical shocks, interference, and to protect against power surges.

Network Operations Centre (NOC): A Network Operations Centre is a centralised facility where network administrators and technicians monitor, manage, and maintain an organisation's network infrastructure, ensuring its availability, performance, and security.

Official Communications: Official communications pertain to formal messages, announcements, or information disseminated by an organisation to its members or stakeholders. These communications are typically authoritative and convey important information or directives.

Open Source Software Deployment: Open source software deployment involves using software that is distributed with a license that allows users to view, modify, and distribute the source code freely. It is often used as an alternative to proprietary software.

Orientation for New Staff and Students: Orientation is a process that familiarizes new staff and students with the organisation's policies, procedures, culture, and resources. It helps newcomers integrate into the community and understand their roles and responsibilities.

Outdoor Access Points Security: This refers to the security measures and protocols in place to protect outdoor network access points from unauthorized access, tampering, or physical damage.

Ownership Rights: Ownership rights pertain to the legal rights and privileges that individuals or entities have over a particular asset or property, including intellectual property or tangible assets. These rights define ownership and control.

Periodic Training: Periodic training involves regular and recurring training sessions or programs designed to update and refresh the knowledge and skills of individuals. It ensures that staff and students stay current with relevant information and practices.

Policy Framework: A policy framework is a structured set of guidelines, principles, and objectives that provide a foundation for developing and implementing policies within an organisation. It outlines the organisation's approach to governance and decision-making.

Policy Statement: A policy statement is a concise and formal declaration within a policy document that states the organisation's position, intentions, or directives on a particular matter or issue.

Portal/Web Policy: A portal/web policy outlines the rules, guidelines, and best practices related to the development, management, and usage of web portals or websites within an organisation.

Preservation and Storage: Preservation and storage involve the activities and processes for archiving and safeguarding digital assets, documents, or data to ensure their long-term accessibility and integrity.

Privacy and Compliance: Policies and practices related to data privacy regulations and compliance requirements, ensuring that data is handled in accordance with legal and ethical standards.

Professional Certifications: Professional certifications are credentials awarded to individuals who have demonstrated a certain level of expertise, knowledge, and competence in a specific profession or field. These certifications are often recognized and respected within the industry.

Proprietary Software Usage: Proprietary software refers to software that is owned and licensed by a specific company or entity. Proprietary software usage involves the use of such software within an organisation.

Safeguarding Intellectual Property Rights: Safeguarding intellectual property rights involves protecting and enforcing the legal rights associated with intellectual property, such as patents, copyrights, and trademarks, to prevent unauthorized use or infringement.

Security Audits: Security audits are systematic assessments and evaluations of an organisation's information systems, networks, and security measures to identify vulnerabilities, weaknesses, and areas that require improvement.

Security Measures: Security measures encompass the policies, procedures, and technologies put in place to protect an organisation's digital assets and information from threats, breaches, and unauthorised access.

Security-Proof Network Equipment Control Rooms: These are specialized rooms designed to house network equipment and ensure their security, often featuring access controls, surveillance, and environmental controls.

Selection of Software Vendors: The process of choosing and contracting with software vendors or suppliers to provide specific software solutions or applications to meet an organisation's needs.

Service Level Agreement (SLA): A formal agreement that defines the level of service, performance standards, and responsibilities expected from a service provider in a contractual relationship.

Staff and Student Training: Training programs designed to educate and develop the skills of staff and students to fulfill their roles effectively within an organisation.

Staff Strength: The total number of employees or personnel working within an organisation, typically measured as full-time equivalents.

Student Population: The total number of students enrolled in an educational institution during a specific period.

Sustainable ICT Ecosystem: A sustainable ICT ecosystem refers to an information and communication technology environment that is designed to be environmentally friendly, efficient, and capable of long-term growth and adaptability.

System Audit Unit: A system audit unit is a specialized team or department within an organisation responsible for conducting audits of information systems and technology infrastructure. Their role is to assess the security, compliance, and performance of these systems, identify weaknesses or vulnerabilities, and recommend improvements.

Training and Awareness: Training and awareness refer to the activities and programs designed to educate individuals within an organisation about specific topics, such as information technology practices, security protocols, and best practices. This

helps employees and stakeholders become more knowledgeable and conscious of important aspects related to their roles or the organisation's goals.

Training for Role Players: Training for role players involves providing instruction and guidance to individuals in specific roles within an organisation. This training ensures that individuals understand their responsibilities and can perform their duties effectively. It can encompass both general job-related training and specialized training for particular roles.

Training Manuals: Training manuals are written documents or guides that provide structured information and instructions for training purposes. They typically include step-by-step procedures, explanations, and reference materials to help individuals learn and perform specific tasks or functions.

University Community: The university community refers to all individuals who are part of or associated with a university, including students, faculty members, staff, administrators, and sometimes alumni. It represents the collective body of people who contribute to and participate in the university's activities and goals.

User Responsibilities: The roles and responsibilities of individuals within the organisation, such as faculty, staff, students, and administrators, in using and managing ICT resources.

User Training Manuals: User training manuals are instructional documents or guides specifically created for individuals who are using a particular system, software, or technology. These manuals provide users with information on how to effectively and correctly use the technology or service.

Vendors' Registration: Vendors' registration is the process by which suppliers, companies, or individuals who provide goods or services to an organisation officially register their details and credentials. This registration often includes verification of qualifications, legal documentation, and compliance with procurement or vendor management policies.

Vulnerability Assessment: Vulnerability assessment is the process of identifying, evaluating, and documenting weaknesses or vulnerabilities in an organisation's information systems, networks, or infrastructure. The assessment helps to determine potential security risks and threats that need to be addressed.

Warranty Agreements: Warranty agreements are legal contracts or guarantees provided by manufacturers or suppliers to ensure that their products or services meet certain quality and performance standards. These agreements outline the terms and conditions under which the warranty is valid and what remedies are available if the product or service fails to meet these standards.

Zone Officers: Zone officers are individuals responsible for overseeing and managing specific geographic or functional areas within an organisation's network or infrastructure. They are typically responsible for the maintenance, monitoring, and troubleshooting of systems and services within their designated zones.

ACRONYMS FOR ICT POLICY

The following is the collection of acronyms used in the University of Ilorin ICT Policy

COMSIT: Directorate of Computer Services and Information Technology

ICT: Information and Communication Technology

IDE: Integrated Development Environment

ISPs: Internet Service Providers

MIS: Management Information System

NOC: Network Operations Centre

NUNet: Nigerian Universities Network

OEM: Original Equipment Manufacturer

SLA: Service Level Agreement

UNILORIN: University of Ilorin

VoIP: Voice over Internet Protocol