UNIVERSITY OF LAGOS

AKOKA

ICT POLICY

April 2019

1. INTRODUCTION

It is the vision of record of the University of Lagos (UNILAG), "*To be a top-class institution for the pursuit of excellence in knowledge, character, and service to humanity"* and informed by this vision, the University's mission is *"To provide a conducive environment for teaching, learning, research and development, where staff and students will interact and compete effectively with their counterparts globally"*

In furtherance of the strategic objectives implicit in these statements of vision and mission, the university, in 2001, established a Directorate of Centre for Information Technology and Systems (CITS) for the purposes of leveraging the possibilities offered by the Information Communication Technologies (ICT) towards systematically supporting her core business processes for efficient services delivery. And drawing from experiences accruing from over a decade of the CITS' operations, UNILAG has adopted and formalized an ICT policy, which, complemented by other relevant university policies, will guide and set standards for the acquisition, deployment and use of the ICTs, as well as define a path for the evolution of the CITS

1.1. PURPOSE OF ICT POLICY

The objectives of the ICT policy includes the following:

❍ set forth guidelines for a systematic development of a ubiquitous, resilient, reliable, and secure ICT infrastructure to support all university business processes, in a manner consistent with her vision and mission statements;

❍ define the essential supporting structure for the provision and management of ICT network services to guarantee equitable, reliable, secure, and economically efficient access to ICT resources by staff and students;

❍ establish consistent principles and procedures for the acquisition (or development, as may be expedient) of software and hardware information systems for use with university business

❍ provide a comprehensive set of security requirements for the entire extent of the university's network infrastructure

❍ specify best practices for the prudent use of the university's internet and intranet facilities and resources and access control policy to the university network

❍ safeguard the university’s integrity, image and reputation by prescribing guidelines and standards designed to ensure that the contents of the university’s website are accurate, up-to-date, consistent, and reflect UNILAG’s vision and mission.

❍ define the responsibilities of the CITS as a support and innovation center with the statutory mandate of enhancing the ability of users and ICT asset owners to make optimum use of services and resources

❍ provide a flexible template for the establishment of a sustainable UNILAG ‘*DEVELOPERS THINK-THANK’*, with the assignment of supporting the development, adaptation and customization of applications software and hardware for use with university business.

❍ provide conditions under which consultants, contractors, and providers of ICT goods and services may be engaged, and prescribe general terms and conditions for such engagements

1.2. SCOPE

This policy applies to students, staff, and associates of the University of Lagos (as defined by the University of Lagos Governing council), including persons (such as consultants, contractors, and representatives of organizations) with access to the university’s ICT resources or engaged with the development, implementation, and using ICT-based information, devices, and platforms owned, managed, operated or supported by the UNILAG.

2. DATA COMMUNICATION INFRASTRUCTURE MANAGEMENT AND DEVELOPMENT POLICY

2.1. INTRODUCTION

In general, data communication infrastructure may be regarded as consisting of the data communication network, the data center or network operating center, and ICT resources for end-users. These combine to link users of digitized information to the sources of the desired information items. At the University of Lagos, the data communication infrastructure has evolved over time to include a complex network that facilitates ICT support for educational content delivery, research activities, and other university businesses and processes. Network functions extend over considerations concerning the development of ICT infrastructure, campus Local Area Network/Wireless Local Area Network (LAN/WLAN), access to ICT facilities and resources, and monitoring of network performance.

2.2. OBJECTIVES

It is the objective of this policy to provide a detailed network development and management policy to guide the operational and management needs of the University's ICT infrastructure. The policy's provisions specify guidelines and responsibilities for activities of interest to developing, managing, installing, monitoring, and maintaining UNILAG's ICT network, such that the network remains reliable, resilient, and available at all times to offer support for university business and processes continuously.

2.3. GENERAL PROVISIONS

2.3.1. The Network

The University of Lagos, as a matter of policy, will continue to develop, support, manage, and operate a university-wide ICT network as a basic infrastructural service for purposes of facilitating access to, and sharing of ICT resources by all members of the university community and other persons formally engaged with legitimate university business, as may be determined from time to time.

2.3.2. Network Availability

i) The university's network will retain its present design and implementation, which extends services to all members of the community resident in all campuses, and wherever possible, will be extended to those located elsewhere.

ii)It will remain the university's ultimate goal to ensure that every room in the university that hosts teaching, research, and support activities is connected to the network; and every student and member of staff of the university will be enabled to have access to the university's ICT infrastructure.

iii)The university will maintain only one coherent/logical network that supports access to all general ICT support services. Where, however, the need arises, there may be private networks (independent of the university backbone), installed at the expense of the Faculty/Department/Unit concerned. In such cases, the installation must adhere to university standards, and the network's operation must not interfere with the university's network.

2.3.3. Network Reliability

i) All considerations concerning the design, construction, and operation of the university's network must be informed by the key objectives of high levels of availability, reliability, and maintainability.

ii) Network design and its implementation must be flexible enough to accommodate emerging technologies and standards as often as is desirable to do so.

2.3.4. Network Operations Center and Data Center

i) All back-end servers and associated equipment that constitute the hardware platform on which central network services are provided, will be hosted by the Network Operations Center (NOC).

ii) In addition to being the main gateway for data communication traffic, the Data Center shall establish and maintain a Disaster Recovery Center (DRC), preferably at a remote location, to guarantee an almost seamless turn-around, in the event of a disaster.

2.3.5. Inter-Campus Connections

This refers to those services and associated equipment, which facilitate the ability of a remote campus or remote university facility to access the University's backbone. It shall be the university policy that

i) the network(s) located at remote sites are so configured and implemented as to maintain a point of connection to the University's network backbone. If it is infeasible to establish a single connection, multiple, cost-effective connections may be established.

ii)Network protocols utilized for inter-campus connections must be characterized by approved configuration parameters, including approved network identifiers.

iii) All inter-campus connections are required to meet policy standards concerning security and management practices.

2.3.6. Private Networks

i) Private networks maintained by Departments or units may extend between buildings

ii)Where desirable, the CITS may provide links for private networks; but expenses due to requirements outside the capability of the University Backbone Network shall be borne by the Department or unit.

iii) Only private networks that cater for all occupants of a building may be considered for the provision of a campus gateway.

2.3.7. Routine network operations

a) The responsibility for the installation and maintenance of active network devices and equipment (switches, hubs, routers) shall reside exclusively with designated members of staff of the CITS working with the Networking Team.

b) When the CITS Networking team so recommends, and the CITS Director approves, other Staff of the CITS or University Technical staff may install and maintain switches, routers or hubs within local networks, provided that such installation and maintenance activities do not extend to points at which the devices and equipment connect to the university's backbone.

c) Domain Name Services (DNS) associated with the university network shall be centrally managed and monitored by the CITS.

d) All equipment connected to the University network shall be assigned unique IP addresses

- IP addresses assigned to equipment shall be very clearly and visibly displayed on equipment casing
- It shall be the responsibility of the Head, Networking Team, to plan and allocate blocks of IP addresses to different sub-nets, and maintain a central inventory of records of equipment and associated IP addresses.
- IP addresses that remain inactive three months after the initial assignment shall be withdrawn.

e) It is prohibited to link MODEMS or other means of access to other networks via equipment located on university-owned or managed premises to the university network, without a written explicit permission from the Director of the CITS

f) The CITS shall be responsible for providing and managing web cache facilities for downstream web traffic; and all web access setups shall be such that use is made of the university's web cache facility for downstream internet traffic.

g) For the purposes of compliance enforcement and promotion of acceptable use policies, the CITS shall acquire and deploy appropriate filtering facilities for web-based and non-web-based internet traffic and other bandwidth-use-intensive services that are not of direct relevance to content delivery (teaching) and research activities.

h) The networking team shall monitor and document the University's network performance and keep a monthly record of appropriate performance indices.

2.3.7.1. Server Administration Policy

This section serves the purpose of providing policy guidelines that will inform the Center‛s ability to discourage practices that tend to degrade the usability of network resources, and hence reliability of Internet (and associated) services provision.

Organizational Scope

i. Each server is required to have a **server administrator,** assigned the responsibility for the management and maintenance of the server

ii. No server administrator is ordinarily allowed to carry out routine inspections or monitor/disclose information hosted on servers without the permission of the asset owner

iii. When a server administrator is obliged to inspect databases in the course of discharging administrative duties, access shall be limited to the minimum required for the desired level of inspection, and shall not extend the right to disclose confidential information.

iv. Large and complex networks invariably rely on a number of directory services utilized for the identification of components connected to the network. ONLY those units of the University duly authorized by the CITS' networking team many run ANY of these services

v. Inappropriately configured of misconfigured servers occasion such problems as

- disruption of network packet routing, which effectively brings the network down
- mis-delivery name-dependent protocols
- server crashes, data loses, and extended down time .

Any server that falls into the category within a stipulated time frame shall be disconnected from the Network until the networking team is satisfied that the configuration (or similar problem) has been appropriately resolved.

Additional Server Security Policy Provisions

a) Server Administrators for servers connected to the UNILAG network are responsible for the security of the server as prescribed by the University's ICT policy. In particular, the server administrator shall

- be accountable in the event of the occurrence of a compromise

- at all times, demonstrate reasonable precautions to secure the host

b) Administrators shall be required to limit **log-ons; account log outs after three failed log on attempts is recommend.**

c) A regular review of accounts shall be carried out for the purposes of identifying inactive accounts, which shall then be disabled. Administrator may only use local accounts (accounts not located on/authenticated against an authentication service, e.g. kerberos) when absolutely necessary.

d) it is recommended that whenever possible, a logon banner displaying messages of the type "*this server if for authorized use only*" should be displayed during any attempt to logon on to system; and if possible, some form of logon restriction (time of day, system address, for example) should be implemented.

e) Logs of users activities (including date, time, user-id, commands executed, ID of local or remote terminal utilized for access, error condition, etc) shall be retained for a period of 12 months, during which a backup of all log files should be carried out.

2.3.8. Voice over IP (VoIP) Policy

Objectives and Scope

The term VoIP refers to a technology that facilitates voice communication over data networks and between the traditional (legacy) networks and data networks. This technology is fast replacing traditional telephone networks, which are no longer being manufactured, making it imperative that the University migrates voice services to the data communication network.

The VoIP policy, therefore, serves the purposes of ensuring that

- Devices acquired by departments/units are in compliance with VoIP network and security standards that may be adopted by the University
- Interoperability issues are resolved before acquisition, thus minimizing the cost of university- wide implementation.

Provisions of the policy are applicable to all students and members of staff that are desirous of connecting VoIP devices to the University's data network.

Policy Statement

a) The CITS shall maintain a list of approved VoIP devices, for the purposes of regulation

b) Only approved VoIP devices acquired by, or through departments and units of the University of Lagos may be connected to the University's data network

c) Departments or units desirous of acquiring VoIP devices shall ensure that the devices are type- approved prior to acquisition

d) A list of VoIP devices connected to the data network shall be maintained by the CITS

e) Established network and security procedures shall inform the connection of VoIP devices to the network.

RESPONSIBILITIES

- It shall be the responsibility of the CITS to maintain a register of type-approved VoIP devices and to grant type-approval to devices to be connected.
- It shall be the responsibility of the CITS to develop, certify, and clarify VoIP security and network standards and procedures
- It shall be the responsibility of the CITS to monitor the use of VoIP devices connected to the network for the purposes of detecting non-compliant devices.
- Sanctions for non-compliance shall be determined, from time to time, by the CITS management Board and made available to the University community.

2.4. ACCESS CONTROL POLICY

Policy provisions in this section specify the category of persons allowed access to the ICT facilities, infrastructure, and services provided by the University of Lagos, and define the logical and physical conditions under which access is permitted. The objectives of the provisions include:

- ***emphasizing the need for access control***
- ***establishing specific control measure for protection against unauthorized access***
- ***ensuring that the ICT infrastructure is capable of fostering data communication and data sharing without compromising the security of ICT resources.***

Public or private services provided by the University are available only to authorized users. Services including (but not limited to) publicly available services and information available on the University website as well as services offered by the University Library are regarded as 'public services'. All other services are private services provided by the University of Lagos for use by authorized persons only.

Every authorized user remains eligible to run an active account if his/her relationship with the University is current. At the expiration of their relationships with the University of Lagos, such persons will no longer belong to the class of authorized users and their access rights shall be withdrawn.

2.4.1. Authorized Users

Only persons associated with the University of Lagos in any of the following capacities automatically attract the status of 'authorized user'

✓ serving employees or officers of the University of Lagos

✓ duly registered full-time students of the University of Lagos

✓ duly registered students of University of Lagos' degree-awarding part-time programs

✓ non-employe members of the Governing Council of the University of Lagos

Time-bound authorized-user status may be granted to persons falling into any of the following categories:

✓consultants/contractors engaged by the University of Lagos under a formal contractual arrangement

✓members of collaborative partnerships involving the University of Lagos

✓non-university personnel with legitimate access interests, who having completed an on- line application and subsequently recommended by a designated CITS official, receive the approval of the Director of the CITS.

2.4.2. User Accounts Administration

Activation: an account creation occurs when a person assumes the status of an authorized user through a valid and *bona fide* relationship with the University; that is, the account is created when a

- student is enrolled and is duly registered
- member of staff assumes office through a specified human resources process
- non-university staff has has completed a prescribed application process and is duly registered as a non-university staff.

No user account shall be created before a person assumes the status of an authorized user.

When the account creation is completed, the user account will be registered and become active after first login session.

Deactivation: user accounts shall be deactivated when the user ceases to have a formal relationship with the University of Lagos either by reasons of expiration or termination of appointment or studentship, as may be applicable.

- STUDENTS

In particular, deactivation shall occur in the case of students when the student

a) graduates from a course of study

c) is suspended, expelled or withdrawn from the university

- STAFF

And in the case of University staff, account deactivation shall occur when for the member of staff, his/her

a) appointment is terminated

b) services have been withdrawn

c) retirement commences

- Non-University Persons

For non-university persons, access rights shall be withdrawn and associated accounts deactivated, when

a) contractual arrangements or consultancy services reach end-of-life

b) collaborative research projects are concluded

c) Sabbatical/associate appointments expire

Account Privileges

Account privileges shall be assigned on the basis of the *principle of minimal privilege*[1]. Accordingly, authorized users shall be provided only with access limited to that specified by their roles within the University of Lagos. Whenever the authorized user's role attracts *significant changes* , his/her access rights shall be reviewed to reflect the new role.

Account Auditing and Security

It shall be a University policy to carry out scheduled auditing of user accounts for the purposes of identifying and revoking inactive, barely-utilized, or unauthorized accounts. Account audit processes shall also review authorized accounts for the purposes of reallocation or revocation of access rights, following changes in status of authorized users. All accounts are required to have a minimum level of security provided by passwords that meet the requirements specified in §3 of this policy document.

2.4.3. Use Policy Breaches and Sanctions

Due process shall be applied in imposing sanctions following the detection and establishment of a breach of the use policy provisions or rules.

a) Any alleged breach of use policies shall be investigated by designated person(s)/agent, and findings shall be communicated in writing to the Director of the CITS.

[1] *access is limited only to information and resources necessary for execution of person's legitimate business*

b) Upon receipt of the investigation report, the Director shall classify the breach either as 'non-serious' (*not constituting a risk to university or imposing an economic burden on the university)* or 'serious'.

c) In the case of 'non-serious', the Director has the discretion of imposing either of the following sanctions:

- suspension of the user account for a minimum of three months
- suspension of the user account for a minimum of six months in addition to a suspended sanction of permanently disabling the user account

d) In the case of 'serious' breaches amounting to misconduct as defined by appropriate university policies, the Director, upon receipt of the findings shall refer the case to the University for formal disciplinary actions.

3. SECURITY POLICY

3.1. INTRODUCTION

The main objective of the policy provisions in this section is to guarantee protection for the University's ICT resources from malicious or inadvertent disclosure, unintended modification, or malicious destruction, without compromising the ability to serve the requirements of open information sharing. By including the specifications of what constitutes acceptable use of university ICT facilities and in furtherance of the university's culture of promoting best practices in all areas of endeavor, the policy establishes a basis for a generic understanding of information security as defined by the conventional principles of *confidentiality, integrity, and availability*[2].

3.1.1. Scope

Provisions of this section of the policy document are applicable to all categories of users defined in §2 including personnel engaged by third parties, and extend over all ICT devices, equipment, and software in use by the university.

3.2. Responsibilities

Whereas it shall be the responsibility of the CITS to provide a reasonable level of privacy to all authorized users, the CITS shall not be responsible for guaranteeing the confidentiality of personal information transmitted over or stored on any network, device, or equipment owned by the university.

[2] *confidentially* restricts access only to authorized user accounts; *integrity* protects data against malicious alterations; and *availability* guarantees that desired information items are accessible as often as required.

a) The protection of the university's network and mission-critical university data and systems shall be the responsibility of the CITS. But the CITS shall not be responsible for the protection of personal data existing on the university's ICT infrastructure.

b) It shall be the responsibility of users to exercise good judgment concerning the reasonableness of personal uses to which university ICT services are put. Where policy provisions are available, personal uses shall be informed by the policy provisions, and in the absence of explicit positions, user shall be obliged to seek guidance from the CITS.

c) Authorized members of the CITS shall have the responsibility of monitoring equipment, network traffic, and associated systems for the purposes of security and maintenance.

d) The rights of the CITS staff to carry out monitoring activities for compliance enforcement shall not be challenged by any user.

3.3. Confidential Information

All items of university information residing on CITS systems shall be categorized as either 'confidential data' or 'non-confidential' data. Confidential information shall include (but not limited to) data concerning payroll, human resources management, research data, and students' examinations results. It shall be the responsibility of all employees engaged with data processing activities associated with confidential information to abide by access control measures taken to prevent unauthorized access.

a) Accounts sharing of any type is strictly prohibited, and it shall be the responsibility of all authorized users to keep passwords secure.

b) System-level passwords shall be changed quarterly, and user level passwords, at least twice a year.

c) All official PCs, laptops, and work stations shall be characterized by password-protected screen savers set to activate when the system is unattended for no more than 10 minutes; or to log-off when the host is unattended for no more than 10 minutes. Defaulters will be sanctioned as determined by the CITS Director.

d) All devices connected to the University network shall at all times be required to be protected by an approved and up-to-date anti-virus software.

3.4. Unacceptable use

All users (employees, students, contractors, consultants, or any other authorized user) are prohibited from engaging in activities that are illegal under the Nigerian or International

Law when using the University’s ICT facilities. Examples of unacceptable use include (but not limited to) the following:

i) activities that violate copyright, trade mark, patents or other intellectual property laws or associated provisions of the university’s code of conduct.

ii) deliberate introduction of malicious codes (viruses, trojan horses, worms, and general malware) into university network or servers

iii) revealing or sharing passwords of university accounts

iv) activities that amount to sexual harassment or lead to the existence of a hostile business environment

v) deliberate precipitation of a security breach such as logging on to a server or database for which access is explicitly prohibited or outside the scope of designated assignments,.

vi) activities that lead to disruption of services, such as *pinged attacks, sniffing, packet spoofing, denial of service attacks, and forged routing for evident malicious purposes.*

vii) unauthorized port scanning or security scanning

viii) deliberate interception of data meant for some other destination

ix) deliberate bypassing of authentication or similar security features of any user account, host, or server.

x) programming activities designed and executed for the purposes of interfering with or disabling another host’s session

xi) the use of university infrastructure for non-official purposes, particularly on a commercial basis.

Another class of unacceptable use includes those associated with email and voice communication activities such as the following:

i) unsolicited (‘spam’ or ‘junk’) email messages or other advertorial materials sent to individuals who did not request for them

ii) forging or unauthorized use of email header information

iii) creating or sending fraudulent mails or ‘chain letters’

iv) all forms of harassment via email or voice communications as determined by language of communication or size/frequency of message

3.5 EMAIL POLICY

This policy is applicable to, but not limited to, University members of staff, visiting staff, physicians, non-teaching staff, students, contractors, volunteers, and guests who are provided email services managed by or for the University of Lagos.

A. USE OF EMAIL ACCOUNTS

The CITS provides Email services to allow members of staff to conduct University business. Personal use of email is allowed, provided that personal use (a) does not interfere with performance of work responsibilities, (b) does not affect the University network performance and (c) is otherwise in compliance with other University policies.

B. OFFICIAL EMAIL ADDRESS

i. An Official Email Address will be assigned to Students and University members of staff, which will include a mailbox assigned to one of the Official University email systems:

- Staff email system (Google Mail)
- Student email system (Microsoft Office 365)

ii. University business-related emails are to be sent and received via the Official University Email Address and to be used for all University Email correspondence lists, and for the official online directory. Official communications from University Offices, such as the Vice-Chancellor's Office, Human Resources, the faculties, Security and others, will be referred to the Official Email Address. Consequently, users shall be acknowledged to have received all official University Email messages sent to their Official University Email Address.

iii. Human Resources department shall inform the CITS on all appointments, retirements and disengagements of staff from service.

iv. Email account shall be created for all visiting members of staff within the period of stay in the university

v. Staff email account shall be deactivated immediately if such staff member is suspended, retired or have his/her appointment terminated.

vi. Student email account shall be active all through their study period. Students shall retain their email accounts after graduation.

vii. Students shall be contacted by the Alumni via their University email account in order to foster continuous dissemination of information after graduation.

In a case where an individual has both a student and employee affiliation to the University of Lagos, provisions will be made for a separate email box for each affiliation. Email services are made available only while a user is employed by or enrolled at the University of Lagos. Exceptions may be approved for conditions such as indefinite email extension for emeritus status, or to a period of six months after staff retirement.

C. MISUSE

Email is simply a communication tool. Use of Email in violation of other University policies is also a violation of this policy.

Examples of improper uses of University email are:

- Concealment or misrepresentation of names or affiliations (e.g., misrepresenting oneself as another user);
- Use of email to send spam (unsolicited non-University commercial email);
- Alteration of source or destination address of Email;
- Use of University of Lagos email to violate the law.
- unsolicited ('spam' or 'junk') email messages or other advertorial materials sent to individuals who did not request for them
- forging or unauthorized use of email header information
- creating or sending fraudulent mails or 'chain letters'
- all forms of harassment via email or voice communications as determined by language of communication or size/frequency of message

D. SANCTIONS

Violations of this policy may or will result in:

- suspension, blocking, or restriction of access to information and network resources when it judiciously seems necessary in order to protect the integrity, security, or functionality of University of Lagos resources or to protect the University from liability;
- a department being held financially responsible for the costs incurred as result of a data breach, loss or illegal disclosure.

3.5. Password Policy

Passwords in use by authorized users for the different access levels shall be guided by the following provisions.

a) System level passwords (*root, enable, server administration, accounts administration etc)*

shall, as much as possible, be changed every three months

b) Users are encouraged to change user-level passwords (*email, web access, personal computers)* at least twice a year.

c) Passwords for user account with system level access privileges shall be different from those in use for all other accounts held by the user.

d) it is forbidden to include passwords in emails, except for the express direction of the CITS Director.

e) all university passwords fall into the class of 'confidential information' and shall not be shared with anyone including personal assistants or confidential secretaries

f) whenever an account or its password is suspected to have been compromised, the password shall be changed immediately and the account suspended by the system administrator for a period of two months,.

g) it shall be the responsibility of designated CITS staff to randomly scan passwords with 'cracking' or 'guessing' tools as a proactive means of identifying vulnerable passwords. Whenever the process identifies such a password, the user shall be required to immediately change it.

All users, as a matter of policy, shall be required to familiarize with the following established rules for creating **strong passwords.**

a) should be at least 8 alphanumeric characters long

b) should include at least one lowercase and one uppercase letter

c) should include at least one numeral (0 -9) and some special character such as #, $, %, ^, ‽, «, ῳ, ‡, ὒ

d) should NOT be based on personal information, family names, vehicle registration number, phone number, etc

3.6. Server Security Policy

Servers deployed within the university's network shall be associated with distinct operational groups, with whom server administration responsibilities shall reside. It shall be each operational group's responsibility to ensure server configuration compliance and to implement exception policies specified for their business environments. For security reasons, each operational group shall establish a secure server configuration change, process, and in the case of servers running mission-critical applications, the process shall undergo a review and consequent approval by the CITS management.

The CITS shall establish and maintain a record of servers attached to the University network, including, at a minimum, information concerning

- physical location of server

- contact details of server administrator

- hardware specifications and operating system version in use
- a brief on the functions and applications of the server.

3.6.1. General Guidelines for Server Configuration

The configuration of server operating systems shall be informed by the following general guidelines:

a) Services and applications (FTP, NFS (Network File System), TELNET, etc) that are not in use shall, at all times be disabled.

b) A record (log) of access to services shall be maintained, and where possible, such access shall be protected by the best available access-control method.

c) Whenever immediate installations will not interfere with business processes, the most recent software patches shall be installed on server systems.

d) Because trust relationships (such as NFS) between systems, constitute security risks, it shall be the policy to avoid the use of trust relationships when alternative secure communication protocols are available.

e) assignment of server user access privileges shall be based on the principle of minimal privilege as described in §2.

f) where a non-privilege access will suffice, 'super-user' access user rights shall not be assigned.

g) whenever a technically feasible *secure channel connection* methodology is available, privilege access assignment shall occur over secure channels.

h) it shall be forbidden to locate and operate servers from uncontrolled or easily accessible open locations.

i) a record of every security related event (*port scan attacks, unauthorized access to privileged accounts, abnormal occurrences that are unrelated to specific applications associated with host)* on critical or sensitive systems shall be maintained, and all scheduled system back-ups shall include audit trials of the events. Corrective actions shall be prescribed as may be appropriate.

For the purposes of audit, all desirable access types shall be granted to the CITS team constituted for performing auditing tasks. Access types shall include

- user level and/or system level access to target computing or communication device
- access to data produced, transmitted, or stored within the university infrastructural environment
- access to otherwise restricted business environments

- permission to interactively monitor and document traffic information on the university network

3.8. Security Policy for Non-CITS Computer Laboratories

Each university department or unit that runs a computer laboratory shall appoint an officer (Laboratory Administrator) and formally communicate the name and contact information of the officer to the CITS. The departmental/unit laboratory administrator shall be the focal point and liaises with the CITS for all operational issues concerning the laboratory. In addition to having the responsibility for the day-to-day running of the laboratory, the laboratory administrator

a) shall be responsible for ensuring compliance with relevant university policies; particularly security policies as well as whatever impact(s) the laboratory may have on the university network

b) shall have the responsibility of controlling access to the laboratory and limiting access only to legitimate users

c) shall provide the CITS with a record of IP addresses and associated configurations for all hosts in the laboratory. Changes to documented configurations shall only be effected with the permission of the CITS network management team.

d) shall notify the CITS in the event that the department/unit wishes to add external connections to the laboratory whilst retaining connection to the university network. And in such cases, the notification shall include schematic diagrams of the proposed connection and a brief providing justification for the proposal. Implementation may only proceed, after the CITS has evaluated and passed the security provisions of the proposals.

e) shall ensure that the laboratory does not replicate services offered by the CITS, including shared critical services (world wide web -www proxy services, email services, web hosting, FTP services) provided via the university network that generate revenue streams or facilitate user capabilities, and which shall remain the exclusive preserve of the CITS.

f) shall understand that the CITS reserves the right to suspend connections to the laboratory, if such connections are adjudged to destructively interfere with CITS infrastructure.

- Laboratory administrator shall arrange to be available round the clock to attend to emergency situations that may develop and therefore avoid connection suspension actions, where it is possible to do so.

- Requests for waivers from the provisions of this section shall be treated on the merits of individual cases.

3.8.1. General Guidelines for Laboratory Server Configuration

a) All traffic between sub-nets and computer laboratory shall be subjected to firewall screening, and computer laboratory devices (wired or wireless) are prohibited from bypassing screening firewalls.

b) Departmental/unit computer laboratories are NOT permitted to engage in *port scanning, network auto-discovery, traffic spamming or flooding* activities with potentials of destructive interference with the university backbone or any other network.

c) Laboratories (such as training laboratories) that routinely grant access to non-university persons are prohibited from having direct connectivity to the university backbone. And no university confidential information (as defined in this section) shall reside in such laboratories.

3.9. ANTI-VIRUS POLICY

The University of Lagos subscribes to a site-licensed commercial anti-virus software for use by bona-fide members of the university community with university owned, and personal computers. Because viruses, trojan horses, worms, and other malicious software can destroy confidential or mission-critical data, compromise data integrity, or generate voluminous traffic, a few infected systems can disastrously affect the university's network and consequently fatally limit the university's ability to carry on with its core business of teaching and research. Therefore, as a key component part of measures designed to protect university ICT infrastructure, an anti-virus software policy, with provisions prescribed below, shall be implemented.

a) All computers (university owned and personal) connected to the University network and running an operating system for which the University has a site-licensed anti-virus software shall install and enable the university licensed anti-virus solution.

b) Authorized users desirous of using alternative anti-virus solutions shall ensure that the software is on the list of approved anti-virus software maintained by the CITS; or apply for approval by the CITS.

c) Computers running on operating systems other than those for which the university has site-licensed anti-virus solutions are not required to be compliant. However, such computers shall acquire, install, and enable anti-virus software capable of mitigating identifiable risks.

d) it shall be the responsibility of CITS staff with appropriate administrative privileges to install, troubleshoot, and maintain of the site-licensed anti-virus software. The anti-virus software shall be actively managed such that up-to-date signatures are installed.

e) the anti-virus software shall be configured to ensure updates are frequently and regularly available automatically either directly from the solution provider or from a campus-wide distribution center at the CITS.

f) computer systems detected to be in violation may be denied access to the network, and in such cases, access rights shall not be restored until the machine is certified to be in compliance.

The CITS shall advertise the following precautions and any other precautions that may become desirable, to all users:

- files or macros attached to emails from unknown, suspicious, or non-trusted sources should NEVER be opened. Such emails should be deleted completely from the computer, including its trash bins.
- spam, chain, and junk emails should NEVER be forwarded and should be deleted
- file attachments from unknown sources should NEVER be downloaded
- direct disk sharing with read/write access should be avoided.
- removable media (diskettes, flash disks) should ALWAYS be scanned for viruses before being attached
- critical data and system configurations should be backed periodically, and back-up data stored in a safe medium

3.10. Physical Security Policy

Server Rooms

a) all computer servers shall be located in purpose-built rooms equipped with adequate air-conditioning systems and through which water and rainwater drainage pipes do not pass.

b) whereever possible, raised false-floors shall be installed to accommodate computer cables/cable trays to reduce the risk of inadvertent damages.

c) power sources to the servers shall include Uninterrupted Power Supply (UPS) units with surge protectors to facilitate safe shut downs in the event of extended periods of power failures

d) only authorized university staff shall have access to server rooms

e) all non-CITS staff engaged to work in server rooms shall be supervised at all times. A notice of at least twenty-fours shall be given prior to the commencement of activities involving non-CITS staff to enable suitable arrangements for supervision.

f) appropriate automatic fire-fighting system shall be installed in all server rooms.

g) physical access control features and surveillance cameras shall be installed in server room/ data centre facilities.

Access Control

a) only designated systems administrators responsible for particular systems shall have the authority to assign system, network, or server access rights

b) it shall be the responsibility of designated system administrators to maintain system and associated information integrity.

c) access granted to non-university (third-party) users shall include measures to mitigate identifiable risks and protect university information assets.

d) supervisor passwords for all mission-critical equipment/CITS servers shall be disclosed in confidence to the Director of the CITS , who shall retain the passwords in secure custody for use ONLY in emergencies.

e) all severs shall have system audit capabilities installed for the purposes of logging all login attempts and failures, and tracking changes made to the system

LAN/WAN Physical Security

a) Equipment for the university's LAN/WAN (switches, routers, hubs, etc) shall be located in secure rooms with access restricted to only CITS networking team staff.

b) Cabinets housing the devices shall be kept under lock, and whenever access is required for legitimate business, it shall be granted under the supervision of designated CITS staff.

4. SOFTWARE DEVELOPMENT, ACQUISITION AND MANAGEMENT

4.1. INTRODUCTION

The University of Lagos is a degree-awarding institution whose multidisciplinary teaching and research activities rely on efficient, secure, and reliable operations supported by information technology. This implicit statement of dependence on information technology and systems for core business activities underscores the need for a reliable information systems environment, characterized by policy positions that can readily adapt to the ever-changing world of information technology.

4.1.1. Objectives

It is the main objective of this policy to prescribe the requirements for the development/ acquisition, adaptation and management of new applications software for various uses in the University. The provisions of the policy address the functional and operational needs of information technology resources deployed for the purposes of processing and storing confidential and mission critical information, and set forth a set of mitigating measures for the security risks associated with the acquisition and development of new applications software.

4.1.2. Scope

The policy covers software development, acquisition, and management, including Software Development Life Cycle (SDLC), and applies to all information resources asset owners, systems analyst/administrators, and management personnel.

For the purposes of identifying asset owners and assigning responsibilities, software will be categorized into two types; namely: *centralized operations software,* and *unit-specific software.*

- ‘*centralized operations software’* refers to software for applications run from central locations (servers) and utilized by the entire university community. Such applications are hosted, maintained and supported by units in the CITS
- ‘*unit-specific software’* refers to software acquired by units/departments/faculties to meet unique needs, and for which procurement and maintenance is the responsibility of the unit/department/faculty.

It shall be the responsibility of the Software Engineering and e-Applications (SE&E) Unit of the CITS to evaluate both software types for resource requirements, interfacing requirements (where applicable), security features, vulnerabilities, compatibility, and possibility of duplication.

4.2. General Procedure

a) All in-house developed software shall be developed according to a Software Development Life Cycle (SDLC) plan, and it shall be the responsibility of unit/ departmental/faculty heads to develop, maintain, and participate in the SDLC plan.

b) SDLC plans shall, at a minimum, address issues concerning *requirements analysis/ feasibility study, risk analysis and associated mitigation, systems analysis, detail design and documentation, quality assurance, acceptance testing, roll out (or implementation), post-implementation maintenance, and review.*

c) each product shall have designated asset owners and custodians, who shall have responsibilities for periodic risk assessments for the purposes of evaluating the effectiveness of security/control measures

d) unit/departmental/faculty heads or asset owner shall ensure that all relevant systems have documented access control processes, which restrict access to systems and assign privileges available to system users.

e) whenever possible, development, production, and testing environments shall be separated in order to impose strict security measures for the production system and allow fewer security risks for the development and testing environments for optimum productivity.

4.3. Software Acquisition

The process of acquisition of any new software shall be conducted in consultation with the SE&E unit of the CITS, and at the time of acquisition the SE&E unit shall, through the Director of the CITS, advice the asset owner on the most appropriate options, using the following considerations as guidelines.

- **In-house Development**

For centralized operations software, the Director of the CITS, in consultation with the Deputy Director Operations shall constitute the team with clear and specific terms of reference informed by the general procedure of §4.2. and designate a team leader.

And in the case of unit-specific software, the development process will involve the SE&E unit, and informed by the general procedure outlined in §4.2. In both cases, cost and human resources requirements shall justify the decision to proceed with development. Where in-house software development is the preferred option, the development will be carried out centrally to preclude the possibilities of duplication of efforts and ensure optimum use of available resources.

And whenever it is technically and economically efficient to do so, existing software shall be extended/fixed/upgraded rather than embarking upon the development of a new solution.

- **Off-the-shelf Purchases**

Where outcomes of feasibility studies indicate that the in-house development option is either not viable or expedient, the possibility of acquiring a propriety software shall be considered. For centralized operations software, it shall be the responsibility of the CITS to identify suitable software and determine modifications that may be necessary for successful adaptation to university needs. For unit-specific software the responsibility shall be that of the unit/department/faculty concerned, in consultation with the SE&E unit through the Director of the CITS.

The CITS shall evaluate the desired software and produce an assessment report including a definite recommendation on the advisability of purchasing the software.

- **Free and Open Source Software**

Free and open source software (FOSS) represent the class of software whose license terms provide that the source code and associated rights are freely available in the public domain. Users are free to modify, adapt, improve, and redistribute the software in whatever form (original or modified) they deem fit without any financial considerations.

a) the university shall encourage the use of FOSS where it is feasible to do so, as a capacity building strategy.

b) in cases where the use of FOSS will lead to significant dependence on the developers (particularly for a fee) for intervention during operation, the software shall be classified 'off-the-shelf' and its possible acquisition treated accordingly.

4.4. Software Usage

The purpose of a software usage policy is to guide the direct or indirect use of licensed software by members of the university community. Such policies specify best practices for software acquisition, copying, use, and transfer; and serve to inform the university community about the gravity of misconducts associated with software misuse.

4.4.1. Scope

This policy is applicable to all software by or on behalf of the University of Lagos, regardless of where it is put to use (and regardless of how it is acquired.)

Software within the scope of this policy shall only be used in compliance with all license terms and provisions of the purchase agreements.

All software acquired for or on behalf of the University of Lagos or developed by university employees or contractors shall be deemed university property.

4.4.2. Guidelines

a) every user has the individual responsibility to carefully read, understand, and ensure compliance with all licenses, notices, and agreements that come with software acquired, copied, transmitted, or utilized.

b) any duplication of software except for the purposes of back-up and archiving shall be regarded as a violation of this policy, with the exception of cases where license terms permit such duplications.

c) all software that fall into the category of university property shall be copied prior to first use and the 'master copy' kept in safe custody by the CITS.

- shall have master copies that are reserved only for the purposes of recovery due to computer disasters (virus infections; hard disk crashes, physical damages, etc) which make it impossible to access or use the original copy
- shall automatically impose license terms of the original copy on the 'master copy'

d) no user has the rights to sell, lend, sublicense or make available university software to any unauthorized individual or entity.

5. USER SUPPORT POLICY

The CITS statutorily acquires, develops, and produces a range of information technology tools and resources to provide IT support for university core and support business activities. And in some cases, the tools and resources are made available for use by employees and students. In order to ensure that full advantage is taken of the capabilities of such IT tools and that the resources are put to optimum use, it is desirable to institute a set of guidelines to systematically develop end-user skills.

5.1. Policy Objectives

The objectives of the policy include the development of the ability of *bona fide* University of Lagos end-users of ICT tools and resources to:

- independently, efficiently, and effectively utilize available tools and resources
- make significant contributions to the tools and resources acquisition processes of specification, design, and implementation
- develop a keen awareness of end-user responsibilities in the usage of ICT tools and resources

5.1.1. E-learning Objectives

It shall be the university policy that staff and students of the university acquire competence in skills required for the effective use of the Learning Management Systems (LMS) and associated tools that management may provide from time to time. Accordingly:

- all academic staff and students shall acquire levels of skills necessary for the effective use of MOODLE LMS (or any other LMS) for e-learning activities
- all academic staff shall acquire levels of skills necessary for the effective use of the TURNITIN (or any other) anti-plagiarism tool acquired by the University.

5.1.2. Scope

The guidelines provided in this section are for use by employees and students of the University of Lagos and they cover end user support service including network services, hardware maintenance services, user training services, procurement support services, and information systems support services

5.2. Policy provisions

It shall be the responsibility of the Directorate of the CITS to provide support services that facilitate the ability of end-users of university ICT tools and resources through the provision of technical expertise and logistics support towards efficient roll out and subsequent utilization of ICT resources.

- Consultancy services on ALL ICT matters shall be provided by the CITS.
- The CITS shall have competent representation at all meetings and on all committees concerning university-wide ICT matters.
- The CITS shall, from time to time, develop and communicate ICT technical support information for dissemination to end-users; and shall provide a liaison to interface with end-users for the resolution of technical problems.

User support areas shall include the following:

5.2.1. Procurement support

a) End-user ICT acquisitions and purchases shall be informed by specifications for minimum standards outlined in the procurement policy for ICT hardware, software, services and consumables. Failure to comply with this provision may lead to inability of the CITS to offer effective support.

b) The CITS shall participate in undertaking surveys and preparing design specifications and Bills of Quantities/Materials, as well as implementation/supervision of implementation (as may be applicable) of all ICT infrastructural resources in the university.

c) All purchases and acquisitions shall be vetted by designated CITS support function staff for compliance with standards.

d) All categories of software in common use by staff and students shall receive support from the CITS, as may be desired or desirable.

5.2.2 Hardware and Network Devices Support

a) whereas asset owners shall be responsible for daily handling and routine maintenance of ICT hardware owned by them, the CITS shall offer 'second level' support for all categories of hardware (desktops, palmtops, laptops, tablets, PDAs, projectors, UPS, LCDs, etc) in common use by staff and students for university business.

b) Ownership of the University's backbone network (including associated switches, bridges, routers, and gateways) shall belong to the CITS, whose responsibilities for them include:

- establishment and maintenance of an adequate operational environment
- carrying out routine preventive and corrective maintenance activities, and maintaining standard log books
- carrying out upgrading activities

c) IT support units on all campuses of the university shall have a stock of standard tools and tool boxes for use with hardware maintenance. The tools shall include those for the removal and replacement of Surface Mounted Devices (SMDs) and Ball Gate Array (BGA) ICs.

d) an inventory of available tools shall be maintained centrally at the CITS.

e) it shall be the responsibility of the CITS to ensure the availability of logistics resources in the form of transportation for the rapid movement of men and materials to, and between support sites, and communication between support sites and office locations.

f) in the case of building or office renovations in the university, CITS must be notified at least two (2) weeks before commencement of work, so that ICT Infrastructures are appropriately safeguarded to avoid damages that result in wastage of resources.

g) The CITS recommends that new building construction should include computer network design

6. MAINTENANCE POLICY FOR ICT EQUIPMENT

In recognition of the importance of maintenance in ensuring that ICT equipment and devices are always in service conditions conducive to the timely delivery of quality services to end-users, the university has adopted a set of maintenance guidelines for ICT equipment maintenance personnel in the university.

6.1. Policy Objectives

Guidelines provide in this section serve the objectives of ensuring that ICT devices and equipment remain in serviceable conditions throughout the manufacturers' prescribed equipment service life; by specifying best practices associated with the maintenance of various equipment types, including how to minimize down time in cases of scheduled preventive maintenance and fault-related corrective maintenance activities.

6.1.1. Scope

Provisions in this section of the policy document apply to all persons utilizing ICT equipment and devices owned, supported, managed, or operated by, or on behalf of the University of Lagos, including university employees, students, ICT equipment suppliers, and contractor/consultant personnel engaged for the purposes of carrying out maintenance work on such equipment. Policy provisions prescribe maintenance service types and necessary associated skills that will facilitate effective and efficient use of available resources as well as general steps and procedures for use in carrying out common maintenance tasks.

6.2. Policy Provisions

- preventive maintenance schedules shall be prepared by responsible officers, preferably according to manufacturers' specifications.
- where equipment or device is under subsisting warranty, terms of the warranty shall be invoked, if applicable, to invite maintenance intervention from the equipment vendor.
- asset owners, using available resources shall resolve basic maintenance problems as the first level of maintenance
- all levels of maintenance beyond first level shall be escalated to the CITS to address such problems..
- any case of third-party technicians involvement must be through the Director of the CITS

.

- the use of third-party consultants/contractors shall be guided by the provisions of the policy on the 'hiring of contractors/consultants'.
- all maintenance units shall stock adequate supply of spares to be utilized for corrective maintenance purposes, in order to minimize down time

- standard maintenance logs containing a record of major corrective maintenance works on equipment and device shall be maintained in all cases.

6.2.1. Responsibilities

a) The CITS, through its Hardware and Facility Maintenance team, shall be primarily responsible for the provision of maintenance support for all types of ICT equipment including (but not limited to) desktops, laptops, notebooks, computers, scanners, printers, projectors, monitors, and sundry network equipment in common use as IT support for core and support university services.

b) Departments, units, and faculties that purchase equipment for official use shall, with support from the CITS, be responsible for the following:

- provision of conducive operating environment (floor space, air-conditioning, back-up power supply, and physical security)
- system installation and post-installation administration
- routine maintenance, including system upgrades when desirable
- compliance with relevant university policies
- cost of preventive and corrective maintenance activities

c) Privately owned equipment shall be repaired or serviced at a cost to be borne by the asset owner

6.2.2. Obsolescence

It shall be the responsibilities of 'officers-in-charge' to maintain and update records of manufacturer's recommendations concerning the obsolescence of hardware equipment. Maintenance teams shall carry scheduled periodic checks to identify, retire, and replace equipment that have reached 'end-of-life' according to manufacturers' recommendations.

6..3. Policy on the Engagement of Consultants/Contractors

The university understands that as citadel of learning and research with departments (systems engineering, computer science, computer engineering, and electrical/electronics engineering) offering degree and certificate level courses and conducting research in areas relevance to various aspects of the ICT; it should, ordinarily, not only be self-sufficient in matters concerning the ICTs, but should also be in a position to offer consultancy services in these areas. It is nonetheless conceivable that given the diversity and rage of skills required, there may be certain situations (including maintenance of equipment that cannot be supported by university expertise) where the desired expertise is as yet, unavailable in the university.

For such cases, external expertise (contractor/consultants) may be hired based on the provisions of the university policy outlined below, as follows.

a) external experts shall be hired, only when a diligent and exhaustive search reveals the absence in the university community, of the desired expertise

b) recommendations for the hiring of external consultants/contractors shall include written justifications describing the process and outcomes of the search for the desired expertise within the university

c) contracts terms for the hiring of external experts shall include Service Level Agreements (SLAs[3]), characterized by the usual clauses and the following particular clauses:

- a 'capacity building'/'knowledge transfer' clause, under which the contractor/consultant shall be obliged to train designated university personnel, over a reasonable time interval, to enable them repeat the same tasks, should a future situation so demand.
- a penalty clause for non-compliance with the 'capacity building' clause
- a clause requiring comprehensive details of each of the services to be rendered.

6.4. ICT equipment procurement policy

The success of equipment management and maintenance programs depends to a significant extent, on whether the equipment is a genuine manufacturer's product or a fake. It is important therefore to have in a place, a policy that ensures that only genuine products, carrying manufacturer's warranty, are purchased for use within the university.

Accordingly, the following shall be the policy of the University of Lagos on the procurement of ICT equipment, without prejudice to the provisions of the ACT/POLICY that guide procurement procedures in the university.

a) only Original Equipment Manufacturers (OEMs) or their accredited local partners shall be invited to submit quotations when new ICT equipment and devices are to be procured.

b) when there are no OEMs or accredited partners for the desired equipment, suppliers and vendors shall be required to provide verifiable warranties

c) the CITS shall develop, maintain, and periodically update a list of OEMs and gold partners of manufacturers of ICT equipment in the country, for use by university community

~~d) The CITS shall be~~ consulted, by units or departments intending to procure ICT equipment of any sort, to make recommendations on ICT equipment specifications that will be most appropriate for optimal functionality and compatibility with the existing University ICT infrastructure.

[3] Service Level Agreements document the common understanding concerning services, priorities, responsibilities, warrantees, and guarantees.

7. ICT TRAINING POLICY

Training requirements for effective and efficient use of ICT resources available at the University fall into two categories:

i) end-user training, through which the CITS shall offer training support towards enabling university persons (particularly staff) acquire skills necessary for the optimum exploitation of IT support services in discharging statutory duties; and

ii) ICT staff development training, which will serve as the main capacity building strategy for filling identified skill gaps in ICT personnel.

7.1. Policy Objectives

The main objective of this policy to set forth guidelines that will inform strategies and associated programs designed and implemented on the one hand, for the training of staff and students (where applicable) as university ICT facilities end-users; and other hand, for the training of ICT staff for capacity building and knowledge update purposes.

7.1.1. Scope

The policy applies to staff and students who utilize ICT infrastructure owned, operated, and managed by, or on behalf of the University of Lagos, for the purposes of the core university businesses of teaching and research, as well as for rendering services in support of the core businesses.

In the case of end-users, general approaches to training are described by the policy provisions, including broad training contents and methodology. For ICT staff, the procedure for identifying gaps in competencies and skills and consequently specifying efficient and cost-effective training (in-house organized/on the job; vendor/contractor organized; certification programs) strategies is also prescribed by the policy.

7.2. End-User Training

It is university policy that all university staff shall be literate users of ICT support services made available by the university, with a ***minimum*** level of literacy that is consistent with the associated demands of their job specifications. End-user training shall therefore have as training outcomes, the acquisition of skills that facilitate the effectiveness and efficiency with which the end users exploit available services.

7.2.1. Training Modalities and Responsibilities

a) ICT end-user training programs shall be developed by the CITS in collaboration with the University’s Human Resources Development Center (HRDC) and organized on a continuous basis, using facilities available at the CITS and the HRDC or both, as may be desirable.

b) Resource persons or Facilitators shall normally be University personnel nominated by the Deputy Director of the CITS in charge of training after an informed assessment of training needs; and approved by the Director. External resource persons shall only be utilized, where expertise is manifestly unavailable within the University.

c) No end-user training shall take place outside the University

d) where a department or unit, after a needs assessment, is desirous of a training program outside those mounted by the HRDC/CITS team, it shall request the intervention of the CITS for the organization of the training program.

e) every training program shall have specific training outcomes that shall be assessed at the end of training.

f) Only candidates that meet minimum performance standards, using pre-specified training outcomes as metrics, shall be entitled to 'successful participation certification' at the end of training.

7.3. ICT Staff Training

ICT Staff have the responsibility for the efficient delivery of IT support services through the management and maintenance of platforms, systems, and base technologies. And in that connection, they are obliged to ensure reliability through systematic programs for monitoring, maintaining, and continuously improving infrastructural capabilities. In addition to technical knowledge and field operations competencies, ICT staff also need vendor management skills for the purposes of extracting optimum solutions from service providers. Given the foregoing observations and the fact of the ever evolving-nature of ICT, it is apparent they shall often require continuing education for professional skills development and filling competency gaps. Training needs can be met through programs that fall into the categories of 'in-house/on-the-job' (mainly for newly recruited staff), vendor/contractor organized (when new equipment or service delivery platforms are acquired), and certification courses-for filling competency gaps.

7.3.1. In-house/on-the-job training

a) the CITS shall develop in-house training programs, including training on network security, risks assessment, and university policy, for all newly recruited members of operational staff or those members of staff whose job functions change require additional training

b) where feasible, in-house training, using University Resource Persons shall be organized towards filling identified competency gaps

c) in cases where circumstances so dictate, and provided that the cost/benefit index is favorable, practicing professional colleagues identified as established experts in certain areas where skills are lacking in the University, shall be invited for token honoraria, to train ICT staff on specific aspects of their job responsibilities.

7.3.2. Vendor/Contractor Organized

a) every contract for the acquisition of new technology (software or hardware) shall include a clause that obliges the vendor to organize documented training sessions for operational staff to implement the technology

b) every maintenance contract signed with external experts shall include a clause that obliges the contractor to organize documented training sessions for operational staff to implement the technology

7.3.3. Certification Training

a) ICT operational staff shall be encouraged to enroll in such industry-recognized certification courses as Microsoft, CISCO, LINUX, ISC2, PMI, CompTIA, and Oracle, to mention a few.

b) enrollment in certification courses shall be sponsored by the university under a staff development program, for staff recommended by their supervisors during annual performance appraisal exercises.

c) certification courses already existing at the CITS shall be continuously strengthened to enable them to be positioned to meet the certification training needs of the university at large and opportunity for new certification trainings will be explored (e.g.: CISCO, MICROSOFT, ORACLE, etc.).

9. SUSTAINABILITY OF ICT INFRASTRUCTURE

The ability of the university to sustain and improve upon its ICT infrastructure will depend on its ability to meet the recurrent cost elements identified below, as follows:

a) cost of high speed global internet connectivity solution (bandwidth)

b) cost of equipment maintenance

c) recurrent cost of applications software licenses

d) cost of acquiring new equipment for upgrades and replacing aging equipment.

Each of these cost elements are relatively high, which makes it mandatory for the university to develop strategies for income generation and attracting funding support for sustaining its ICT infrastructure, from both internal and external funding agencies.

9.1. Internal Income Generation

Certification Courses

The CITS shall be empowered to run fee paying certification courses in collaboration with the Human Resources Development Center (HRDC) and / or the UNILAG CONSULT.

Establishment of ICT Certification Testing Centers

The CITS shall make good of the University's clout to explore the establishment of notable ICT Certification test centers the likes of Prometric ® and Vue® test centers.

Technology Fee

University management shall, from time to time, determine a 'technology fee' payable every year, by each student. The fee shall represent a fraction representing the 'recovery of cost of services' provided for the students.

SOME IDENTIFIED OMISSIONS

1. University Website Administration Policy

   a. Administration

- Designated ICT personnel in the CITS Web Team shall be given administrative privileges of accessing the University of Lagos website backend.
- The recurrent payment for the renewal of University domain (unilag.edu.ng) shall be the responsibility of the CITS.
- Decisions on Upgrade, update and/or total transformation of the University website shall be informed by:
  - Evolution in applicable technologies in website development;
  - A directive from the University management.

   b. Content Development and Update (Responsibilities and Guidelines)

- Content development for pages of the University of Lagos website shall be the responsibility of the respective department or unit.
- Each department/unit will be required to assign a Web Content Officer who will be responsible for developing content and periodically updating the same.
- Contents created shall be required to follow the appropriate guidelines as will be provided by the CITS team.
-

   c. **Subdomain Administration (Guidelines for Creation, Discontinuation, agencies or** centers that are not direct University of Lagos department or unit)

- Creation of subdomains (e.g.: studentsportal.unilag.edu.ng) under the unilag.edu.ng domain shall be the exclusive responsibility of designated CITS personnel.
- Units or departments in the University of Lagos that desire to have subdomains shall make written requests to the Director CITS.
- Centers or agencies affiliated with the University of Lagos, (which are not direct departments under the University) that wish to be included in the University domain will be required to forward written request to the Vice Chancellor to seek approval.

d. Other Website Optimiztion Procedures (SEO, SSL Certificate, etc)

- All website optimization procedures shall be the duty of designated CITS personnel
- Optimization of appropriate features and plug-ins shall be carried out following a regular pre-determined schedule.
-

10. APPENDIX -DEFINITIONS AND GLOSSARY OF TERMINOLOGIES