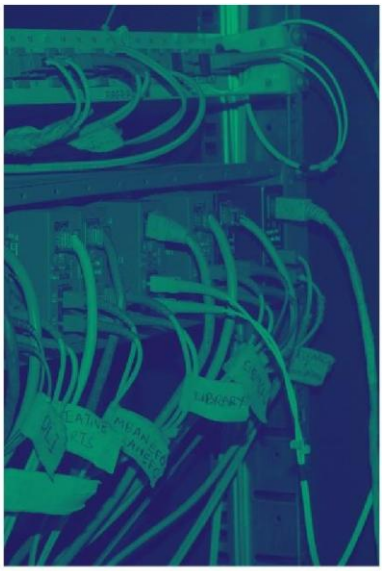


ICT POLICY

UNIVERSITY OF LAGOS

MESSAGE FROM THE VICE-CHANCELLOR

Information and Communication Technology is central to sustaining the vision and mission of the University of Lagos as a top-class institution committed to excellence in knowledge, character, and innovation. In a world where the pace of change is unrelenting, ICT underpins governance, teaching, learning, research, and our service to society. This ICT Policy provides the framework to ensure that the University harnesses these tools responsibly, strategically, and sustainably.

The policy speaks to the daily operations of this University. It affirms the role of ICT in strengthening data governance, automating administrative workflows, supporting electronic elections, and improving access to health services through digital records. It is the University's vision for every student, staff member, and partner to work in an environment where ICT systems are secure, reliable, and user-centred.

The principles set out here are also values. Security, resilience, adaptability, compliance, sustainability, and ethical use of ICT are guidelines that define how we will conduct ourselves as an institution. They reflect our determination to ensure that digital transformation strengthens rather than distracts from our academic mission.

As Vice-Chancellor, I affirm the University's full commitment to this policy. We will invest in the infrastructure, processes, and training required for its implementation. We will monitor performance and hold ourselves accountable to measurable outcomes.

I call upon all Deans, Directors, Heads of Departments, staff, students, and partners to take ownership of this policy. Its effectiveness depends on collective action: compliance with standards, vigilance in cybersecurity, innovation in teaching and research, and collaboration in implementation. We will thereby ensure that the University of Lagos is a leader in digital transformation in Africa.

Professor Folasade T. Ogunsola OON, FAS
13th Vice-Chancellor,
University of Lagos

MESSAGE FROM THE DIRECTOR, ABS-CITS

Every day, the University depends on ICT systems to function. When these systems are not properly managed, the results are clear: delayed services, unreliable data, and networks that expose us to risks. These problems affect teaching, research, and administration alike.

This policy has been developed to reduce those risks and to make sure that everyone is working with the same set of rules. It sets out what is expected when using University systems, how responsibilities are shared, and what standards guide new projects or procurements. Without these rules, each unit would work in isolation, and the University would lose both efficiency and security.

The policy applies across the institution. A faculty handling student records, a medical centre using electronic health files, or a department moving to automated processes must all comply with the same requirements. Moreover, ABS-CITS cannot carry this responsibility alone. Every faculty, department, and office should take ownership for the responsible handling of the systems they use. Staff and students should follow the guidelines for safe usage and reporting. Researchers and instructors need to choose tools that meet our requirements for security and for smooth integration into the University's existing platforms. We must keep in mind that policy only becomes effective when everyone treats it as necessary for achieving our institutional goals.

For ABS-CITS, this policy guides how we maintain networks, secure information, and support users. It explains why we insist on compliance with data privacy rules, why we ask units to use approved systems, and why new platforms must be reviewed before they are adopted. These are not bureaucratic steps. They are safeguards that make ICT reliable for us all. We will continue to provide training, publish clear guidelines, and monitor system performance. My responsibility is to make sure that this policy is not merely produced, but to also ensure that it is put into consistent practice.

Professor Muhammed Olawale Hakeem Amuda
Director, Adetokunbo Babatunde Sofoluwe-Centre for Information Technology and Systems (2023-) University of Lagos

TABLE OF CONTENTS

PART A: GENERAL INTRODUCTION

1.0 BACKGROUND

Information Communication and Technology (ICT) is central to sustaining the vision and mission of the University of Lagos as a top-class institution for the pursuit of excellence in knowledge and character in a conducive environment for teaching, learning, research and development**;** where staff and students can interact and compete effectively with counterparts globally. In order to maximise the benefits of ICT for teaching, learning, administration and governance, the University of Lagos understands that the deployment of ICT infrastructure and services must be guided by a set of robust guidelines and instruments in the form of a policy document. Therefore, the University has designed and instituted a comprehensive ICT policy, which provides a regulatory framework for the planning, development, and provisioning of ICT infrastructure (including the safe and responsible use of ICT services.) to drive the vision and mission of the University, In addition, the policy is directed at ensuring value for investment and management of risks associated with deploying ICT for teaching, learning, research and development, administration and governance, in alignment with the University's strategic goals and objectives.

2.0 DECLARATION

The University of Lagos is committed to the safe and responsible deployment of ICT to drive University processes and services. The University commits to ensuring that ICT equipment, devices and supporting accessories comply with all standard specifications and regulations of relevant regulatory bodies (NCC, FCC??, etc.) and that deployed infrastructure is secured at all times against cyber threats and attacks, as well as unavoidable disasters. For responsible use, the University declares that its ICT infrastructure and associated applications shall not be

deployed for any service(s) other than those in the pursuit of the University's core vision and mission. Responsible use also extends to fair usage (needs to be clearly defined) of the University's ICT infrastructure and services.

3.0 POLICY OBJECTIVE

The main objective of the UNILAG ICT Policy is to provide documentation that will guide the University's ICT strategic initiative, including but not limited to the following:

a. Governance, administration and management

b. ICT infrastructure design, development, maintenance, and investment

c. Software acquisition(?), subscription and development

d. Workflow automation (processes and services)

e. Scope and procedures for services delivery and career structure for ICT personnel

f. ICT vendors and third-party engagements, including acceptable service-level agreements types and associated provisions.

g. ICT capacity building for members of the University Community

4.0 PHILOSOPHY/VISION/MISSION

- PHILOSOPHY

The University's ICT strategy is motivated by the desire to ensure that every aspect of the University's processes and services is constantly attuned to digital transformation and automation opportunities, towards continually improving efficient and effective services, characterised by readily discernible value for investment.

- VISION STATEMENT

This policy document envisions a University of Lagos where, all core business processes and services are fully automated, empowering students and staff to be globally competitive.

- MISSION STATEMENT

The harnessing of ICT infrastructure and associated applications to support the delivery of business processes concerning teaching, learning, research and development, administration and governance, in synchronism with the University's vision and mission statements.

- SCOPE

The University of Lagos' ICT policy provisions extend over the provisioning, governing, administration, and management of University ICT assets, infrastructure, and support for services delivery. Specifications include privileges and responsibilities for all categories of staff, students, vendors, and third parties, that interface with the University's ICT infrastructure and services. The provisions also embody a manual that prescribe scope and procedure for the services deliverable by the main ICT support unit, as well as a career structure for ICT personnel.

5.0 DEFINITION OF TERMS

1. Acceptable Use: The usage of ICT infrastructure and services in accordance with the relevant provisions of the University ICT policy

2. Access Control: A system that implements regulations concerning permission or eligibility for physical or remote access to an ICT facility, or view or retrieve applications or data.

3. Artificial Intelligence: The ability of a computer or computer-controlled device to perform the functions otherwise attributed to humans.

4. Authentication: The process of verifying the identity of a user accessing ICT resources or the process that validates a user's login information by comparing the username and password to a list of authorised users.

5. Availability: The assurance that information and services are delivered when needed.

6. Backup: As used in ICT, a backup is a copy of data (computer) and applications taken and stored elsewhere for use later; particularly for disaster recovery purposes

7. Bandwidth: In this context, it is the capacity at which a network can transmit and retrieve data. It is measured in bps.

8. Bespoke/In-house software: A tailor-made software developed by the ABS-CITS' ICT personnel or co-created or developed by other members of the University community.

9. Career Structure: A series of progressions that an ICT personnel can make at the University of Lagos from the least to the peak.

10. CBT: Computer-Based Testing, which is a facility that deploys computers to conduct performance/knowledge assessment tasks.

11. Cloud Services: The University's ICT services that include data storage, computing and allied services hosted in remote facilities, often off-

premises

12. Code of Conduct: A set of rules expected to guide usage or engagement with a provided service.

13. Confidentiality - The assurance that information is disclosed only to those systems or persons who are intended to receive the information.

14. Core ICT Services: The several main ICT solutions and resources offered by the University to her community, such as internet connectivity, email messaging, VoIP telephony, Learning Management System, Computer-based Testing services, record / information management services, digital library repository services, virtual and video conferencing, digital media services, e-administration, and e-examination/thesis, and e-community.

15. Data custodian/protection officer: Individual or group responsible for classifying data and generating guidelines for its lifecycle management. Synonymous with “information custodian.”

16. Data: Coded representation of quantities, objects and actions. The word “data” is often used interchangeably with the word “information” in common usage; and in another context, collections of related facts and statistics for reference or analysis

17. Digital systems: A discrete electronic aggregation of entities such as hardware, software and networks used to store, process and communicate.

18. Digital: data and information in electronic format (could also be analog!)

19. Disaster recovery: The process of restoring or reestablishing vital infrastructure and services to minimise service disruption occasioned by unforeseen /unavoidable circumstances.

20. Downloading: A network trafficking of data files originating from an external network and destined for the University network.

21. E-learning and digital resources: The deployment of electronic resources to support teaching and learning.

22. E-mail and messaging services: The use of electronic devices to exchange messages, notifications, and digital content within and outside the University of Lagos.

23. Emerging Technologies: These are evolving digital solutions that make intelligent decisions based on computing devices' predictive power.

24. Enterprise Resource Planning: A software system that onboards organisational information, processes, governance, and administration via workflow automation.

25. Hacking: The use of a computer or other technological device or system to gain unauthorised access to data held by another person or organisation.

26. Hardening Standard: protocols for addressing security vulnerabilities in hard/software

27. Hardware: This is also known as tangible ICT equipment that facilitates digital framework.

28. ICT Asset: This represents the embodiment of the University's ICT hardware and software in the University's digital network such as Applications, computer systems, servers, networks and related devices owned by or entrusted to UNILAG.

29. ICT ecosystem: The entire University’s ICT infrastructure, solutions, services and users.

30. ICT Security: Cocktail of measures and applications implemented by the University to ensure that the network is not vulnerable to cyber threats and attacks.

31. Impact: A combination of data confidentiality, integrity and availability. Whether a set of data is LOW, MEDIUM, HIGH, or of VERY HIGH impact

will inform the data classification and whether or not it should be considered sensitive data.

32. Information custodian: Individual or group responsible for classifying data and generating guidelines for its lifecycle management.
33. Information: Data processed into a form that has meaning and value to the recipient to support an action or decision. “Information” is often used interchangeably with “data” in common usage.
34. Integrity - The assurance that information is not changed by accident or through a malicious or otherwise criminal act.
35. Internet Domain Naming Convention: These are the global best practices guiding internet domain names.
36. Licences: defines the permission to use and distribute hardware and software within original equipment manufacturers’ guidelines.
37. Logs: Collections of information typically used to document activity and events.
38. MFA (Multi-Factor Authentication): The use of two or more authentication methods to enhance security.
39. Mirror site: A duplicate Web site that contains the same information as the original Web site and reduces traffic on that site by providing a local or regional alternative.
40. Mobile Computing: The ubiquitous connection of portable devices in order to access data and services irrespective of time, space and geography.
41. Monitoring tools: Logging and analysis tools used to accurately determine traffic flows, utilisation, and other performance indicators on a network.
42. Network: The interconnectivity of two or more devices to exchange files or information.

43. Operational Manual: The sequential documentation of protocols or guidelines governing the processes and procedures for performing the range of ICT functions domiciled at the University ICT directorate.

44. P2P (peer-to-peer): In the context of this policy, P2P is direct data communication between two or more network-capable devices over the Internet or other network, usually to share any data file (including, but not limited to, music, pictures, video, software, and documents).

45. P2P file sharing: direct communication or sharing of resources between commercial or private users of the Internet.

46. P2P network: A collection of distributed network-capable devices participating in P2P activity.

47. Peer-to-peer (P2P) application: Any application that allows a network-capable device to participate in one or more P2P networks.

48. Proxy server: A software package running on a server positioned between an internal network and the Internet.

49. Quality Assurance: Broad processes and practices for preventing quality failure or deterioration of service delivery.

50. Remote Access: The ability of a user to access a device, network, or service from any location.

51. Service Level Agreement (SLA): A documentation of a formal agreement between a service provider and a client, which outlines the commitments, obligations, rights and privileges, and restrictions

52. Sharing: In the context of this policy, it is the action and activity of making any data file available to one or more P2P networks.

53. Software: these are computer programs that drive processes and services whose use may be governed by commercial regulations. It may be bespoke or bought off the shelf.

54. Streaming: The playing of sound or video over the Internet or a computer

network in real time.

55. Subscription: The right to use and/or maintenance acquired applications/solutions through a contractual agreement between the proprietary owners and the end-users.

56. Sustainable Funding: deliberate and strategic undertaking by the University to consistently and perpetually prioritise investment in digital infrastructure to sustain the vision and mission of the University.

57. The University network and networking resources: describe all materials and devices owned by the University and used to provide network connectivity to any network-capable device. This includes all jacks, cables, hubs, wireless access points, switches, and routers, etc.

58. Third-party service providers: Any unaffiliated person, company or entity that has a contractual agreement to deliver ICT services to the University of Lagos.

59. UNILAG Information: All information that the UNILAG or its agents use in the course of conducting UNILAG business.

60. Uploading: Network trafficking of data files originating from the University network and destined for an external network.

61. User Accounting: The profiling of access logs and other details associated with a user accessing a network or digital services.

62. User Authentication: A process that verifies a person's identity and determines eligibility for an online service, connected device or other resource.

63. User Authorisation: The process of extending privileges to a user to access a resource or function.

64. User: Any individual with authorised access to UNILAG ICT resources.

65. Web Hosting: A service that provides storage for files that make up a website, as well as the software, physical hardware, and network infrastructure.

66. STANDARDS/BEST PRACTICES FOR VARIOUS ITEMS?

PART B: UNIVERSITY OF LAGOS ICT DIRECTORATE

1.0 ABOUT THE ICT DIRECTORATE

Named after its 10th Vice-Chancellor, the University's ICT Directorate, Adetokunbo Babatunde Sofoluwe-Centre for Information Technology and System (ABS-CITS), administers and coordinates ICT infrastructure and support services within the University of Lagos. Since its establishment in the late 1960s as the Institute of Computer Studies, the directorate has constantly reviewed and expanded its mandates. Initially, the focus of the institute was to expose the students to the emerging world of computer technology. However, in the 1970s, the institute evolved into a computer centre that not only provided training for students but also offered computer services to the technology industry.

Then, in 2005, the University during the administration of the 8th Vice-Chancellor, the distinguished late Professor Oyewusi Ibidapo-Obe (OFR, FAS) expanded the mandate of the computer centre to accommodate and manage the University's internet network infrastructure, access control and surveillance, and student information management system. He named the expanded unit "Centre for Information Technology and Systems (CITS)". In the last 15 years, new ICT frontiers have emerged which has improved teaching, learning, research and development, administration and governance, such as enterprise resource planning, learning management systems, virtual communication platforms, and digital immersions. This further necessitates the expansion of the mandates of the ICT directorate and arming the centre with the requisite human capacity to handle the expanded scope.

ABS-CITS has built up a rich repository of experience about the University ICT landscape, making it the natural directorate for implementing University ICT policy.

2.0 MANDATE

The ABS-CITS of the University of Lagos shall be responsible for the design, planning, coordination, administration and management of all ICT-related activities in the University, ensuring that there is value for investment. It shall be responsible for providing strategic direction and playing an advisory role in all ICT-related matters for both the Vice-Chancellor and the Senate. The specific mandates of the directorate shall include but not be limited to:

1. Designing and planning the ICT infrastructure landscape for the University to support teaching, learning, research and development, administration and governance in alignment with university vision and mission statements.

2. Administering, managing and superintending over the ICT infrastructure in the University while ensuring value for investment.

3. Ensuring that members of the University community are digitally literate (training and retraining) and familiar with ICT trends, equipment and applications of relevance to the University's core business and ancillary proceses..

4. Advising the Vice-Chancellor and Senate of the University on emerging trends and global best practices in the ICT sector, as may be desirable.

5. Formulating guidelines and protocols that guide the deployment and usage of ICT infrastructure for university processes, businesses and services.

6. Ensuring that the University's internet network and supporting infrastructure are robust, effective and secure to support University processes and services.

7. Coordinating and managing the University ERP, LMS, CBT, cybersecurity infrastructure and other digital facilities to optimise University workflow processes, teaching, learning, assessment, research and development, administration and governance, including public engagement.

8. Providing technical specifications for hardware and software requirements to

sustain the University ICT infrastructural assets and end-user devices.

9. Ensuring safe and responsible deployment of ICT to drive University processes and services.

10. Serving as contact and representative in interfacing, regulating and managing University engagements with third party ICT service providers.

2.0 ADMINISTRATION

1. The Vice-Chancellor shall oversee the directorate for ICT through the appointed management Board headed by a Professor as Chairman who shall be a senior professor of not less than ten years from engineering or physical sciences with significant experience in university administration in addition to exposure in ICT or digital ecosystems.

2. Amongst other considerations in constituting the Board of the directorate, the Vice Chancellor shall endeavour to include alumni representative who is well-established in ICT industry as a member of the Board.

3. The directorate shall be headed by a Director who shall be appointed by the Vice Chancellor to coordinate the day-to-day running of the directorate. The Director shall be supported by three Deputy Directors, as indicated subsequently: two for Akoka and one for the College of Medicine comprising the College and the Faculty of Pharmacy.

    i. Deputy Director I, Network, Infrastructure and Services (NIS)-Akoka

    ii. Deputy Director II, Operations, Akoka

    iii. Deputy Director III, CMUL (responsible for both NIS and Operations at the College).

4. The directorate shall have nine (9) operational units covering the mandates specified in Part B Section 2.2 or any other number of units as the mandates

change.

5. Each of these units shall be headed by a senior officer of not less than an Assistant Chief System Analyst/IT Equipment Engineer or equivalent.
6. The Director, ABS-CITS shall, at a request from a deserving autonomous academic unit like the School of Postgraduate , School of Foundation Studies, Distance Learning Institute, Office of the Dean, Students' Affairs or acting on assessment reports give approval for the establishment of an ICT desk at such a unit and the second requisite ICT staff to manage ICT-related activities at the Unit.

The organogram for the directorate is shown in Figure 1.

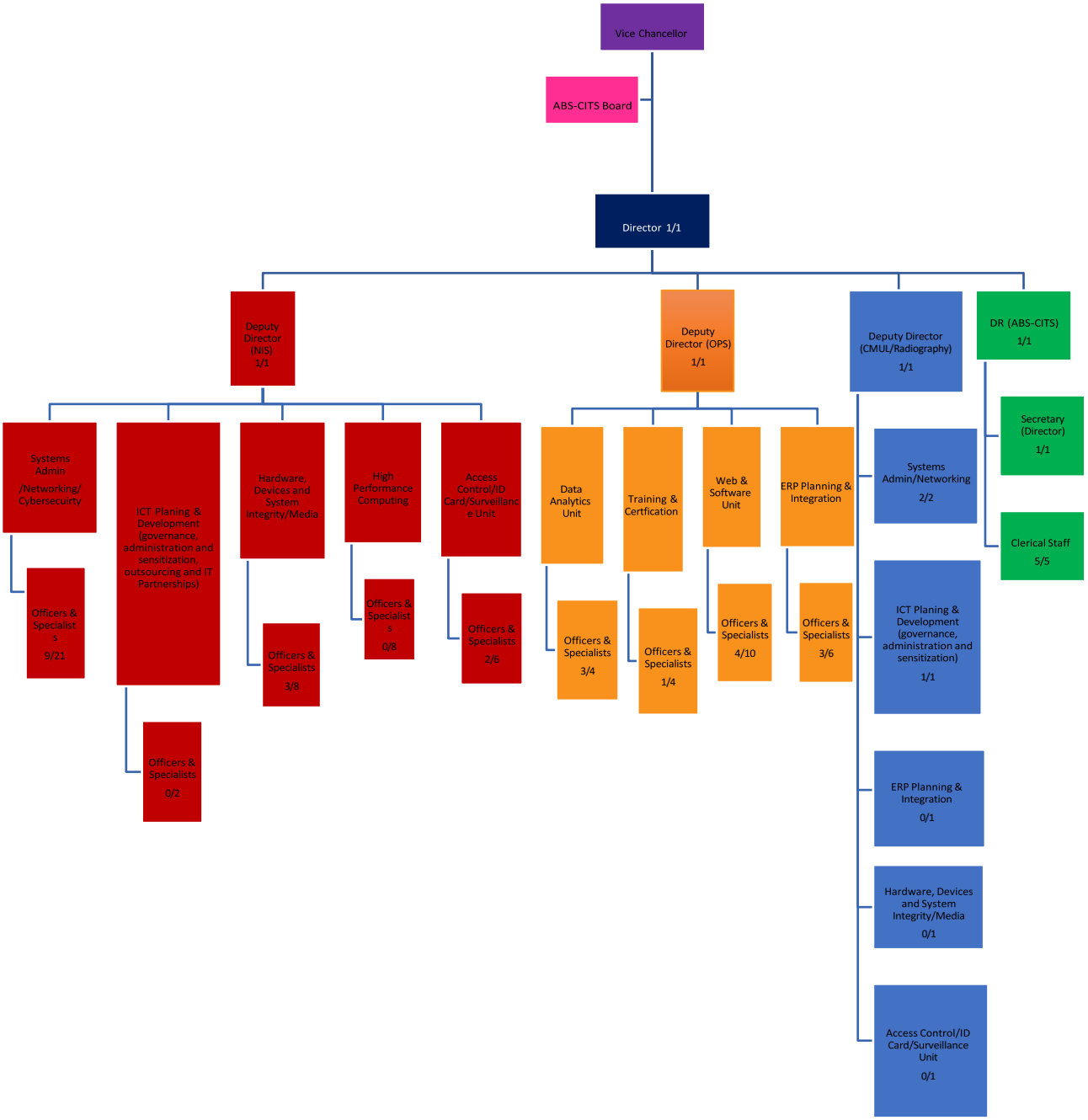


FIGURE 1. THE ORGANOGRAM OF ABS-CITS

7. Various units in the Directorate

   i. Systems Admin, Networking, and Cyber Security: This unit is responsible for the installation, configuration and maintenance, including ensuring reliable operation of computer systems, software and networks, especially multi-user computers, such as servers and other peripherals. This extends to systems upgrades (new releases and models), system performance monitoring, troubleshooting, ensuring efficiency of ICT Infrastructure at all times, and implementing robust security architecture through access controls, backups and firewalls. The unit is essentially the pillar anchoring the digital ecosystem of the University on which other ICT systems and operations rest.

   ii. ICT Planning and Development (ICT P&D): The ICT-P&D unit aggregates the ICT plans of the University in relation to its strategic goal of deploying digital infrastructure for automation of university processes and services. It drives the administration and implementation of the University's ICT policy. It regularly promotes the deepening of ICT culture, ensuring that ICT policy is well domesticated in members of the University community through sensitisation and awareness. It harvests behavioural patterns in the community to inform ICT policy direction and governance. Its crucial role is ensuring that the University's ICT infrastructure, systems and people align with its strategic goals and objectives, enhance operational efficiency, and remain secure and current. Further, the unit coordinates the engagement of outsourcing and ICT partnerships.

   iii. Hardware, Devices, and Systems Integrity/Media: This unit is concerned with providing specification guidance in the acquisition of hardware and devices (computer systems, scanning and photocopying machines, cameras, projectors and multi-media systems, screens, public address systems, and microphones) to

support a robust ICT infrastructure for the University. The unit equally assesses hardware and devices for replacement and boarding and conducts an integrity assessment of these assets to ensure optimal performance.

iv. Access Control/ID Card/Surveillance: The unit implements the digital security architecture for controlling access and tracking human traffic on campus to maintain the security and safety of the University's assets, staff, and students. The unit handles all activities and processes to control access to physical spaces and monitor activities. It designs and implements Access/ID Card and surveillance technology in-house or in partnership with third-party service vendors, incorporating smart features and emerging technologies.

v. High-Performance Computing: This unit houses a dedicated cluster of networked computers with advanced processors (including many-core CPUs and GPUs) for simulating and providing solutions to real-world problems in life and physical sciences, engineering, finance and economics, and other complex analysis.

vi. Data Analytics Unit: The University has a rich data ecosystem that is crucial in business decision-making based on curated behavioural data patterns via analytics. This unit provides institutional in-house service to support the Directorate of Academic Planning in deploying a custom Data Management and Analytics Solution (DAMAS) to guide strategic planning.

vii. Training and Certification: The Training & Certification (T & C) unit coordinates all training and certification programmes of the ABS-CITS dedicated to bridging ICT digital skill gaps in members of the University community and the public. The unit hosts the CISCO and HUAWEI academies. These two academies are reinforced by other bespoke short-term courses such as proficiency in computer, Graphic Design, Python programming and Data Analytics for the acquisition of *in-demand* digital skills. The unit ensures that employees and

professionals have the necessary skills and qualifications to perform their jobs effectively and meet industry standards.

viii. Web & Software Development Unit: This unit is responsible for the planning, design and development of bespoke software solutions and applications that drive the University e-processes and services (e.g., design and hosting of the University's website). Additionally, the unit renders third-party solutions to members of the University community and the public. Some of the recent solutions from this unit include the e-election platform, test-on-line, Electronic Medical Records (EMR) e-application for convocation ceremonies, e-inventory, Staff annual leave calculator, and exam-ticketing solution and e-notification of payslips, etc. The unit, in conjunction with the ICT Planning and Development, advises the University on software licensing and subscription.

ix. ERP Planning and Integration: The ERP Planning and Integration Unit coordinates the development of an Enterprise Architecture for the University which drives the Enterprise Resource Planning (ERP) vision of the University. The Unit hosts/coordinates a third-party commercial ERP solution for the automation of the University processes and services. The extension and integration of any other automation application to the University's EA is coordinated by the ERP Planning and Integration Unit.

PART C: ICT ADMINISTRATION AND GOVERNANCE (POLICY STATEMENTS / PROVISIONS)

C.1 Governance, Administration and Management

This section of the policy outlines the principles, guidelines, and procedures for managing and administering the University of Lagos (UNILAG) ICT ecosystem. The Governance, Administration and Management (GAM) philosophy of the UNILAG ICT policy is driven by the following key guidelines:

i. Security and Resilience: The security and resilience of our ICT ecosystem shall be accorded top priority at all times; cybersecurity shall be an integral part of every decision and action taken in managing and administering the University's ICT infrastructure.

ii. Innovation and Adaptability: The GAM framework of the ICT policy shall embrace flexibility, innovation and adaptability in leveraging emerging technologies to support University processes and services.

iii. Efficiency and Optimization: GAM is committed to optimising University ICT resources to support University processes and services, drive efficiency, and ensure value for investment.

iv. User-Centric Approach: The GAM approach in the University ICT policy shall be governed by putting the users at the centre of all ICT services.

v. Collaboration and Communication: GAM shall facilitate collaboration and partnership between the University ICT ecosystem, technical/development partners, service providers, original equipment manufacturers, and government regulatory agencies in deploying ICT to drive efficiency and enhance user experience.

vi. Data Privacy and Compliance: GAM shall ensure compliance with all statutory data privacy and protection Acts or regulations both in-country and internationally.

vii. Continuous Improvement: GAM shall commit to regular evaluation and upgrade of the University's ICT ecosystem to improve efficiency, enhance user experience, and maximise investment value.

viii. Sustainability and Environmental Responsibility: GAM shall commit to the responsible deployment of ICT solutions without adverse environmental impact and promote sustainable practices within the University ICT ecosystem.

ix. Ethical and Professional Conduct: GAM shall ensure the safe and responsible deployment of ICT infrastructure and services to serve the needs of the University community at all levels. It shall ensure that the code of conduct guiding the deployment and use of ICT infrastructure and services is strictly adhered to.

C.2 ICT Asset Provisioning and Management Policy

This section of the policy relates to issues related to the provisioning and management of the University of Lagos (UNILAG) 's ICT assets. It streamlines appropriate provisioning, deprovisioning, and management processes for the University.

2.1 Applicable Assets: assets applicable in this policy are:

a) **Hardware Assets:** These include the University ICT infrastructure, such as Network devices, Servers, multi-user systems, fibre networks, storage devices, end-user devices (desktop computers, laptops, portable computing devices) and ancillaries (fire alarm systems, burglary alarm systems, humidifier and air-conditioning).

b) **Software Assets:** Applications installed on infrastructure components and may be separately licensed. These include, but not limited to, Operating systems, middleware, databases and application software.

c) **Information Assets:** These include data such as student data, employee data, financial data, research data and allied data of the University community, which are important to the academic and research mission of the University.

i. Asset Management: All assets shall have a defined asset custodian, which shall ordinarily be the domiciled unit under the supervision and coordination of ABS-

CITS. The custodian shall have overall responsibility for the integrity, availability and protection of the asset. UNILAG, through the ABS-CITS, shall retain the overall responsibility and ownership of all assets, but members of staff, departments and units are tasked as custodians with creating the Register and maintaining these assets.

a. Domiciliation of Asset Registers: The asset register shall be domiciled at the Data Management office in addition to specific inventory at each unit.

b. All assets covered under the scope of this policy (owned and leased), excluding private individual end-user devices, shall be captured on the appropriate ICT Asset Register.

c. Inventory development and maintenance requirements shall vary with types of assets as indicated in the assets' manufacturers' documentations.

d. All such assets shall have an identified custodian, captured in the asset register, with appropriate identification number and be tracked throughout its lifecycle.

e. Periodic checks of the hardware and software installed shall take place to ensure that the asset register is an accurate reflection of the physical installations.

f. Assets owned by the University shall only be disposed of with the agreement of the assigned ICT Asset custodian. Such asset disposal shall ordinarily emanate from the assigned asset custodian.

g. When such assets are disposed of, the Asset Register shall be updated to show that the ICT asset has been decommissioned, including the method of disposal (the asset shall not simply be deleted from the register).

ii. Classification of Information Assets: The classification of information assets shall be governed by the University Data Classification Policy.

iii. Asset Life-Cycle

a. Asset Acquisition

i. ICT asset needs and specifications shall be determined by the ABS-CITS on behalf of the University which shall guide the acquisition of such asset.

ii. Assets covered under the scope of this policy shall be sourced via university-approved channels.

iii. For all ICT asset acquisitions, due consideration shall be accorded to the original equipment manufacturer (OEM) as primary source except when circumstance does not permit.

iv. All third-party ICT hardware and software shall be ascertained by the ABS-CITS for compliance and fitness for usage on the University network.

b. Asset Installation

i. All acquired ICT assets shall be fully and comprehensively tested and assessed for fitness for purpose, hardened to security standards and certified by the ABS-CITS and where applicable by the users before deployment.

ii. Hardening standards must be followed for all new hardware and software prior to production implementation.

iii. All acquired ICT assets shall be installed by appropriately certified personnel.

c. ICT Asset Upgrade and Management

i. The ICT Asset acquisition strategy and register shall be regularly updated to ensure that the University ICT ecosystem is current, addresses security threats, and is compatible with evolving technologies and business requirements. Therefore, the University's ICT asset acquisition strategy shall be reviewed and updated as required.

ii. The Director, ABS-CITS shall be responsible for the initiation and drafting of necessary changes and have them reviewed and approved by the ABS-CITS Board as appropriate before approval by the

University Senate. The Director of ABS-CITS shall communicate Senate Approved changes in the asset acquisition policy to the University community.

d. Asset Disposal and Recycling

i. All acquired ICT assets (hardware, software firmware, etc) shall be safely decommissioned at the expiration of the life span specified by the original equipment manufacturer.

ii. All data and configuration settings (including User IDs and passwords) shall be permanently deleted at decommissioning prior to disposal.

iii. ICT assets shall be disposed-off in a safe and environmentally friendly manner, in accordance with the guidelines in product manual, and Part C, Section a(viii) and local legal requirements (including copyright principles and licence terms).

e. Outsourcing and Third Parties

iv. Third party services shall be considered only where in-house capacity is unavailable or inadequate. Even at that, such third-party engagement shall, where feasible, be anchored on a co-creation model in which claims of copyright and intellectual property including source code shall be exhaustively agreed to.

a) Controls shall be in place to ensure that the third-party outsourcer complies with UNILAG asset management policies. (SPECIFICS OF THESE CONTROLS SHOULD BE PART OF THE POLICY STATEMENT-REFERENCE TO RELEVANT POLICY PROVISION SHOULD BE HELPFUL)

b) Frameworks shall be in place to ensure that third parties, outsourcers, and service providers do not put UNILAG at a disadvantage or vulnerable position, e.g., by not providing sufficient licence rights for software used by UNILAG staff. Outsourcers and service providers shall provide sufficient and

elaborate documentation that would empower the ABS-CITS directorate or any other user of such third-party applications, or services to competently operate, diagnose, maintain, engage and use them proficiently and competently.

c) The custodian of the ICT Policy shall ensure that the third parties, outsourcers and service providers comply with the relevant restrictions and requirements as set-out in the University ICT policy where applicable.

d) On termination of an outsourcing or service agreement, UNILAG shall be provided with sufficient licence rights to continue using the software previously provided by the outsourcer.

e) Controls and reporting processes shall be emplaced to ensure the efficient use of assets deployed for ICT service delivery to UNILAG to ensure value for investment.

f) All new and existing vendors of ICT services shall be subject to service audits in the areas of contract, fiduciary, performance, relationship and risk management.

2.2 SOFTWARE ACQUISITION, DEVELOPMENT AND USAGE POLICY

This section outlines the guidelines and procedures for managing the software procurement, upgrade, development and distribution processes for University of Lagos ("UNILAG"). It serves as a guide for UNILAG faculty and staff who would like to request new academic and administrative software as well as protocols guiding in-house software development, upgrade, support and maintenance.

2.2.1 Software Acquisition and Development

i. The ABS-CITS shall, in collaboration with such expertise as may be available within the University, but outside the Center, facilitate the acquisition and distribution of academic and other commercial software to support University

processes and services (administrative, academic, teaching, learning and research activities).

ii. Software acquisition shall be guided by compliance with software asset management best practices by collaborating with departments, faculty, and staff in procuring, managing, and complying with the terms of licensed software.

iii. ABS-CITS shall establish guidelines for the request, evaluation, and acquisition of commercial software and the development of in-house software, including guidelines for requesting software upgrades;

iv. ABS-CITS shall ensure that members of the UNILAG community using or procuring licensed software accept, and strictly adhere to the terms and conditions contained in the licensed agreements.

v. ABS-CITS shall outline the guidelines and procedures for distributing software (both proprietary and bespoke) acquired by the University, or any unit in the University for the purposes of enhancing university processes and services.

vi. ABS-CITS shall seek to maximise the benefits of the acquisition, development, distribution, maintenance, and use of software resources. This applies to any software (stand-alone, network or cloud-based) that is installed on any device(s) connected to UNILAG's networks or installed on university-owned hardware that is supported by ABS-CITS.

vii. *Any member of the University community seeking information about* the acquisition, development, or upgrade of software in the University for official use or to facilitate processes and services shall make appropriate requests to ABS-CITS for attention. Under no circumstance shall anyone attempt to use unlicensed software on the University network or to accomplish tasks or schedules.

viii. *For bespoke software, the ABS-CITS shall determine the availability of capacity in the community to develop such software, and where the capacity is not, or is partially available within, the ABS-CITS shall determine the framework for collaboration with a consultant or third party in a manner that clearly protects the University's interests.*

ix. *In the event of a request for a software upgrade, ABS-CITS shall determine the resources required for the upgrade and the associated financial implications, including human resource capacity, and advise on the feasibility of the request.*

x. *ABS-CITS shall keep and manage inventories of licensed servers, network devices, institutional end-user devices and the applications running on these devices.*

xi. ABS-CITS shall make adequate arrangements to ensure that all software installed on university devices are regularly updated to the latest version.

xii. ABS-CITS shall ensure that the University makes adequate budgetary provisions to sustain subscriptions to licensed software running on the University network and devices.

2.2.2 Right of Use-Software Licensing

i. All software installed on the University's ICT infrastructure and systems shall be licensed software, and the right of use shall be based on user authentication.

ii. Though a user might have been authenticated to access a service, the level of accessibility, privileges and functions shall be governed by user authorisation.

iii. All authenticated and authorised users shall be profiled based on user accounting.

iv. Approval of software licence agreements (including End User Licence Agreements/ EULAs) shall be done through university procurement procedures.

v. Purchase documentation (including executed contracts) relating to software shall be filed and retained in perpetuity to provide a historical record and evidence of prior licensing arrangements, including evidence of entitlement to current versions of software based on an upgrade programme or plan.

vi. Software licence certificates shall be retained in a secure environment with limited and managed access controls.

C.3 Backup, Disaster Recovery and Procedure

This section provides guidelines for the creation and retention of backups for the purpose of disaster recovery and business resumption consequent upon service disruption or downtime.

i. The backup strategy of the University ICT ecosystem shall be driven by the need to restore services within a reasonable amount of time with minimal loss of data.

ii. The ABS-CITS, the custodian of ICT infrastructure and services in the University, shall generate and keep multiple copies of backup.

iii. Backups of all records and software shall be generated and maintained such that computer operating systems and applications are fully recoverable.

iv. The frequency of backups shall be determined by the volatility of data, and the retention period shall be determined by the criticality or nature of the data.

v. A copy of a fully recoverable version of data or information shall be maintained both on-premises and on the cloud.

vi. Derived data should be backed up only if restoration is more efficient than recreation in the event of failure.

vii. All information accessed from workstations, laptops, or other portable devices shall be stored on networked file server drives to allow for backup.

viii. The ABS-CITS shall keep a record of backup documentation for ease of retrieval.

ix. Backup and recovery documentation must be reviewed and updated regularly to account for new technology, business changes, and application migration to alternative platforms.

x. The ABS-CITS shall ensure that the University invests appropriately in ICT backup infrastructure for disaster recovery.

xi. The University of Lagos shall not be liable for the restoration or restitution in instances where data loss arises from hardware failure caused by troubleshooting or diagnostic intervention arranged in a personal capacity.

xii. Recovery procedures must be tested on an annual basis.

C.4 Bandwidth Provisioning, Use and Network Connectivity

4.1 BANDWIDTH PROVISIONING AND USE

i. The University shall commit to providing adequate high-speed internet access for its business activities and ensuring that the bandwidth is sourced from the most competitive Internet Service Provider (ISP) with favourable terms and conditions.

ii. The University's bandwidth provision shall be dedicated to the University's core businesses and services (teaching, learning, research and development, administration, and governance) in alignment with the University's vision and mission statements.

iii. The bandwidth provisioned by the University shall be responsibly deployed and used by members of the University community.

iv. The ABS-CITS shall, on behalf of the University, track and maintain utilisation report for the purpose of bandwidth allocation, traffic assessment and control, and adequacy of bandwidth resources.

v. ABS-CITS shall maintain the right to block any traffic that contravenes the University ICT terms of use and other privileges.

vi. ABS-CITS shall maintain the right to give priority to one type of traffic over the other based on predefined rules.

vii. ABS-CITS shall maintain the right to enforce user authentication for using the Internet by assigning them accounts and keeping usage history logs to analyse user behaviour. Users will be responsible for all usage history registered in their accounts.

viii. Scheduled Officers at the ABS-CITS shall be empowered to use the proxy server to access the Internet for centralised bandwidth monitoring and management purposes.

4.2 Network Connectivity Guidelines

i. The University's network connectivity infrastructure, comprising Local Area Networks (LAN), Wide Area Networks (WAN), and general network assets (workstations, servers, switches, routers, printers, optical devices, scanners and

cameras, cables, and network wall outlets) at all campuses, shall be maintained in good condition at all times to ensure effective and efficient service delivery and continuity.

ii. Only University-owned or managed devices shall be permitted to be connected to the University network. At no point shall privately-owned or managed, contractor-owned or managed, or third-party-owned or managed devices be allowed on the University network without appropriate permission from ABS-CITS.

iii. At no time shall any device, without exception, not under the direct management and operation of ABS-CITS, be connected directly to the University WAN across the campuses.

iv. The UNILAG provides no service guarantee regarding its Public Network and reserves the right to revoke connectivity for any and all devices attached to the network at its sole discretion, without prior notice to or permission from any user or device owner.

v. The University wireless network access users are subject to the regulations guiding the wired network.

vi. ABS-CITS shall handle the onboarding of new members of the University community onto the University connectivity network upon the approval of a formal application from an intending user.

vii. At no time shall any user or person, irrespective of the status of affiliation to the University, connect, disconnect, install, uninstall, add, remove, or modify, in any manner, any University-owned or managed network asset, excluding clearly marked wired Public Network outlets.

C.5 Data Classification

The guidelines on data classification provide a framework for protecting University data or data held by the University in terms of confidentiality, integrity, and availability. This guideline covers all data captured, processed, or stored by the University and applies to all members of the University community.

i. There shall be a Data Protection Officer (DPO) for the University, in compliance with the Nigerian Data Protection and Regulation Act 2023), who shall be the compliance officer with regards to how the university handles and processes data within its ecosystem as stipulated in the NDPR Act.

ii. The classification of information shall be the responsibility of the DPO also known as the Information Custodian.

iii. Individual staff members shall be responsible for ensuring that the sensitive information they generate or are in the custody of is appropriately protected and marked with the appropriate classification as provided by the DPO.

iv. All existing University information shall belong to one of the classifications listed in this section, either as public, classified, confidential, restricted, or sensitive, and shall be appropriately so designated.

v. DPOs shall implement control measures according to the classification of the information.

vi. Any person found to have breached the provision of these guidelines shall be subjected to disciplinary measures as outlined in the conditions of service in the case of staff or Matriculation Oath when the provision(s) is/are breached by the student(s).

Note: All University records are subject to the Nigerian Freedom of Information Act (to the extent that making them public does not infringe on the NDPR Act) subject to compliance with the necessary conditions for accessing the records. Categorising information does not exclude it from the provisions of Freedom of Information or Data Protection legislation.

C.6 ICT Security

The University's ICT security guidelines seek to protect the University's ICT resources from accidental or malicious disclosure, modification, or destruction while preserving the University's commitment to open information sharing in compliance with the culture and practices of the higher education institution ecosystem.

i. This guideline shall conform to the general standard of information security principles of integrity, confidentiality and availability as enshrined in the ISO/IEC 27002:2005 (Information Technology - Security Techniques, Code of practice for Information Security Management).

ii. The University's network security guidelines enunciated in this section shall apply to all members of the University community and all others granted access to and use of the University's ICT resources. It applies to all ICT domains and sub-domains within the university and associated colleges to the extent of their access to and use of the University ICT resources.

iii. Individuals, Faculties, Schools, Departments, and Units tasked, as custodians, with creating and maintaining these assets shall be responsible for their protection, integrity, and availability and for implementing the appropriate controls and protocols to ensure that they are safe and free from potential security breaches.

iv. Custodians shall ensure that controls are in place to prevent unauthorised intrusions into systems and networks and detect any intrusion.

v. Custodians of assets shall ensure that administrative access protocols include provisions for alternative administrative access in the event that the primary access holder is incapacitated or otherwise unable to perform the required administrative activities.

vi. The custodian of University ICT assets shall endeavour to ensure that any activity that harms or poses a threat to the whole or part of the University ICT assets is promptly detected, identified, isolated, and mitigated.

vii. All network security incidents or threats to the University's ICT resources shall be promptly reported to the ABS-CITS.

viii. Users of University ICT resources shall not be excluded from the responsibility of making incident reports on observed or suspected security weaknesses or threats to the University's ICT resources.

ix. The University shall commit to maintaining robust ICT resources that can detect and disarm suspected threats or security breaches.

x. The Vice-Chancellor, through ABS-CITS, shall have overall responsibility for the University ICT security guidelines to protect UNILAG's assets.

xi. Third-party access to University ICT resources shall be governed by the responsibility to ensure that such access does not breach the integrity of the University network.

xii. The Director ABS-CITS shall ensure that these network security guidelines are constantly updated to keep up with trends in network security.

C.7 Digital and Network Access Control

This guideline on digital and network access control seeks to protect the University of Lagos's wired and wireless network from unauthorised access and usage while ensuring that bonafide members of the University community can utilise network services for legitimate purposes.

Individuals who connect computers, servers and other devices to the University network shall follow specific standards and protocols.

i. Anyone who uses the campus ICT resources shall have appropriate status (e.g. staff, faculty, current students, alumni, and guests) and must be properly authorised to access the university network.

ii. Users shall not engage in activities outside their access privileges. These include but are not limited to:

    a. Performing an act that negatively impacts the operation of computers, peripherals or networks or impedes someone else's ability to do their work. Tampering with any transmission medium or hardware device or

connecting any unauthorised device (such as a router, switch, hub, wireless access point, etc.) or computer to the University network.

b. Propagating a software virus or worm.

c. Damaging or destroying data owned by the University or anyone else

d. Modifying any disk or software directory provided by the University for any special use.

e. Performing an act that places an unnecessary load on a shared computer or University network.

f. Illegal file sharing.

g. Attempting to circumvent protection schemes for access to data or systems or otherwise uncover security loopholes.

iii. No member of the University community shall grant unauthorised access to computers, devices, software or data. This includes, but is not limited to:

a. Admitting someone into a restricted area/ facility

b. Revealing a password to any account, including one's own personal account, without permission.

c. Permitting the use of any account, including one's own personal account, in a way that allows unauthorised access to resources.

iv. The University ICT resources shall not be used to broadcast unauthorised or personal messages to large segments of the user community, such as:

a. Advertising campaigns for personal financial gain or political purposes.

b. Pranks and chain messages.

c. Announcements not approved for dissemination by this method.

v. Logs detailing Peer-to-Peer (P2P) traffic and usage on the University network shall be collected and analysed to support network administration and management.

vi. Logs shall contain Internet Protocol (IP) addresses involved in data transfer, direction of transfer (if retrievable), metadata of file (if retrievable), time, protocol used, and amount of data transferred.

vii. Logs shall not contain any personal identifying information and shall be archived for a reasonable length of time.

viii. Harvested logs may be used to investigate complaints or suspicious traffic patterns.

C.8 Digital Systems and Cloud Services

This section sets out the guidelines for evaluating the University's subscription to digital systems and cloud services (also known as "Cloud Computing" or "Cloud").

i. The University shall ensure that all relevant provisions (legal, ethical and industry standards), including cybersecurity conventions and data protection regulations, are complied with in the procurement, evaluation and use of all digital systems and cloud services.

ii. The Director, ABS-CITS shall be responsible for maintaining the University's subscription to digital systems and cloud services on behalf of the University and ensure that such subscription does not contravene any national or international convention on cloud services. In particular, consideration shall be accorded a possible requirement for a Data Protection Impact Assessment (DPIA) and Data Processing Agreement.

iii. The Director, ABS-CITS shall ensure that the subscriptions to digital systems and cloud services do not expose the University network and resources to unauthorised use of University data and information.

iv. Where data integration becomes necessary, the Director, ABS-CITS shall ensure that the derivable benefits shall not compromise the integrity of the University network and data taking into consideration the University network security and data protection guidelines.

v. The University's subscription to digital and cloud services shall be undertaken with the assurance that services can be restored in a timely manner in the event of network failure or disruption.

C.9 Remote Access

This section provides guidelines for connecting remotely to the University network from any host. This is designed to prevent or minimise the potential exposure of the University's network to damage or breach that may arise from the unauthorised use of University ICT resources, including confidential data, theft of intellectual property, corruption of critical University internal systems, and damage to the institution's public image.

i. This guideline covers existing and remote access implementations, including VPN, SSH, cable modems, and others.

ii. Authorised remote access to the University's networks shall be given to individuals and organisations based on requests submitted to the Director, ABS-CITS or his delegate who shall review such requests in relation to the security of university's ICT infrastructure and services.

iii. The authorised user shall ensure that the remote access privilege is not used by any other individual, entity, organisation or party; and where such incidence occurred, the authorised user shall bear responsibility for the consequences of misuse.

iv. Authorised users shall be required to be familiar with and comply with the university ICT infrastructure guidelines listed below.

   a. ICT network security

   b. Bandwidth use and network connectivity

   c. Mobile computing.

v. Routers for dedicated Integrated Services Digital Network (ISDN) lines configured for access to the University's network shall meet the minimum authentication requirements of CHAP (Challenge-Handshake Authentication Protocol).

vi. Reconfiguring a home user's equipment for the purpose of split-tunnelling or dual-homing is not permitted at any time.

vii. All devices connected to the University's network via remote access technologies shall use the most up-to-date anti-virus software.

viii. All devices connected to the University's network shall be running a supported, up-to-date operating system and shall be patched to the latest level.

ix. Organisations or individuals who wish to implement nonstandard Remote Access solutions to the University's network must obtain prior approval from the Director of ABS-CITS.

C.10 Mobile Computing

This guideline on mobile computing seeks to ensure that effective measures are in place to protect data when using mobile computing, communication, and storage devices.

i. This guideline shall apply to university employees, students, and third parties using mobile computing devices (Laptops, Tablets, etc.), mobile communication devices (mobile phones, smartphones, etc.), and mobile storage devices (e.g., External drives, encrypted USB memory sticks) to access University ICT resources.

ii. Users of mobile computing devices shall exercise caution when such devices are to be connected to the University network, ensuring that they are free from any malware (viruses, worms, Trojans) that infect the device and spread rapidly to other devices once connected to the network.

iii. The storage of sensitive personal data on USB is prohibited and same shall not be used to transfer personal data.

iv. Encryption software shall be installed on all mobile devices used to store or transfer University sensitive data.

v. All mobile devices shall have a password-protected keyboard or screen lock that automatically activates when the devices are not in use.

vi. Users shall ensure that when they are not at their desks for an extended period of time, the devices shall be physically secured.

vii. When travelling, users shall ensure that they keep the device in their possession at all times.

viii. Users of mobile computing devices shall not process personal or sensitive data in public places.

ix. Users' passwords for access to the University's network shall never be stored on mobile devices where they may be stolen or permit unauthorised access to information assets.

C.11 Password Guidelines

This section defines the base-level password requirements for accessing the University network resources and services.

i. This guideline shall apply to all accounts used to access the University ICT resources by staff, students, vendors and other third parties (collectively herein referred to as 'Users') who are authorised to access university's systems and information.

ii. These password requirements shall apply to all systems that have the facilities to accommodate them. Where systems do not have the facilities to accommodate the requirements set out in this guideline, alternative requirements, on a case-by-case basis, shall be under the guidance and approval of the Director, ABS-CITS.

iii. The password requirement guideline for accessing University ICT resources shall be based on multi-factor authentication (MFA), in which the first-level passwords shall have a minimum of eight characters, including numbers and special symbols.

iv. After three (3) unsuccessful login attempts, the account shall be locked until it is reset by the Director, ABS-CITS or his designated representative.

v. The initial passwords issued to a user shall be valid only for the first login session, and where the issued password is not used within twenty-four (24) hours after creation, such password shall become invalid.

vi. All University network devices (e.g., routers, firewalls, access control servers, etc.) shall have passwords or other access control mechanisms.

vii. All vendor-supplied default passwords shall be changed before any computer or communications system is used for university business operations.

viii. Passwords shall be promptly changed if they are suspected to have been compromised.

ix. Passwords shall not be sent by email or by regular post.

x. Passwords shall always be encrypted (non-clear text) when stored for any period (e.g., as backup media, batch files, automatic login scripts, software macros, etc.) or when transmitted over networks.

xi. If any part of the log-in sequence is incorrect, incorrect log-in information shall not be disclosed when logging into a university network resources or data communications system.

xii. Users shall not allow others to perform any activity with their user IDs. Similarly, users are forbidden from performing any activity with IDs belonging to other users.

C.12 Internet Domain Naming Conventions

This guideline defines the Standard for Internet Domain Name Registration for the University and its affiliated units (e.g. *unilag.edu.ng* is a domain name).

i. The word "UNILAG" shall appear in the domain names of all University of Lagos-related organisations (e.g. organisations based on campus and using the resources of the University).

ii. All sites being accessed on a *unilag.edu.ng* domain shall adhere to the university Web Hosting Policy.

C.13 ICT User Authentication

This section outlines guidelines and procedures for authenticating users accessing the University of Lagos's ICT resources. It shall apply to all users, including staff, students, and third-party contractors, who access University ICT systems, networks, data, and services.

i. All users shall be responsible for:
   a. Creating strong, unique passwords.
   b. Safeguarding their authentication credentials.
   c. Reporting any unauthorised access or suspicious activity.
   d. Participating in cybersecurity awareness training.

ii. The University shall permit users to authenticate access to the University network and ICT resources using a username and password. This may be completed with an MFA.

iii. Authentication with passwords shall comply with the requirements listed below.
   a. Contains a minimum of eight (8) characters.
   b. Contains a combination of upper- and lower-case letters, numbers, and special characters.
   c. Passwords must be changed every 90 days.
   d. Passwords shall not be reused within six (6) previous password changes.
   e. Accounts shall be locked out after three unsuccessful login attempts. Users can reset their passwords following the University's password reset procedures.

iv. User accounts shall be provisioned upon confirmation of their affiliation with the University. In the same vein, accounts shall be deactivated or removed upon separation or as determined by the University's Human Resource Management Directorate. However, staff and students may have their email privileges in perpetuity subject to responsible use or otherwise.

v. The University shall monitor and audit user authentication activities to detect and respond to potential security threats.

vi. In the event of threats related to user authentication, users shall be required to report the threats promptly.

C.14 Sustainable Funding For ICT Equipment and Infrastructure

This guideline establishes clear pathways and models for sustainably funding the provisioning and maintenance of ICT infrastructure and services at the University of Lagos.

i. The University shall commit to the sustainable funding of ICT equipment and infrastructure to support and sustain the University's drive to deploy ICT for University businesses and services.

ii. University ICT investments shall align with the strategic objectives of its mission statement as it concerns the University's academic and research focus; systematically supporting the advancement of teaching, learning, research, and administrative processes.

iii. The University shall be responsible for managing ICT resources efficiently and ensuring that funding is allocated judiciously to ensure optimal resource utilisation.

iv. The University shall continually explore a wide range of sources to provide financial investment for the modernisation and upgrade of the University's ICT infrastructure and services. Sustainable funding shall be pursued from:

a. Annual Budget: A certain percentage of the University's annual budget shall be dedicated to investing in its ICT infrastructure- including, possibly, through 'ring-fencing' ICT related income streams.

b. Grants and External Funding: The University shall seek donations and external funding to support specific ICT projects or initiatives that align with its strategic vision and mission.

c. Endowment Funds: Endowment funds dedicated to ICT investments shall be established to ensure a sustainable financial investment for enhancing ICT infrastructure and equipment.

d. Public-Private Partnerships: Where applicable and in the best interest of the University, the University shall explore public-private partnerships to fund and manage ICT infrastructure and services.

v. Risk assessment shall be conducted on the University's ICT infrastructure and services to inform funding decisions and risk mitigation strategies.

C.15 Quality Assurance, Control and Maintenance Management

This guideline outlines the principles and practices for Quality Assurance, Control, and Maintenance Management of IT infrastructure in the University.

i. The Directorate of ABS-CITS, shall implement procedures and protocols to ensure that University ICT resources and service delivery comply with the University Quality Assurance and Servicom guidelines.

ii. The Directorate of ABS-CITS, shall conduct regular risk assessments to identify vulnerabilities and threats to the University's ICT infrastructure and develop risk mitigation strategies and contingency plans.

iii. The Directorate of ABS-CITS shall ensure that the University ICT infrastructure complies with relevant laws and regulations.

iv. The University, through the directorate, shall implement monitoring tools to track the performance of critical systems and network infrastructure, set performance benchmarks and establish alerting mechanisms.

v. The University, through the directorate, shall implement strict access control measures for its ICT infrastructure, limiting access to authorised personnel only.

vi. The University shall establish a robust change management process to control and document all changes to the ICT infrastructure.

vii. The University shall employ up-to-date security measures such as firewalls, intrusion detection systems, and antivirus software to protect the University network from malicious attacks.

viii. The University, through the directorate, shall implement automated and regular data backups for disaster recovery.

ix. The University shall develop a preventive maintenance schedule for the University's ICT hardware, including servers, switches, and other critical equipment.

x. The University shall schedule routine software updates and patch management.

xi. The University shall maintain detailed documentation of its ICT infrastructure, including network diagrams, configurations, and asset inventories.

xii. The University shall establish strong vendor relationships to ensure prompt support and access to critical updates. The University shall review vendor contracts and service-level agreements.

xiii. The University shall commit to providing regular training for the University ICT staff on the latest technologies, security best practices, and compliance requirements.

xiv. University ICT staff shall be encouraged to pursue relevant certifications and professional development.

xv. The University shall create awareness among members of the University community about ICT security best practices and shall conduct awareness campaigns on phishing threats and data protection.

xvi. The University shall conduct periodic audits and reviews of the ICT infrastructure to identify areas for improvement.

xvii. The University shall establish an incident response plan to address ICT infrastructure emergencies.

xviii. The University shall encourage users to provide feedback on ICT infrastructure services and infrastructure, using the feedback to improve and enhance the user experience.

C.16 Acceptable Use Guidelines for ICT Services

Members of the University community should see access to the ICT facilities and resources provided by the University as a privilege that must be deployed and used lawfully, ethically and responsibly. Therefore, the guidelines on Acceptable Use of ICT services in the University provide sets of regulations governing the use of ICT hardware, software, virtual communication platforms, email services, and other ICT-related resources regardless of ownership.

i. The University shall make every reasonable effort to respect and protect individual privacy, including information guaranteed by the NDPR Act. However, members of the University community shall not acquire a right to privacy for communications transmitted or stored on the UNILAG's resources.

ii. Notwithstanding the provision of Section 16(i), the ABS-CITS, on behalf of the University, shall endeavour to exercise extreme caution to ensure that sensitive community members' information stored on the University ICT repository is protected and not vulnerable to malicious access.

iii. Any use that materially disrupts the University's day-to-day business activities shall be prohibited without an explicit exception.

iv. Personal use of University ICT resources for activities other than academics, research and development, administration, and governance shall be prohibited at all times.

v. Use of University ICT resources by non-University community members should be incidental and minimal.

vi. ICT Asset custodians must be able to demonstrate that critical business applications that include licensed software are identified and that the licence permits the use of that software at a different site, University location or computer, all of which may be operated by a third party either on the University's:

- Network
- Web
- End-user Devices (Units and Individuals).

vii. Following the same standards of common sense, courtesy, and civility but subject to the right of individuals to be free from intimidation, harassment, and unwarranted annoyance. All users of UNILAG's computing resources, whether via personally owned and/or UNILAG-owned and managed devices, shall adhere to the requirements enumerated below.

a. The University explicitly prohibits using any information system for fraudulent and/or illegal purposes. While using any of the University's ICT resources, no member of the University community shall engage in any illegal activity under local, state, federal, and/or international law.

b. No member of the University community using the University ICT resources shall violate the rights of any individual or company involving information protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of pirated or other software products that are not appropriately licensed for use by the University.

c. No member of the University community shall deploy the University ICT resources to violate, in any way, copyrighted material, including, but not limited to, photographs, books, music, software or other copyrighted resources for which the University does not have a legal licence.

d. No member of the University community using the University ICT resources shall export software, technical information, encryption software, or technology in violation of international or regional export control laws.

e. No member of the University community using the University ICT resources shall issue statements about warranties, expressed or implied, unless it is part of normal job duties or make fraudulent offers of products, items, and/or services.

f. Any member of the University community that suspects or is privy to the use of University ICT resources by an individual or group of individuals for any activity described in this section or any other activity they believe may be fraudulent or illegal must alert his or her immediate line manager.

g. If any member of the University community creates any liability to the University arising from inappropriate use of the University ICT resources, that member of the University community shall take full responsibility, indemnify and hold the University free and harmless.

viii. The University shall ensure that:

a. Transmitting or recording confidential information by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, audio recordings, etc.) is prohibited.

b. Writing or storing confidential information on mobile devices (phones, tablets, USB drives) and removable media shall be prohibited. Mobile devices that access confidential information will be physically secured when not in use and located to minimise the risk of unauthorised access.

c. Members of the University community and University-approved third-party service providers shall use approved workstations or devices to access University data, systems, or networks. Unapproved non-University-owned devices that store, process, transmit, or access confidential information are prohibited. Accessing, storing, or processing confidential information on home computers is prohibited.

d. All University-owned portable devices shall be securely maintained when in the possession of any member of the University community. Such devices shall be handled as carry-on (hand) baggage on public transport. They shall be concealed and/or locked when in private transport (e.g., locked in a secure area of an automobile) when not in use.

e. Photographic, video, audio, or other recording equipment will not be utilised in secure areas without specific exceptions addressing what is recorded and how recordings are to be performed from the UNILAG's information technology systems.

f. All confidential information stored on University workstations and mobile devices must be encrypted.

g. Members of the University community who use University-owned workstations shall take all reasonable precautions to protect the confidentiality, integrity and availability of information contained in the workstation.

h. Members of the University and affiliates who move electronic media or information systems containing confidential information are responsible for the subsequent use of such items and shall take all appropriate and reasonable actions to protect them against damage, theft, and unauthorised use.

i. Members of the University community shall ensure that they properly sign out and lock their end-user devices whenever they leave their workstations unattended or at the end of the close of business.

ix. The University ICT resources shall not be used to harass any other person via e-mail, telephone, or any other means or actively procure or transmit material that is in violation of sexual harassment or hostile workplace laws. Should any individual feel he/she is being harassed using the University's ICT resources, such shall report it to his/her immediate superior or otherwise in accordance with the UNILAG of Lagos Policy on Sexual Harassment or any other appropriate channel.

x. The University shall endeavour to deal with and respond to any threat or report of threat involving any aspect of the University ICT ecosystem, including but not limited to:

a. Loss, theft or inappropriate use of institution access credentials (e.g. passwords, key cards or security tokens), assets (e.g. laptops, cell phones), or other information shall be appropriately incident with the scheduled unit of the University, such ABS-CITS and the University's Security Unit.

b. No member of the University community shall prevent another member from reporting a security incident involving the university's ICT infrastructure and services.

xi. The use of the University's ICT resources for malicious activity against other users or members of the public is prohibited.

xii. No member of the University community shall prevent any other member of the University community from using the University ICT resources in the form of Denial of Service. Specifically, no individual or group of individuals shall:

a. Perpetrate, cause, or in any way enable disruption of the UNILAG's information systems or network communications by denial-of-service methods;

b. Consciously or deliberately introduce malicious programs, such as viruses, worms, and Trojan horses, to any information system; or intentionally develop or use programs to infiltrate a computer, computing system, or network and/or damage or alter the software components of a computer, computing system or network.

xiii. No member of the University community shall:

a. Perpetrate, cause, or in any way enable security breaches, including, but not limited to, accessing data of which the individual is not an intended recipient or logging into a server or account that the individual is not expressly authorised to access;

b. Facilitate use or access by non-authorized users, including sharing their password or other login credentials with anyone, including other users, family members, or friends. Additionally, all members of the University community shall take responsibility for the safekeep of access credentials.

c. Use the same password for the University accounts as for other non-University UNILAG access (for example, personal ISP account, social media, benefits, email, etc.);

d. Attempt to gain access to files and resources to which they have not been granted permission, whether or not such access is technically possible, including attempting to obtain, obtaining, and/or using another user's password; or

e. Make copies of another user's files without that user's knowledge and consent.

f. Ensure that all encryption keys employed by individuals are provided to Information Technology Services if requested in order to perform the functions required by this policy.

g. Base passwords on something that can be easily guessed or obtained using personal information (e.g. names, favourite sports teams, etc.).

xiv. No member of the University community shall:

a. Circumvent the individual authentication or security of any ICT system;

b. Add, remove, or modify any identifying network header information ("spoofing") or attempt to impersonate any person by using forged headers or other identifying information;

c. Create and/or use a proxy server of any kind other than those provided by the University or otherwise redirect network traffic outside of normal routing with authorisation or

d. Use any type of technology designed to mask, hide, or modify their identity or activities electronically.

xv. No member of the University community shall:

a. Use a port scanning tool targeting either UNILAG's network or any other external network, unless this activity is a part of the individual's normal job functions, such as an authorised ABS-CITS member (from the Networking Team, Software Development & E-Services (SD&E) Team, Web Team, or Hardware Team or Cyber Security Team), conducting a vulnerability scan, and faculty utilising tools in a controlled environment.

b. Use a network monitoring tool or perform any kind of network monitoring that will intercept data not intended for the individuals unless this activity is a part of the individual's normal job functions.

xvi. The University prohibits the use of institutional ICT resources for accessing or distributing content that other users may find objectionable. Individuals must not

post, upload, download, or display messages, photos, images, sound files, text files, video files, newsletters, or related materials considered to be:

- Serving a Political interest
- Racist
- Sexually-explicit
- Exciting, igniting or promoting violence

xvii. The University prohibits the use of unapproved hardware or unlicensed software. ABS-CITS shall maintain an up-to-date list of prohibited hardware and software types and impose sanctions when violation is detected. Further, it shall be the responsibility of 'asset owners' to manage their assets responsibly (may be) with possible expert support.

xviii. Members of the University community shall not:

a. Install, attach, connect, remove or disconnect hardware of any kind, including wireless access points, storage devices, and peripherals, to any institutional infrastructure or similar core network information systems without the knowledge and permission of the ABS-CITS.

b. Download, install, disable, remove or uninstall unlicensed software of any kind, including patches of existing software, to any institutional information system without the knowledge and permission of the University.

c. Use personal flash drives or other USB-based storage media on institutional facilities or infrastructure without prior approval from the ABS-CITS.

d. Use personal USB devices, if enabled, that have been used on other systems without first running a manual scan on the device to ensure it is free of malware or viruses.

e. Take any University ICT equipment off-site without prior authorisation.

xix. The ABS-CITS directorate shall track any software purchased or downloaded and retain this information for potential management and assessment needs.

xx. Members of the University community shall ensure that:

i. E-mail messaging facilities provided by the University through the ABS-CITS shall be used with care, ensuring that e-messaging protocols enshrined in the guidelines are complied with. In particular, members of the University community shall not send personal information, attempt to open files or follow links from an unknown or suspicious source, and should only use appropriate language in e-messaging. Email usage may be monitored and archived.

ii. No member of the University community shall use a non-institutional email account for email messaging over the University emailing infrastructure.

iii. There are legal risks associated with email messaging. Therefore, members of the University community shall demonstrate extreme caution when using the University e-messaging infrastructure ensuring that the University is free from any legal liabilities arising from using the e-messaging facility. This includes but is not limited to:

a. Sending emails with any libellous, defamatory, offensive, racist or obscene remarks.

b. Forwarding emails with any libellous, defamatory, offensive, racist, or obscene remarks.

c. Transmitting or forwarding confidential information;

d. Forwarding or copying messages without permission or implied permission.

e. Knowingly sending an attachment that contains a virus that severely affects another network or other users.

f. Forging or attempting to forge email messages.

g. Sending email messages using another person's or a bogus email account.

h. Copying or forwarding a message or attachment belonging to another user without the permission or implied permission of the originator.

i. Disguising or attempting to disguise user identity when sending an email.

iv. Additionally, members of the University community shall not:

j. Stream video, music, or other multimedia content unless the content is required to perform the individual's normal functions; particularly, if these activities negatively impact UNILAG's network performance.

k. Use the University's ICT resources to play games or provide similar entertainment.

l. Use the University's ICT resources for commercial use unless a specific exception is granted (e.g., CBT, University media services).

C.17 Enforcement and Penalty

i. The Director, Adetokunbo Babatunde Sofoluwe Centre for Information Technology and Systems, through designated personnel, shall have the responsibility of enforcing the guidelines in this document. The Director shall transmit the incident report to the Vice-Chancellor through the Management Board of ABS-CITS.

ii. The ABS-CITS shall be proactive in enforcement to ensure compliance with this policy, including surveillance commensurate with appropriate maintenance of the right to privacy.

iii. The University reserves the right to revoke network connectivity from any device or deny any user at any time at its sole discretion without prior notice if any portion of the University's terms of use of the network services is violated. In addition to any other disciplinary procedures, violator(s) may be subject to federal, state, or local law enforcement.

iv. Individuals who violate this policy may be denied access to institutional

resources and may be subject to disciplinary action in accordance with the extant provisions of the University of Lagos's conditions of service (staff) or student codes of conduct.

v. The accounts of such individuals may be temporarily suspended prior to the initiation or completion of disciplinary procedures when it is reasonably suspected that the integrity, security, or functionality of the University's ICT resources is threatened or to protect the University from liability.

vi. Material (software, hardware, or data) found to violate this policy shall be banned, confiscated, or otherwise eliminated from the University ICT ecosystem.

vii. Exceptions to the policy may be granted by the Vice-Chancellor or by his/ her designee. All exceptions shall be reviewed regularly.

PART D: ICT SERVICES

D.1 WEB HOSTING SERVICES

i. The University shall commit to the provision of effective and secure web services ensuring compliance with legal and regulatory requirements to support teaching, learning, research and development, administration and governance.

ii. These guidelines shall be applicable to all members of the university community comprising students, faculty, staff and affiliates.

iii. The web services covered by these guidelines shall include but not limited to
   a. University websites
   b. Web applications and databases
   c. Mobile apps
   d. APIs

iv. For the purpose of maintaining a reliable, secure and scalable web hosting service, the university shall commit to ensuring that server capacity is regularly expanded to accommodate growing needs of the university and that all hosted sites are secured with an active Secure Socket Layer (SSL) certificate.

v. The web hosting philosophy of the university shall be primarily based on *hosting on premise*. Third party cloud hosting services shall only be considered if in-house capacity is lacking, and in that situation, the decision on cloud hosting shall be assessed with respect to sustainability of financial investment. In this wise, a combination of hosting strategies comprising:
   a. Shared hosting
   b. Virtual private server (VPS) hosting
   c. Dedicated hosting
   d. Cloud hosting; shall be explored.

vi. Website development in the university shall be based on a template approved by the directorate of ABS-CITS which at the moment, except otherwise stated, shall be based on WordPress. All units of the university shall commit to adopting this template or any other approved template for their website development.

vii. The ABS-CITS shall be solely responsible for all issues relating to website development and hosting. Third-party engagement for website development and hosting by any unit in the university shall be in consultation with the ABS-CITS.

viii. Any website outsourced in violation of the provision of Section D.1(vii) shall lose the privilege of being hosted on the university server, except the website is donor-financed and even at that, the approval of the Director, ABS-CITS shall be necessary.

ix. The design and feel of the university website shall comply with a standard format including logo, size and fonts.

x. The ABS-CITS shall keep and maintain a register of all websites in the university and regularly subject them to vulnerability and penetration test (VAPT).

xi. It shall be the responsibility of faculties, departments and units to administer content and maintain their website while ABS-CITS provide support services within its mandates to ensure that all websites hosted on the university server are live and active. The ABS-CITS shall not take responsibility for violation of the terms of use of the university web hosting services.

xii. Websites hosted on the university server shall not be used for political or any other purposes contrary to the promotion of teaching, learning, research and development, administration, and governance.

xiii. The university shall commit to the establishment of a disaster recovery mechanism such as installation of mirror servers for all websites and external storage for both on and off-site data back-up.

xiv. There shall be no illegal, unethical, malicious, not duly authorized copyrighted and proprietary contents on any website hosted on the university server.

xv. The university shall own all websites hosted on its server while content creators retain the ownership of their contents or submissions.

xvi. The University shall commit to protecting web-user data and maintaining confidentiality.

xvii. Violation of any section of these guidelines shall be treated in accordance to the extant provisions on acceptable terms of usage.

D.2 E-ADMINISTRATION AND VIRTUAL ASSESSMENT

The University as part of the wider digital transformation initiative seeks to deploy e-administration solutions for its day-to-day administrative activities to engender improved service delivery by facilitating prompt and secure dissemination of information and execution of assigned tasks within and across units in the University as well as engagements with external stakeholders. Thus, the University of Lagos e-Administration Policy provides the guidelines for the design, implementation, management and deployment of e-administration solutions for the purposes of digitally integrating the administrative flow of various units into a cohesive flow for the delivery of university processes and services including engagements with external stakeholders.

i. Scope: this policy shall apply to all staff of the university, students and other stakeholders including service providers, vendors, and partners who have the need to interact or partner with the university. For employees of the university, the coverage of the policy shall extend to all units identified and recognised in the university organogram particularly the chancellery, registry, bursary and other support units; whereas for students and other stakeholders, it shall be to the extent as would be necessary for them to be adequately served. In specifics, it shall accommodate the deployment of digital technology to enable virtual assessments for academic purposes vis-à-vis interviews and examinations. This is without prejudice to the university's preference for physical and onsite assessments for recruitments and promotions in the case of staff, and examinations in the case of students.

ii. Objectives: the e-administration policy of the University seeks to foster prompt dissemination and implementation of administrative communication, ensuring efficiency, improved productivity, shorter turn-round time, operational cost saving and supports sustainability by minimizing environmental impacts of paper-based administrative processes. Additionally, it seeks to permit the deployment of digital technology for screening, interview and assessment for recruitment and promotion. In specifics, the policy seeks to:

a. Streamline and automate administrative workflow, eliminating manual and paper-based processes, and weak points resulting in improved administrative communication and decision making.

b. Ensure rapid transition to a connected workspace in which exchange of information amongst university leadership, staff, students and external stakeholders is seamless and accessible irrespective of distance and time.

c. Emplace transparency and accountability in administrative processes by providing real-time access to data and status of assigned tasks.

d. Support data-driven decision making by providing access to real-time reliable data and information.

e. Ensure security and confidentiality of digital records to protect confidential information.

iii. The University e-administration infrastructure shall be organically driven by an Enterprise Resource Planning (ERP) solution capable of integrating distinct units of the university as a single enterprise, permitting seamless interaction and exchange of administrative responsibilities amongst the various units.

iv. The e-administration infrastructure of the University shall be deployed to design plan, and implement recruitment and job responsibilities, employee leave entitlement and performance appraisal system, automation of attendance, communication with and notices to staff such as e-circulars, orders, facility booking and usage map, appointment scheduling, and others.

v. The digital infrastructure of the university shall be deployed to accommodate virtual assessment for academic purposes for the screening, recruitment and promotion of staff without prejudice to the university's preference for physical and onsite assessment. The philosophy underpinning the deployment of university's digital infrastructure for virtual assessment shall be to:

a. Promote Equity and Access. This shall reduce barriers to participation for candidates facing logistics or financial constraints. This ensures that candidates are exposed to the same condition, the same quality of interviewers as long as they are in the same discipline.

b. Strengthen Interview Quality. This shall ensure thorough assessment of candidates' skills, experience, and suitability for the position.

c. Enhance Institutional Resources: This shall promote investment in technology, infrastructure and personnel to sustain virtual assessment.

d. Fairness and Consistency: This shall ensure that candidates are evaluated using consistent and fair process, regardless of the interview format.

e. Transparency and Documentation: The deployment of virtual assessment model shall ensure that proceedings are recorded as part of documentary evidence by the Human Resources Management Directorate.

vi. Eligibility for virtual assessments shall be governed by the following criteria:

a. **For Staff Interview**

a) Existing staff-Teaching and Non-Teaching Staff

i. Those on officially approved exchange programmes, internship or research leaves abroad.

ii. Those who for reasons of health, travel or visa restrictions or whatever officially approved reasons cannot physically attend an interview.

iii. Members of staff at professorial cadre or promotion to CONTISS 13 and above who are on approved leave outside the country.

b) For New Staff Recruitment: Virtual assessment shall be permitted for only new applicants not resident in Nigeria.

b. **For Assessors:** Virtual assessment can be deployed when international assessors cannot appear in person for any reason

c. **For Students**

i. **Ph.D. APC and Final Defence:** Virtual assessment can be permitted where students are abroad with official permissions, and conditions set by the School of Postgraduate Studies are met with proper documentations provided all required courseworks and

seminars were done physically.

ii. **Masters Viva**: Students in this category can benefit from virtual assessment where they have travelled out with approval with proper documentation.

iii. **Undergraduates**: Undergraduate students who are on officially approved exchange programmes or are ill on hospital admission can be assessed virtually.

vii. The University e-administration infrastructure shall be under the custodian of the directorate of ABS-CITS for operation and maintenance, whilst the various units of the University shall be assigned privileges as determined by the university organogram, roles and responsibilities.

viii. Authorised users on the university's e-administration infrastructure shall be granted access based on their roles and responsibilities.

ix. Data stored on and processed through the e-administration infrastructure shall not infringe NDPR Act or any other regulations dealing with accessing and processing of personal or confidential information. Misuse or unauthorised access to the University's e-administration shall be considered a serious infraction and shall be subject to appropriate disciplinary procedure as specified in relevant regulations for either staff or students.

x. It shall be the responsibility of every staff to report to the appropriate authority any observed misuse of the university e-administration infrastructure.

xi. Students' or external stakeholders' access to the e-administration infrastructure shall be in line with guidelines on acceptable use of university ICT infrastructure and services by students and external stakeholders.

xii. The e-administration infrastructure architecture for the university shall incorporate a feedback mechanism to harvest users' experience, evaluate e-administration solutions to ensure that infrastructure aligns with the dynamic needs of the university.

D.3 E-LEARNING AND DIGITAL RESOURCES

This section provides guidelines on the deployment, management and use of the University's e-learning and digital resources.

i. The University shall commit to deploying e-learning infrastructure, applications, and solutions to facilitate teaching, learning, research, and assessment across all its programmes (certificates, diplomas, undergraduate and postgraduate) including enabling e-thesis assessment.

ii. There shall be a digital teaching and learning centre at the ABS-CITS directorate that shall coordinate the digital teaching and learning resources for the University.

iii. Staff and students shall undergo necessary capacity building to ensure ability to efficiently and effectively use the e-learning and digital resources competently.

iv. The adoption of e-learning infrastructure for assessment via CBT examination shall be limited to courses in 100 and 200 levels. Such infrastructure shall not be extended to the examination of courses in the higher levels.

v. The University shall implement and maintain a robust and secure e-Thesis adjudication platform to facilitate prompt thesis assessment in alignment with the University's vision and mission.

vi. E-learning and digital resources shall not be used in a manner that does not support academic and research activities at the University of Lagos.

vii. Academic staff shall be responsible for making necessary academic resources available on the e-learning and digital resources in compliance with academic best practices.

viii. All users of the university's e-learning infrastructure and solution shall ensure that any piece of content uploaded to e-learning and digital resources does not infringe any copyright privilege or is free from any sustainable charge of plagiarism.

ix. Students of all categories shall commit to ethical and responsible use of the University e-learning and digital resources.

x. The ABS-CITS directorate shall be responsible for maintaining the technical infrastructure required for e-learning and digital resources, including user support

services, server maintenance, and security.

xi. The ABS-CITS shall ensure data security and protection of personal information and encryption of enrollees' records on the resources.

xii. The DVC (A&R) shall ensure that development and onboarding of digital resources shall meet high standards.

xiii. The University shall regularly evaluate the effectiveness of the e-learning and digital resources.

xiv. Any breach of the e-learning and digital resources guidelines shall be treated according to the Terms of Use provisions.

D.4 HARDWARE AND DEVICES REPAIR

This section provides guidance in the acquisition and repair of hardware and devices (computer systems, scanning and photocopying machines, cameras, projectors and multi-media systems, screens, Public Address Systems, including digital plug-in devices) and their usage for teaching, learning, research, and administrative activities.

i. The ABS-CITS, on behalf of the University, shall compile and maintain a specification register/database to guide the acquisition of hardware and other digital devices in the University.

ii. ABS-CITS shall be responsible for regularly updating the register and communicating it to various university units to promote awareness and compliance.

iii. No unit in the University shall procure hardware or any other digital device not captured in the register or whose specifications do not conform to the guidance in the register. In situations where such hardware or devices are not accommodated in the Register, the procuring unit shall seek the ABS-CITS's advice before proceeding with the procurement.

iv. A breach of the provision of Section D.4 (iii) shall amount to an infringement of the procurement guidelines outlined in this policy and shall be treated as such.

v. The University's hardware, devices, and related digital assets shall be deployed for the purpose of teaching, learning, research and development, administration, and governance in alignment with the University's vision and mission statements.

vi. The ABS-CITS shall ensure that these assets are used according to the terms and conditions specified by the Original Equipment Manufacturer (OEM).

vii. The ABS-CITS shall ensure that the hardware and device assets of the University are always in top-notch condition to facilitate University businesses and services.

viii. No unit shall contract any third-party consultant for troubleshooting or repairing any out-of-service hardware or device. This shall be the sole responsibility of the ABS-CITS. In such situations, where the ABS-CITS's in-house capacity is inadequate, the directorate shall determine the framework for contracting a third-party service provider.

D.5 E-MAIL MESSAGING AND COMMUNICATION OVER THE UNIVERSITY MAIL SERVERS AND INFRASTRUCTURE

The guidelines in this section set out the terms and conditions for the use of University email services and communication over the University internet infrastructure, including the protocols for managing created and received messages in support of University businesses and services. The University currently runs two email mail client servers: Google Workspace station (Education), which is strictly for staff and Microsoft 365 Live for both staff and students.

i. The University shall provide all staff with either Google Workspace (Education) or a Microsoft 365 live account for the duration of their employment or a Microsoft 365 live account for students during the duration of their studentship. After this time, the email accounts and associated services shall be retired from use and deleted six (months) after exit; except the university decides otherwise.

ii. ABS-CITS, on behalf of the University, shall be the domain administrator for both Google and Microsoft facilities and administer all email accounts in accordance with its Data Protection and responsible use policy.

iii. Email accounts shall be automatically created for all University staff and students in the employment of or studying in the University. For staff, it shall be created once the Human Resource Management Directorate communicates to the Director, ABS-CITS or a staff member, through the endorsement of the Unit Head,

requests for a University email account. For students, it shall be automatically created after successful admission screenings. Unit emails shall be created to ensure a dedicated account for general departmental communications rather than using employee accounts. Also, special email accounts may be created for any of the under-listed for a short time so they can use the University ICT infrastructure, subject to the approval of the Director, ABS-CITS.

a. Adjuncts/visiting lecturer
b. Postdoctoral fellows
c. Exchange students/staff
d. Conference/workshop/colloquium
e. Governing Council members
f. Special events

iv. The University's email facility shall be deployed to support learning, teaching, research, administration, and governance in alignment with the University's vision and mission statements.

v. It shall be the responsibility of all members of the University community to ensure safe, responsible and ethical use of the University's email facility. Users shall ensure that under no circumstance is the University's email facility deployed to defame, harass and infringe copyright and data protection regulations. Any misuse of the facility shall cause the invocation of a formal disciplinary procedure as stated in the applicable code of conduct for staff or matriculation oath for students.

vi. Users of the University email facility shall take responsibility for ensuring that their access credentials are free from unauthorised use, as they shall be held responsible for the consequences of unauthorised access.

vii. The University shall not be liable for improper use of the University email facility.

viii. The use of email services shall comply with regulations applicable to other forms of communication at the University.

ix. All email communications over the University mail server shall be subject to Data Protection and Freedom of Information legislation and may be legally admissible

in certain situations as applicable in other University policies, such as the sexual harassment policy.

x. Members shall ensure full compliance with corporate protocols when creating email signatures for the purpose of maintaining a consistent and professional image for the University.

xi. Staff shall properly set up an "out-of-office" email message with alternative contact details whenever they are absent from their desks to ensure that enquiries are promptly attended to within a reasonable timeframe.

xii. Users, if their roles permit, shall avail a colleague delegated access to their email accounts so that messages can be accessed and acted upon if that staff is not available for whatever reason. Under such conditions, the period of the delegated/transferred access shall be recorded and communicated well, and the staff shall immediately change the access credentials upon return.

xiii. Users shall regularly review their emails and ensure that those that have served their purposes are deleted from the system. This will ensure that users' email storage capacity is not exhausted.

xiv. Emails constitute legal digital records of the University and shall be managed as efficiently as paper and other electronic records of the University.

xv. Staff and students shall not use non-institutional emails on University systems.

xvi. When a scheduled staff member is transferred to another unit or exits the system, it shall be the responsibility of such staff member to ensure that his/her message privileges are transferred appropriately to colleagues or retained in the system with full disclosure of access information.

xvii. Although the University e-mail servers automatically scan messages for viruses and spam. Account holders shall yet take additional measures to prevent the introduction and transmission of computer viruses onto the University mail client server by ensuring that:

a. Attachments from unsolicited or untrusted sources are not opened.

b. Virus-infected attachments are not transmitted or forwarded.

c. Antivirus/anti-spyware software is installed and maintained on the devices they use to gain access to the University's IT infrastructure.

xviii. Unauthorised interception of, or access to, the email messages of other members of the University community, other than as part of a formal monitoring process, shall be an infringement under this provision, and such infringements shall be subject to the University policy on acceptable use.

xix. Incidental personal use may be permissible provided it does not consume extensive resources, does not interfere with productivity, is not for private business activities and does not involve any illegal or unethical activities.

xx. Users of University email services shall exercise extreme caution when using Internet services to transmit confidential or sensitive information. While the University shall do its utmost to ensure privacy, users of the facilities are advised to be aware of the possibility that electronic communications might be intercepted, copied, forwarded, printed, or stored by others. Particular care should be taken when submitting card details and transacting over the University's internet infrastructure.

xxi. Each user shall be responsible for the content and use of their own account. Passwords should not be shared with others and should be maintained in accordance with the University password policy.

xxii. Access to the Internet is provided via a proxy server. In exceptional circumstances, direct access may be required. Applications for direct access should be submitted to the Director, ABS-CITS, for approval.

xxiii. Users of University email services shall ensure they exercise extreme caution to avoid breach of copyright or of other intellectual property rights and that the use of the services conforms to all relevant policies and procedures, including, but not limited to, the University general ICT policy.

xxiv. Where there is a genuine need to access websites that would normally be considered to be inappropriate, for example, for particular research, teaching or

learning activities, the authorisation of the Dean/Head of Department/Units shall be required and the Director, ABS-CITS afterwards appropriately informed.

xxv. Users accessing University email services via mobile devices shall ensure that appropriate security settings are configured on the device and conform to the University's ICT policy on mobile computing devices.

xxvi. The University cannot guarantee that users of the computer facilities will be protected from receiving material that may be offensive to them.

D.6 CORE ICT SERVICES AND SERVICE LEVEL AGREEMENT

i. This Core ICT Service Level Agreement (SLA) guideline shall outline the terms and conditions governing the provision of any core ICT service or any other ICT service by any third party to the University of Lagos.

ii. Core ICT services in this policy shall refer to:

   a. Bandwidth provisioning for internet connectivity
   b. Enterprise Resource Planning applications
   c. Payment Gateway
   d. Biometric solution and surveillance services

iii. It shall ensure that services provided by a third party are those for which in-house capacities are not or partially available. In the latter case, contractual engagements shall be on the basis of co-creation.

iv. The SLA shall ensure that the terms of the agreement are not injurious to the University's interests in terms of quality of service, its sustenance, and value for investment.

v. SLA on ICT services with any third-party service provider shall be coordinated by the Director, ABS-CITS, on behalf of the University in conjunction with the Head, Legal Unit of the University.

vi. The SLA, regardless of other conditions that may arise in the future or with any particular ICT service, shall contain the elements listed below.

   a. Scope of service and the associated conditions

b. Date and time of the commencement day of the ICT service(s) and expiration.

c. Service Hours indicating days and hours when ICT services shall be available

d. Commitment to maintaining a minimum ICT service availability of 99% during normal service hours.

e. Commitment to the following response times for reported issues:

   i. Priority 1: Critical Issues shall be resolved within 24 hours

   ii. Priority 2: High-priority issues shall be resolved within 8 hours

   iii. Priority 3: Medium-priority Issues shall be resolved within 2 hours

   iv. Priority 4: Low-priority issues shall be resolved within the hour

f. Commitment to emergency support on a 24/7 basis to address emergency issues.

g. Commitment to providing the source code and building capacity, particularly in a co-created ICT service.

h. Operating contact of the service provider comprising street address, email address and telephone numbers.

vii. In the event that a service provided by a third-party service provider is not available, an incident report shall be raised to the Director, ABS-CITS, for his attention. Should the in-house personnel be unable to resolve the incident, then the Director shall contact the service provider for resolution.

viii. Should the service provider be unable to resolve the issue within a reasonable time, it shall provide an update to the University through the Director, ABS-CITS.

ix. The SLA shall clearly state a maintenance schedule, the service(s) to be affected, and the period of disruption.

x. Except in emergency maintenance situations, failure to conduct any scheduled maintenance by the service provider shall amount to a breach of the terms of the SLA.

xi. The service provider shall commit to providing periodic performance reports, such as monthly performance reports.

xii. SLA shall have a validity period of not more than a year except in a very peculiar scenario in which a validity period of a year would not be practicable, and in such a situation, the SLA shall not exceed three years.

xiii. The SLA shall provide a framework for terminating contractual agreements between the University and any third-party service provider.

Part E: Artificial Intelligence, Large Language Models and Other Emerging Digital Technologies

Artificial Intelligence represents a key transformative tool that is disrupting the traditional business and service delivery in the higher education institution ecosystem, and the University of Lagos, being a member of the ecosystem, would be affected by the effect of AI and its related technologies on university processes, businesses and services. With regard to this understanding, these guidelines are outlined to provide a framework for the adoption of AI and its affiliated technologies for teaching, learning, research and development, administration and governance at the University of Lagos.

i. The University shall explore the use of AI and its related technologies to the extent that it enhances university processes, businesses and services in alignment with University's vision and mission statements.

ii. The University shall commit to constantly enhancing the capacity of members of the University to keep pace with the development of AI tools via regular capacity-building workshops and training opportunities.

iii. The University shall commit to the safe, responsible, and ethical use of generative AI and other digital intelligence tools to support teaching, learning, research and development, administration, and governance.

iv. Any member of the University exploring AI and its related tools shall comply with the university's other relevant guidelines on ICT resources and services and shall be solely responsible for the outcome of the tool used without any liability, either directly or implied, to the University. Such individuals or group of individuals may be required to sign a consent declaration indemnifying the University against any liability.

v. Any data entered into AI tools shall comply with the requirements of the data

protection policy, ensuring the protection of personal, copyrighted and confidential information. This applies to academic content, research, service works and creative expressions.

vi. Members of the University community using AI tools and its resources shall exhibit transparency and make attributions to the usage of AI tools.

vii. While demanding general compliance with University guidelines on the use of AI tools, the University shall permit academic staff to have the discretion to allow the use of AI tools of various types in their courses, but with clear guidelines on rules of engagement.

viii. The University shall constantly update and make available to members of the University community (faculty, staff and students) guidelines on interaction with AI and all its derivatives.

ix. The University shall equip and support staff and students to use generative AI tools effectively and appropriately in their work and learning process to improve capacity and productivity while not sacrificing academic rigour, integrity, standard and mental exertion.

x. At appropriate time, the University shall permit the integration of AI applications in assessment where this would enhance students learning; and in such circumstance, assessment shall be designed to ensure that integrity and standards are maintained without sacrificing the originality of assessment and pedagogic practice.

xi. The AI shall be deployed in the University as supplementary tools to assists faculty in their academics and continuously enhancing holistic competencies rather than as replacements for human interaction and collaborations.

xii. Lecturers who have chosen to permit the use of AI tools in their courses shall ensure that students are reminded that representing work not done by them as their own, including work generated or AI-modified material, constitutes academic misconduct and shall be liable to face the student misconduct panel.

xiii. Students using AI tools shall commit to abiding by the guidelines, including institutional prohibitions as may be enacted from time to time by the appropriate overseeing authority such as the Deans of faculties, Heads of Departments, faculty members, or supervisors in the case of research works.

xiv. The use of AI tools in academic work shall be limited to harvesting research ideas, brainstorming, and editorial assistance, excluding text generation tools for all categories of members of the University community.

xv. Any use of AI tools in research, scholarship, or any related work affiliated to the University of Lagos shall be clearly documented, acknowledged and cited.

xvi. The Use of University information with any AI tools shall follow the regular guidelines on accessing university data as stated in the relevant guidelines on data classification.

Part F: Ict Communication, Engagement, Operational Manual and Career Structure

Compliance with the provisions of the ICT guidelines rests on the communication and sensitisation of the University community. Otherwise, the provisions would not be internalised, which could expose the University to a wide range of breaches of its ICT infrastructure and services, with no one taking responsibility for non-compliance. Hence, this section of the ICT policy provides guidelines for engaging and creating awareness for

F.1 ICT COMMUNICATION, SENSITIZATION AND ENGAGEMENT

the internalisation of the provision of the ICT policy. Additionally, the operational manual and career structure are accommodated in this section.

i. The University shall ensure that members of the University community are aware of and internalise the policy's provisions regarding service provision, governance and administration, and users' usage and responsibility. This shall include regular communication and engagement sessions via various channels, bulletins, email notifications, montage (short videos), workshops, etc.

ii. The University, through the ABS-CITS directorate, shall conduct regular capacity training to ensure that members of the University community develop the necessary proficiency and competence to use digital resources to perform their tasks and duties.

iii. ABS-CITS shall be responsible for sensitising the University community to updates on the relevant provisions of the ICT policy, new service provisioning, service

downtown, and any other status on the University ICT infrastructure and services that may impugn the performance of their duties.

iv. As part of its mandate to deepen ICT digital literacy, awareness, and deployment in the University, ABS-CITS shall commit to and be responsible for organising the annual World Telecommunication and Information Society Day (WTISD), known as World IT Day, on May 17 every year. The theme will clearly combine the University's ICT strategy with that of the World Telecommunication and Information Society.

v. The ABS-CITS shall compile Frequently Asked Questions (FAQs) to facilitate the troubleshooting and resolution of common challenges members of the University community encounter interacting with University ICT resources and services.

F.2 OPERATION MANUAL

i. The ABS-CITS, as the hub for ICT services in the University, shall have an operation manual containing basic information about the directorate, the organogram, mandates, the various units and their standard operation protocols.

ii. The manual shall be guided by the provisions of the ICT guidelines in terms of service provisioning and reporting line as enshrined in Part B, Section 2.0 of this policy.

iii. The Admin Unit in the ABS-CITS shall be headed by an officer of not less than a Deputy Registrar who shall provide administrative support to the Director.

iv. No technical unit in the directorate shall be headed in a substantive capacity, by a staff below Chief System Analyst/Administrator/Programmer/IT Equipment Maintenance Engineer or equivalent, and where there is more than one on that cadre in the unit, the more/most senior shall be considered and shall not be head of the unit for more than three years per tenure.

v. The operational manual shall be regularly updated to reflect changes and developments in the University's ICT strategy and the IT world.

F.3 CAREER STRUCTURE

i. The ICT directorate shall have a well-delineated career structure that aligns with the conditions of service for technologists/technical staff at the University.

ii. The career structure, in addition to specifying qualifications and experience requirements for each cadre, shall contain the job description and demonstrable skills applicable to each cadre.

iii. The career structure shall make provisions for cadres such as IT volunteers and interns, who shall not ordinarily earn a salary, but shall be provided the opportunity to acquire hands-on experience and upscale their ICT skills while adding to the available ICT hands in the University.

iv. Such volunteers or interns may be hired should the opportunity arise regarding their service to the University.

v. The career structure shall be updated in line with changes in the University's ICT strategies and goals.

Part G: Reviewing the Policy

There are two situations that may warrant a review of this policy. One is an isolated piecemeal review of specific sections or a number of sections in the policy document. The other shall be a comprehensive review, which shall apply to the whole policy document. In either of these situations, the review shall be undertaken as follows:

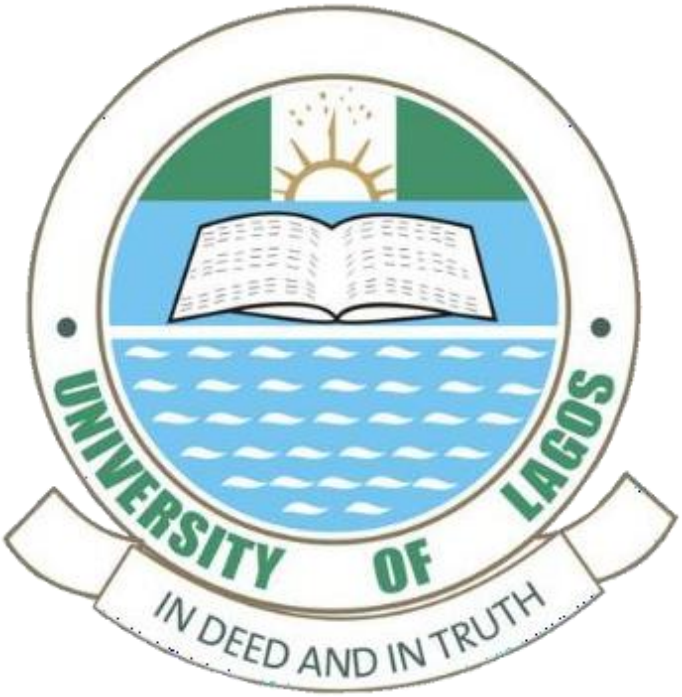
i. An isolated piecemeal review of a section or a number of sections of the policy may become necessary, arising from rapid development in the ICT landscape and international regulations, which is not accommodated in the current policy document. This shall be undertaken as soon as it is materially feasible.

ii. Otherwise, a wholesome review of this policy shall be due every three years, subject to the likelihood that a non-review constitutes a potential risk to ICT governance, administration, and management in the University, including the commitment to safe, responsible, and ethical deployment of ICT infrastructure and services.

University of Lagos

Akoka, Lagos, Nigeria

This policy document is subject to periodic review to reflect changes in technology, institutional needs, and regulatory requirements. The Adetokunbo Babatunde Sofoluwe Centre for Information Technology and Systems is responsible for its maintenance and updates.


UNIVERSITY OF LAGOS
IN DEED AND IN TRUTH