SECTION ONE

Introduction

1.1 Vision

The University has developed the following vision for leveraging Information and Communication Technology (ICT) for fulfilling its mandate,

"To utilize ICT as enabler of University business goals".

1.2 MISSION

"To provide efficient, reliable and cost-effective ICT Services that meets or exceeds NUC's expectations for the benefit of Tansian University, Umunya".

By this statement, we mean: provision of accurate, reliable, acceptable online real-time proprietary academic and non-academic data for planning, implementation and evaluation of university goals; show casing university academic and non-academic programmes.

1.3 Objectives

This document is to serve as a set of policies and procedures for the University in using ICTs to achieve overall development within the University and in delivery of University's services. It will assist in benchmarking University's activities against the Policy, which will enable Tansian University to identify the areas which need attention and where rectification needs to be carried out. It will also ensure consistency in ICT activities and practices. The Policy articulates the minimum requirements expected of Information and Communication Technology (ICT), and management could add on to this and create Tansian University ICT policies and procedures, within this Policy framework. Thus, the Policy is mandatory for providing a unified approach in implementing e-governance and achieving the following;

-Improved efficiency and effectiveness of Tansian University.

-Ease and accessibility of Tansian University information and services for students, and other interested groups.

-Promote good governance.

- Develop ICT competence among Tansian University employees.

- Manage ICT resources in a sustainable manner.

1.4 Operational Framework

Timeframe

The implementation time frame is three years, commencing January 2023 and shall be extended from time to time, as determined by the University, with appropriate modifications. All faculties should adopt the policy and procedures within the assigned time frame. The policies and procedures envisaged under this document will not be static. It will be updated as frequently as required, taking into account changing trends in the environment, in technology, and changes in business processes.

1.5 Responsibility and ownership

ICT Centre is responsible for the formulation, maintenance and updating of the policies and procedures. It is responsible for monitoring the implementation of the policies and procedures. Individual faculties and units in Tansian University are responsible for adopting and implementation of the policies and procedures.

1.6 Scope

These policies and procedures should be adhered to by all faculties and units at Umunya, Oba and any other campus of Tansian University.

The ICT Policy's broad objectives are:

(a) To provide a framework that will enable ICT to contribute towards achieving Tansian University goals.

(b) To transform Tansian University into a knowledgeable University through the application of ICT.

The policy's detailed challenges are as follows.

1.7 Strategic ICT leadership

a) Increase the use of ICT as an enabler in Tansian University activities;

b) Raise the Tansian University level of awareness on the role and potential of ICT, especially in the empowerment of people and in enhancing governance;

c) Prioritize ICT investment in development assistance policies and programmes;

d) Enhance synergy, economies of scale and productivity through the co-ordination of initiatives that deploy or rely on ICT;

e) Create a favourable environment for cooperation and partnership in ICT between the faculties/departments and units in Tansian University;

f) Empower and facilitate Tansian University staff in participating in National

Universities Commission (NUC) and in the global knowledge society activities

This ICT Policy as it relates to Tansian University is aimed at amongst other things address the vision, goals, principles and plans that guide the activities of the University in performing its statutory responsibilities effectively and professionally.

There are some basic ICT Policy Objectives that should drive this initiative.

Some of the basic objectives are stated below:

1. To re-engineer and improve upon the existing ICT human and material infrastructure in the University

2. To enhance the effectiveness of human and ICT resources in the monitoring, control and updating of the National Universities Commission policy

3. To integrate ICT mentality in the staff/students of the University and setup an enduring modern infrastructure in the University

4. To encourage and ensure continuous updating of ICT Systems and infrastructure and also human capacity building

5. To adopt a uniform, holistic and activity driven procurement of ICT Hardware

and Software in collaboration with other faculties/departments in the University

6. To encourage and guarantee the periodic monitoring, supervision and maintenance of ICT Systems and infrastructure in the University

7. To ensure that all technical issues about ICT resources emanating from faculties/departments in the University are channeled to the Director of ICT for appropriate action and resolution

8. To ensure timely and critical backup of data, systems files and other relevant information in the University

9. To strengthen and periodically update the Computer Systems and e-Library

10. To strengthen the existing Computer System laboratory/Maintenance Unit

1.8 Organogram and Spread of ICT centre

The ICT centre (ICTC) is a service and technical centre and had been collaborating with all the faculties/departments of the University on all ICT resources in the Oba and Umunya campuses. However, with the new dawn and dispensation in the University, the ICT centre should be empowered to monitor, service/repair, update hardware and software in all locations of the University where ICT resources and infrastructure are installed.

The two sections of the ICT centre are committed to helping the University meet its statutory, legal and National Universities Commission (NUC) obligations by administering its information expertise in a lawful, ethical, and cost-effective manner.
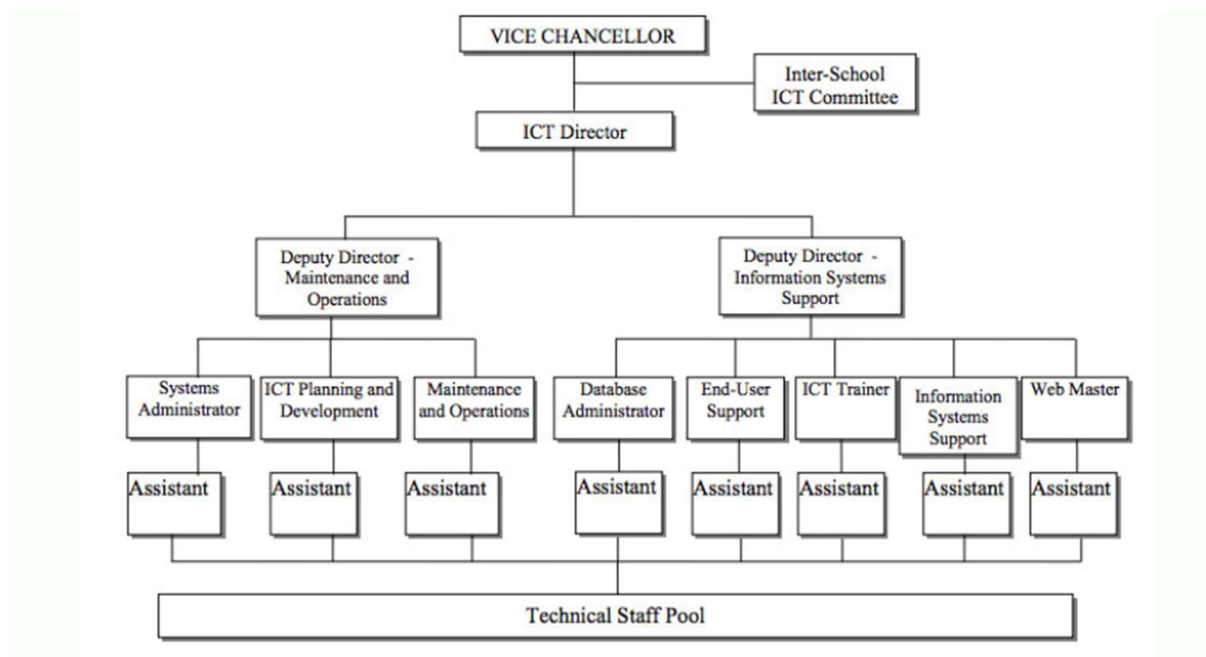
A Draft Policy report is prepared by the ICT centre and this report is expected to be a benchmark and a reference document for the implementation all ICT related activities in the University. The ICT centre has two sections namely:

- Maintenance and Operations
- System Administrator
- Planning and Development
- Maintenance and Operations

- Information Systems Support
- Database Administrator
- End-user Support
- ICT Trainer
- Information Systems Support
- Web master

The responsibilities of the ICT centre towards the University's ICT goals and operations include:

a. Procurement of ICT hardware, software, peripherals and infrastructure of the University

b. Installation and maintenance of ICT equipment, software and infrastructure in the University

c. Design, development and installation of relevant software for the smooth implementation of the University's mandate of promoting learning and research

d. Conduct ICT training primarily for university staff on the operation and

application of ICT equipment and software

e. Ensure efficient operation, supervision and maintenance of the Computer Resources

f. Ensure effective operation of all ICT equipment and infrastructure in the University

g. Ensure effective Network/Data Security, data integrity, data transfer, backup and recovery system

h. Continuous updating and maintenance of the University's website

i. Advice the University on ICT related issues generally such as Department and unit infrastructure like desktop, laptops, notebooks, ipads, tablets, computing facilities and Internet services, Liquid Crystal display (LCD) projectors and laptops for lecture rooms, e mail services, access to digital library (e library) resources,

Computer laboratories (Computer Science, Information Management Technology), Computer for offices, application software, alternative power supply system, Solar inverters, power surge, thunder protectors, other ICT related systems.

ICT centre provide ICT related services to all the faculties/departments and units of the University. Ensuring professionalism, effective management, uniqueness and control of all ICT equipment/resources and infrastructure is very important in the management of ICT systems. Procurement of information systems (IS), ICT equipment, software, software development, and consulting services, shall be carried out in accordance with the applicable "Procurement Manual and Guidelines" of the Project and Procurement unit or any successor thereto, and in accordance with other related regulations.

Guidance from ICT centre is to be obtained in relation to the operational aspects of procurement. The ICT centre should ensure the following before the procurement or purchase of ICT equipment and resources in the University:

i). A bi-lateral meeting between the beneficial or client faculty/department/unit and the ICT centre to determine the appropriate ICT specifications, manufacturer, model and quantity before any formal request is initiated.

ii) A technical team or Committee should be constituted by the client faculty/department and the ICT centre to look at all the issues relating to the procurement of ICT equipment and systems and submit its report and recommendation to the Dean/Head of Department of both entities.

iii)The Vice Chancellor should adopt or approve the purchase of the equipment or systems after the approval of the client and ICT centre.

SECTION TWO

2.0 ICT Resources

2.1 ICT Technical Evaluation Committees

Composition of Technical Evaluation Committees (TEC): In major ICT projects, the Composition could include one person nominated by ICT centre. The relevant faculty/department should request a nomination from ICT centre, in this regard.

2.2 Contractual Issues in procurement

2.2.1 Hardware:

Tansian University when procuring hardware should ensure that appropriate warranties are obtained and also ensure that warranty terms are adequate to take care of defects. Maintenance terms for the hardware after the warranty period should also be negotiated in advance, and should include escalation costs and availability of spares for the life period of the equipment.

Specifications:

Specifications should address scalability. Flexible and extensible systems architecture is recommended. The terms used in the specifications should be technology neutral.

2.2.2 Software:

Licensing: Tansian University should use only licensed software; such licenses can be for either proprietary software, or for open-source software. Use of software without a valid license or making modifications and carrying out customizations to licensed software without adhering to the license conditions would be contrary to the Intellectual Property Act of 2003 and would result in legal penalties (both criminal and civil liability)

Warranties: When securing proprietary or commercial open-source software, Tansian University should ensure that the warranty terms would include a statement stating that the software would conform to the stated specifications and that the software would adhere to the required quality assurance standards. The warranty period should be negotiated in advance.

Maintenance: Support and maintenance of software which was under warranty beyond the warranty period as well as the level of service should be agreed upon

in advance with the solutions provider. Procedures and terms for support and maintenance of software, and future modifications should be planned and documented in advance.

2.3 Intellectual Property Rights

Adherence to Intellectual property (IP) laws to protect owners, inventors, and creators of intellectual property from unauthorized use.

In the deployment of software solutions in universities there is likely to be several options available. Some of the options available would include:

(a) Procurement of retail or "common off-the-shelf" software

(b) Customization or modification to existing licensed software

(c) Provision of "green field" or "built from scratch" software

In the case of option (a) above it is essential to ensure that appropriate licenses fees are paid for, if required. If payments are required and a large number of users are involved, "bulk" or "volume" licenses could be negotiated with the Software provider.

This would entail costs which should be planned and budgeted by the entity concerned. In the case of option (b) above, Tansian University faculties/departments or units could hire software engineers or Service Providers to modify or customize the licensed software. It is important to require the Service Provider to adhere to license conditions imposed by the creators or owners of such Software

Note: There would be service or customization cost involved in modification or carrying out customizations to this category of software, which should be budgeted by Tansian University. Some of the license categories under this option could provide access to the Source Code, enabling the Tansian University to maintain the software using its own resources or a Service Provider or Software Engineers. Replication or re-deployment under this category could take place without incurring license fees, although costs may have to be incurred in respect of services.

In relation to option (c) above, the ownership of Intellectual Property rights would depend on the Agreement between the parties. Such an agreement may include two

options:

(i) Total ownership of Intellectual Property Rights

(ii) Joint ownership of Intellectual Property Rights

If the option (ii) is exercised, Tansian University could have access and ownership to the source code upon completion of the software warranty period, provided that the source code is managed through a "source code management repository" arrangement to be agreed by the two parties. Software developed in this manner would enable both Tansian University and the Service Provider to revise, further develop, replicate or deploy without any restriction after the warranty period.

If the Tansian University is providing significant input to the design of the software it could exercise the right to have total ownership.

If business methods or work routines (confidential or otherwise) belonging to the University are to be included in the Software Development activity, then, appropriate non-disclosure terms should accompany the Software Development Agreement (clearly identifying such components). Non-disclosure agreements should be signed with individual software developers, in addition to being signed with the solutions provider.

2.4 System Development and Management of ICT Resources

One of the most tasking, difficult and important responsibilities of the ICT centre is the system development and management of human and ICT resources in the University. This section will look at the following important areas:

1. System Development, Maintenance and Documentation

2. Network management

3. Physical and Environmental Security

4. Operational Security Management

5. Protection against Viruses, Spyware and Malicious Code

6. Electronic Access Controls

7. Internet, Social Media Networks and Email Use and Control

8. System Monitoring and Privacy

9. Penalties and Discipline

10. ICT Policy, Monitoring and Review

2.5 System Development, Maintenance and Documentation

The ICT centre will ensure that security controls will be implemented during all stages of system development, as well as when new systems are implemented in the operational environment. Such controls will be commensurate with the security classification of the data or information contained within, or passing across information systems, networks infrastructures, and applications. Security controls and requirements for new systems, together with security controls for improvements to current systems, will be identified and documented. Appropriate and adequate planning, testing, and system migration control measures will be carried out when upgrading or installing new systems and software, as a means to ensure the integrity and security of the information resource environment is not adversely compromised or affected.

2.5.1 Network Management

The ICT centre will deplore security measures to protect the University's networks and infrastructure from unauthorized access, and to safeguard data and information integrity and confidentiality. Adequate network access controls will be in place for the prevention, detection, removal, and reporting of attacks of malicious and mobile code, and for the detection of breaches and intrusion attempts. These controls will help ensure that information integrity and security is maintained.

2.5.2 Physical and Environmental Security

Physical entry controls will be in place for areas used in the processing and storage of sensitive data or information. To prevent unauthorized use, tampering, or interference, servers and other critical and/or sensitive equipment will be located in secure areas with access control mechanisms in place to restrict access to authorized staff only. Particular attention and care will be paid to provisions for the secure removal of information when disposing of, or re-using, equipment or storage devices.

2.5.3 Operational Security Management

A basic Operational Security Management ethics code will be developed by the ICT centre to ensure operational procedures and controls will be documented and implemented to ensure that data, information systems, and networks are managed securely and consistently, in accordance with the level of required security. Compliance with all aspects of this documentation will ensure the integrity of the operational environment when information systems and the network are implemented or changed. The Operational Security Management Standard ethics codes or rules for all staff of the University will be segmented into different parts and all staff are expected to familiarize themselves with the document:

a. ICT Standard Codes/Rules for the use of University ICT Resources

b. ICT Standard Codes/Rules for the Procurement of ICT Equipment and Resources

c. ICT Standard Codes/Rules for Computer Passwords and System Access Controls

d. ICT Standard Codes/Rules for Operational Security Management

e. ICT Standard Codes/Rules for the Repair and Maintenance of ICT Equipment and Resources

f. ICT Standard Codes/Rules for the Use of Internet, Social Media Networks and Electronic Mails

2.5.4 Protection against Viruses, Spyware and Malicious Code

The ICT centre will install adequate security controls for the protection of information and systems against viruses, spyware and other forms of malicious code. These controls include processes for the prevention, detection, and removal of malicious code in the information environment. Tansian University staff should familiarize themselves with the relevant ICT Standard ethics document on malicious software protection.

2.5.5 Electronic Access Controls

The ICT centre will ensure that control mechanisms based on university approved access requirements are put in place for controlling access to all, information systems, networks (including remote access), infrastructures, and applications. This access control rules will include:

Network Access

 Operating System Access

 Application Access

2.5.6 Internet, Social Networks and Email Use and Control

The ICT centre will control and monitor the use of Intranet, Internet, social network media and email usage by staff. Staff of the University with internet access must recognize that personal responsibility and accountability for the security of the University data or information and information systems/services is the shared responsibility of all users. ICT Standard ethic control code document will be the guiding mantra for all staff and Students using the Intranet or Internet and everyone must understand and acknowledge that the general principles of law and NUC standards apply to communication and publishing via the Internet. Staff/Students should bear in mind that actions taken by them using the network and Internet resources of the office places primary responsibility and obligation on university as a corporate entity.

Staff/Students should also be aware that there are legal sanctions for the improper use of the Internet, and that some uses may constitute a criminal offence.

2.5.7 System Monitoring and Privacy

The ICT centre on behalf of the University will routinely monitor traffic on Tansian University networks. Log files obtained from monitoring operations will be used for capacity planning, performance measurement, security, accountability, and evidentiary purposes. The Tansian University respects the right to privacy of its staff; however, where there is abuse, or suspected abuse of networks or networks facilities and services, the University retains the right to inspect all University owned ICT devices, together with all files, messages, and log files contained on those devices, to investigate such abuse or suspected abuse. The following ICT Standard ethics code or rule will apply for such cases:

a. ICT Standard Codes/Rules for Computer Passwords and System Access Controls

b. ICT Standard Codes/Rules for the Use of Internet, Social Media Networks and Electronic Mails

2.5.8 Penalties and Discipline

The Management and Senate of Tansian University shall enforce this ICT Policy and failure to comply with the terms may result in disciplinary action and process as determined according to the ICT Standard ethics codes that will be approved by the senate of Tansian University. Conduct in contravention of this policy may also constitute an offence or crime under the appropriate NUC law or legislation, resulting in legal prosecution. Irrespective of whether the violation is an internal (e.g. unauthorized access to information) or external (e.g. unauthorized remote access to University's network by a non-staff or student), where the violation is considered a criminal offence, the Economic and Financial Crimes Commission – EFCC or Police will be informed.

2.5.9 ICT Policy, Monitoring and Review

The Director, ICT centre will be responsible for monitoring, reporting, and review of this policy. He or She shall ensure that:

1. This policy should be reviewed at least once each calendar year because of the dynamic nature of ICT

2. Compliance with this policy is monitored and audited on a regular basis, as determined by risk assessment

3. The effectiveness of this policy is reported to the Management and Senate by the Director ICT centre

4. The review cycle will be dependent on a number of factors, including the level of risk and the rate of change.

2.5.10 Other promptings for renewing this policy include:

i. Changes to departmental operations, including the implementation of new systems

ii. Organizational change

iii. Emergence of new risks

iv. Changes to technologies.

2.6 Repair and Maintenance of ICT Resources and Infrastructure

One of the most important responsibilities of the ICT centre is ensuring that all ICT equipment, resources and infrastructure are working optimally. Constant replacement of worn out or bad hardware parts and maintenance of hardware systems will help in achieving the desired goals of the University. This section will look into the repair and maintenance of ICT resources and infrastructure in the University.

2.6.1 Systems Repair and Maintenance

The ICT centre is responsible for ensuring the smooth operation and working condition of all ICT resources and infrastructure in the University. The ICT centre should be empowered to perform the following functions:

A. Provide information about the physical status of ICT resources and software, networks, and the infrastructure, both in times of normal use and in the event of failure or unforeseen loss of data or information.

B. Undertake scheduled routine equipment and system repair or maintenance services in addition to regular software updates of relevant system and application software. An annual maintenance calendar should be developed for all the ICT resources and systems in conjunction with the client faculty/department/unit.

C. Critical or emergency repair or maintenance sessions may be carried out at any time to safeguard critical equipment and systems from data or information loss or damage.

D. ICT Support: Website, educational portal and application portals, laptops, desktops, printers, accessories

E. In addition, equipment protection like UPS, voltage regulators. All buildings with active devices such as access points, towers and antenna should be properly earthed and checked routinely

2.7 ICT Governance

2.7.1 Roles and Responsibilities within the ICT centre:

The ICTC should be responsible for the information and communication technological operations of the University, for outsourced ICT projects, and be responsible for managing the implementation life-cycle of such projects.

2.7.2 Responsibilities of Director of Information and Communication technology: The DICT shall be responsible for the promotion and development of ICT within Tansian University, and shall be the interface in respect of ICT related programmes and projects on which the Tansian University is interconnected with other Universities. DICT should liaise on the Tansian University's implementation of e-government with the designated person at ICTC at least once every three (3) months or as and when necessary. The following teams should report to the ICTC Head: Technical operations, Project Management and Outsourcing, Planning and ICT Policies, Business Operations, and Outsourced vendors who provide services to implement and operate ICT systems. Tansian University should draft and implement an annual ICT plan which utters the way in which ICT is to be used in realizing the vision and mission of the University. The plan should include the annual plan for ICT procurements. The ICT plan could be part of the main business plan of the University. The plans should be made available, as far as possible, to other faculties/departments/units to minimize the risk of overlap and to maximize the reuse of ICT solutions.

2.7.3 Information Lifecycle Management

The Tansian University shall be committed to complying with relevant record keeping laws, regulations, and standards, which will apply to all records regardless of format, including paper and electronic records. In order to achieve the completeness of the data set, all such data should be transliterated and translated to English language and stored in English Language, regardless of the data input and capture language.

2.7.4 Migration into electronic format:

Data available in Tansian University to be collected, inspected, updated, structured in the required format, and cleansed and its integrity ensured before being migrated into electronic format.

2.7.5 Retention of records:

The information created and stored by the University's information systems must be retained, stored and archived, in conformity with the relevant provisions of the National Universities Commission/Archives and any amendments thereto. The relevant guidelines of the International Council of Archives (ICA) pertaining electronic storage of documents adopted from time to time by the National

Archives Department shall also be complied with. Electronic records should be retained in such a manner so as to retain their accessibility and usability, integrity and authenticity, and their legal admissibility and evidential weight.

Electronic records should be maintained in such a manner to ensure confidentiality and prevent unauthorized access, modification, alteration or deletion / removal. Electronic records should be maintained in such a manner to ensure that they are complete in content and contains the related information necessary for the organization's business and transactions. Information systems should meet with available standards for internal and government audit requirements and with the relevant provisions of the National Archives Act and any amendments thereto. Data migration between platforms: Tansian University should develop a preservation strategy that ensures accessibility and scalability to ensure seamless migration of existing records between technological platforms as software and hardware get replaced. Use of open standards, where the specifications are public and without restrictions in their access or in implementation, for preservation are recommended.

2.7.6 Meta data standards:

Information should be retained to ensure maximum consistency of metadata across the University. Representation of dates and time in documents: Dates, time and time zone should be specified as in ISO 8601 – the international standard for representation of dates and time. The international standard date notation is; DD-MM-YYYY, where YYYY is the year in the Gregorian calendar, MM is the month of the year and DD is the day of the month. The international standard notation for the time of day is hh:mm:ss. The Tansian University shall ensure all staff/student is aware of the Tansian University's electronic record-keeping requirements; and required training for staff shall be provided.

Requirements for retention/ preservation of records in electronic form as well as requirements for originality in the context of electronic documents are prescribed under the Electronic Transactions Act. Electronic records shall be deleted/destroyed only under the normal administrative practices of the University, and in compliance with the applicable laws and regulations.

2.7.8 Protection of personal data

The Tansian University should handle personal information on staff/students in conformance to the relevant laws, codes of practice, regulations, and standards. Personal data and information should be retained in the manner and for as long as it is required as per laws, regulations and rules governing such data and information. Such data and information should be divulged only in accordance with rules and regulations governing such release. (The Data Protection Code of Practice when available would provide appropriate guidelines). Email addresses of staff and students gathered from Tansian University web sites should not be divulged, made available or sold to third parties. Personally identifiable information obtained through Tansian University web site shall not be kept for longer than is necessary for the purpose for which it was obtained.

SECTION THREE: HUMAN CAPACITY BUILDING

3.0 Recruitment and Capacity Building

Transformation of the ICT centre through recruitment and competence development of personnel. Recruit IT professionals to close identified gaps to better equip the ICT personnel with the requisite skills needed to effectively manage the ICT function and information delivery in Tansian University.

This document details the programme development, roll-out, and support services, including tailored courses in ICT and demand-driven training, research, and sharing of best practices through case studies and a "Briefing Notes" series. Key lessons learned on a national level and good practices derived from ICT's approach to ICT human capacity building for development include:

 Develop needs-based programmes

 Adopt a participatory and inclusive approach

 Invest time and resources into identifying and nurturing champions to roll out the training at all levels

 Promote the incorporation of programmes at Tansian University ICT capacity building framework

 Localize training materials to suit local context and specific groups

 Diversify delivery channels

 Establish knowledge sharing platforms and facilitate dialogue

 Promote synergistic partnerships

 Maintain rapport with partners

3.1 CAPACITY BUILDING

a) Increase the size and quality of ICT-skilled human resource base in Tansian University

b) Expand and develop formal and informal education and training;

c) Use ICT to improve the quality of delivery of Tansian University services;

d) Expand digital literacy programmes, notably for retraining and re-skilling the existing workforce;

e) Build awareness among Tansian University staff and students that ICT"s opportunities for spurring innovation abound;

f) Encourage and support ICT training for University Senate and management;

g) Give special attention to providing new learning and ICT access opportunities for all Tansian University staff and students;

h) Promote the broad development, diffusion and exchange of content that is indigenous or locally relevant

i) Develop and deploy a nationwide e-population activity that supports all location training facilities across the university by interconnecting them with each other and with relevant knowledge centres, providing curriculum integration while also generating information to better shape policies, strategic plans and tactical decisions for developing data collection, processing and dissemination in Nigeria.

j) Help increase the productivity of staff by enhancing Tansian University's intention to be a model user of ICT.

k) Empower the public by building a geo portal platform that facilitates their relationship and interactions with the public, and enhances the range and delivery of more effective services, while also generating information to better shape policies,strategic plans and tactical decisions for developing and enhancing the delivery of public services;

l) Promote good corporate and public governance by furthering information sharing, transparency, accountability;

m) Enhance public participation by reducing unnecessary red-tape within the University, and National Universities Commission;

3.2 Human Resource Development

Tansian University shall strive towards computer literacy being part of all programmes.

3.3 Needs Assessment:

Tansian University should carry out an assessment of the training and skills needed for all levels of staff and students to address the University ICT requirements on an annual basis. The Tansian University's ICT planning should include a component for ICT related training of employees.

3.4 Staff:

All staff including senior management and middle management staff in Tansian University must be competent in the use of ICT in their daily work, and necessary awareness and training should be provided to achieve this competency.

Senior management should implement suitable incentive schemes for staff that are proficient in ICT and / or obtain relevant qualifications in ICT.

3.5 Certification:

All staff in ICT centre should be encouraged to obtain National Universities Commission approved computer qualifications including membership of Computer professional of Nigeria (MCPN).

SECTION FOUR: ICT Policy implementation

4.0 ICT Policy implementation

The ICT centre will be responsible for performing the following functions among others:

 Advise the University on updating the Tansian University ICT Policy from time to time at least on yearly basis;

 Create, adopt and update legal and regulatory frameworks from time to time and submit proposals to Senate for action;

 Foster a harmonized competitive environment particularly in the public-private and community-based sectors;

 Design mechanisms to supply feedback on implementation issues for further policy formulation and review;

 Encourage the implementation of this policy, set targets and performance indicators, and monitor the progress of implementation;

 Provide mechanisms for faculties/departments to be involved in the implementation of policy, and the policy review and re-formulation process;

 Conduct and promote research into issues and ICT developments as the need arises, feeding the research results back into the policy formulation process;

 Monitor and react to issues of ICT and digital policy, regulation, development, technology and governance and global levels; and

 Become the focal point for coordinating ICT related activities.

4.1 CO-ORDINATION, IMPLEMENTATION MONITORING AND REVIEW

ICT centre will perform the roles of coordination, implementation, monitoring, evaluation and review of Tansian University ICT programmes and activities. Some of these activities may be conducted by outsourcing, or in innovative partnerships with private, public and non-profit sector organizations.

4.2 ICT investment prospects, funding and promotion

For the University staff to have real access to ICT services, various factors have to be considered: the cost of access; the opportunities offered by local infrastructure and adapted services and content; access to ICT projects

financing and status of the promotion of ICT. Other factors are suitable regulatory and legal framework; economic environment and political will.

4.3 Strategies for policy implementation

It is envisaged that strategies for the implementation of Tansian University ICT Policy would mainly be coordinated, monitored, evaluated and reviewed by ICT centre. Tansian University ICT programme of activities will be prepared in collaboration with other departments.

4.4 Communication Interface

Tansian University Web Portal and Web Site: Tansian University web sites to be developed to ensure interoperability and to maximize access and participation of users. The www.tansianuniversity.edu.ng Web Portal will be an integrated Internet based system to make available the latest, and a wide range of staff/student services and university information, from a single point. All departments or unit should ensure that their available web services can be accessed through the links on the University Portal.

Every department should make available information related to the University and all possible services using ICT, especially through the web. Content on the website of Tansian University should be relevant to the mission and vision of the University.

Content must be provided adequately and organized systematically. An open standard based content management solution should be provided to facilitate the content publishing work flow. It should support all popular web browsers and platforms.

Each department or unit should appoint a 'Content Management Team' (CMT) to approve the content on website. It should be headed by a Content Manager who could be either the DICT or another staff officer appointed by the university. Content Manager is responsible for keeping the contents regularly updated. An appropriate content management and publishing process should be adopted. Content on Tansian University website should be organized so that easy navigation for staff/student is facilitated.

Content that is obscene, misleading or offensive to any ethnic group, gender, accepted religion, culture or to any tradition should not be included in Tansian University web site.

All-important Tansian University policies, Acts, Regulations, Notifications, Circulars and forms should be made available through the relevant web site/portal and other appropriate electronic means. The language used in the websites must be simple, clear, unambiguous and easy to understand. There should be no linking to political sites from Tansian University. Tansian University should use their web sites as a means of promoting transparency by publishing information on the web. Tansian university's web sites should be interactive as far as possible, and requests for information made through web sites should be responded to as soon as possible after the receipt of the request. Tansian University should ensure sufficient security for their web sites to ensure the integrity of the information made available and to prevent unauthorized modifications, amendments, deletions, and other malicious attacks. Tansian University should post documents; i.e. circulars, publications, white papers among others on the University web sites in standard portable document format for web (e.g. PDF files) with appropriate security settings to prevent unauthorized modifications. The web browser should be adopted by Tansian University as the key interface for access of university information systems; other interfaces to be used if necessary, in addition to browser-based ones.

i. Development and implementation of a website (dynamic) that is interactive with web pages, Portals for admissions, fees collection among others.

ii. Development of Students records (Examination results, Transcripts among others.

iii. Development of Indigenous Computer Based Tests(CBT) Software

iv. Development and implementation of electronic smart identity cards for staff and students

v. Internet (Intranet and extranet) available on campus to enable staff and students carry out research, access information and carry out online course registration

vi. Development of on-line application system

vii. Capacity building for staff

viii. Provision of @ tansianuniversity.edu.ng e-mails for staff and students.

ix. Result/Transcript processing

x. Automation and generation of matriculation numbers verification of O'level Results for prospective students.

xi. ICT Support for various units/Departments via Help desks services, network/information security, training, ICT equipment maintenance, advice on ICT hardware and software procurement, harmonization of ICT infrastructure on campus

x. Introduce non degree/ industry-based course.

4.5 Contact information:

Tansian University websites should publish all possible contact information of the principal officers, Dean of faculties, Directors, Head of Departments or units comprising email address, phone numbers and office address and contact person / designation. Copyright and Disclaimer notice: A notice on copyright and a disclaimer stating that all materials provided on Tansian University sites are provided "as is", without warranty of any kind, either express or implied, including, without limitation, warranties of merchantability, fitness for a particular purpose and non-infringement, to be posted on the web portals. Tansian University should migrate towards overall consistency in design of their web sites.

4.6 Networking and Connectivity

Tansian University email shall be used productively and the rules and regulations that apply to other forms of communication shall apply to email.

4.7 Email:

It is recommended that emails on the Tansian University's domain are used only for the University purposes. All official electronic communications should be carried out using the official email address. Content that is obscene, misleading or offensive to any ethnic group, gender, accepted religion, culture or to any tradition of Nigeria should not be sent out, and any form of harassment should not be carried out using emails on the www.tansianuniversity.edu.ng domain. Emails on the Tansian University's domain should not be used for sending out unsolicited email messages unrelated to the academic goal of the University.

Retention and deletion periods for emails should meet University's requirements, legal requirements and the requirements of any relevant circulars. University filing procedures used for paper documents should be used for email

communications – the procedures, if decided on, could be electronic procedures. There should be a common email address for the University in the format info@tansianuniversity.edu.ng to be used for public communication purposes. Departments, units, should ensure that this account is checked frequently and mail directed to the relevant officers with minimum delay. The University should designate a person to be responsible for checking and relaying to the appropriate officers, and for responding, if necessary, email sent to info@tansianuniversity.edu.ng.

Each department should adopt the following nomenclature in providing email addresses to staff; i.e. the user name should be standardized and the domain should be tansianuniversity.edu.ng; the nomenclature recommended is as follows:

For officers whose schedules are transferable:

designation@tansianuniversity.edu.ng

 for the officers who are permanent to the university: firstname.lastname@tansianuniversity.edu.ng.

For non-staff officers: initials.lastname@tansianuniversity.edu.ng

Designation based emails must be accessible by the relevant person's designated assistant in order to enable prompt response in the absence of the officer to whom the mail is directed. An email address should be provided for employees as decided by Tansian University. University emails should include a standard official signature: name, designation, department name and contact information and Tansian University's URL. Emails should contain a standard disclaimer.

The writing style used in business e-mails should be consistent with other forms of the Tansian University's written communications. e-mails should be responded to, as far as possible, in the language (English) in which they are received.

Attachments: When sending attachments, the precautions specified in the Tansian University Information Security Policy should be followed. The University has the right to assign, monitor, and delete any email account or content within purview of the organization.

4.8 Desktop Systems and Mobile Computer Devices/Systems:

Installation of software on desktops should not violate intellectual property rights. Only the systems administrator or an authorized person should have the authority to install software applications. Tansian University should standardize on a single user-platform (operating system) within the University.

It is recommended that PCs, laptops and handheld devices assigned to employees should only be used for relevant official work. Tansian University should ensure that all computers and mobile devices are regularly updated with the required security patches.

4.9 Web Presence

Internet / Intranet:

ICT centre should implement policies to guide users on Internet/Intranet usage. The use of internet should comply with the policies and codes of conduct of the University. Information access restrictions applicable to physical files should be applicable with better audit trails and security to information available via the Intranet.

Exams and Records

. Interactive dynamic university website with web pages, portals for admissions, fees collection among others, https://tansianuniversity.edu.ng Student records (examination results, Transcripts...,) which is part of the university e portal https://eportal:tansianuniversity.edu.ng

. result/transcript processing is also part of the School e-portal https://eportaltansianuniversity.edu.ng. Development of indigenous Computer based Tests(CBT) software

Admissions

. on-line application system which is also built in the university website https://tansianuniversity.edu.ng/admissions.php# online-application

. automation and generation of matriculation numbers verification of O'level results for prospective students

. development and implementation of electronic smart identity cards for staff and students linked to the e-portal for verification and authentication

Registrar's office

. @tansianuniversity.edu.ng email for staff and students which is created and dispatched with strict instructions from the university management because of information security

Bursary

. online payment system which is also part of the school websitehttps://tansianuniversity.edu.ng payment.php

4.10 Tansian University Network Connectivity:

All faculties/departments whether in Umunya or Oba campus should connect to the common Tansian University Wide Area Network infrastructure

4.11 LAN Account Management:

LAN accounts should be created only after clearance by the University's Senate/management and disabled on the same day of employee's departure from the University. Departments or units should define a standard format for the LAN accounts and for the names of the PCs and servers in the network.

4.12 Backup Measures:

The University departments and units should identify and document its critical processes relating to its core business, and the critical assets and resources involved in the University processes. A plan should be developed and implemented to ensure the safety of personnel and organizational property including data and information processing facilities. Adequate backup facilities should be provided to ensure that all essential information and software can be recovered following a disaster or a media failure.

5.0 SECTION FIVE

5.0 Benefit to the University

Benefits of Implementing e Governance Services in Tansian University, Umunya. The University should accept the following factors, which are intrinsic to e-Government, as key principles on which ICT solutions will be implemented. These issues are addressed in the body of the Policy and some issues are addressed in the Tansian University Information Security Policy, but are emphasized below.

Accessibility: Providing information and departmental services over the web and ICT channels will make them available to all stakeholders. Therefore, all possible measures should be taken to make the services accessible to all without discrimination. It is essential that all staff/students including differently-abled persons should be taken into account while devising e-government solutions.

Transparency: ICT based solutions should improve the transparency by allowing the pubic to monitor the mission of the University, functionality, decision making processes, the progress of a process at different stages and clearly informing them of the type and the quality of the services they obtain. The e-governance models should always encourage transparency within the University.

Efficacy: It is important that the services provided by the University using ICTs, meet and exceed the expectation of the stakeholders. The efficacy at which the services offered should be a key factor that determines the quality of the services provided through using ICTs.

Efficiency: Services should be available to the public within the minimum possible time. A concept popular in e-government solutions are "same day service"; where a service requested by a citizen in the morning should be made available to him/her before the end of the same day. Although it is difficult to expect this level of delivery from every service from the inception, the University is expected to provide citizen services efficiently so that the public is not made to wait for the services requested. Staff/Student centric: In providing information and services, the University should establish a staff/student centric approach instead of a traditional organization centric approach. In order to do so, Tansian University should reengineer their processes to convert the University to "one stop shops" thus making their services citizen-friendly.

Stakeholders should be able to then obtain services through submitting minimum necessary supporting documents.

Interoperability: The University should ensure when implementing ICT programs are interoperable - enabling electronic data sharing and data exchange between different systems - throughout the University, and also with the National Universities Commission and other key sectors. Confidentiality, integrity and availability: Tansian University should preserve the confidentiality, integrity and availability of the information within their purview. This entails that stakeholders should have the assurance that Tansian University information is shared only among authorized persons or organizations, that the information is authentic and complete and can be relied on for the purpose for which it is needed, and also that it is accessible when needed by those who need it. This area is further addressed in the government Information Security Policy.

Accountability: The Tansin University should be accountable towards the stakeholders and for the services provided, so as to foster confidence in them in the use of such services.

ANNEX

A.1 STRATEGIC ICT LEADERSHIP

Tansian University's ICT environment has hitherto lacked a focused ownership and authoritative guidance that takes into account the nature of ICT itself. Initiatives have therefore been fragmented, while departments have been segregated at the cost of duplicated efforts, loss of potential synergies and unexploited economies of scale. Clearly, it is imperative that efforts be urgently dedicated towards building strategic oversight and leadership capability to bring cohesiveness to the ICT environment, otherwise it will be difficult for partnerships and collaborative efforts to develop. Such leadership will also help future initiatives to mesh with NUC priorities, be aligned to sector strategies and be in harmony with realities and expectations of stakeholders.

Faculties/departments also have roles to fulfil so that ICT can develop, and the Leadership element of this policy will be responsible for ensuring that such crossdepartmental issues are addressed effectively. Promoting broad-based awareness, with inclusive consultation processes, will be another task of Leadership, which will also have to encourage the expression of differing interests in order to build a viable consensus amongst the diverging priorities and time frames. Leadership is particularly important towards resourcing, to create an attractive fiscal environment for investors and consumers, to identify areas needing priority funding and support, and to obtain and direct resources from either internal or international sources for local initiatives. Consequently, leadership necessarily requires institutional development for organizations involved in ICT to have an established reference point, and for political and executive responsibilities to be assigned towards delivering this policy. Therefore, Strategic ICT Leadership is accorded specific emphasis within the University ICT policy.

A.2 LEGAL AND REGULATORY FRAMEWORK

Globalization and the pervasiveness of the Internet have given rise to new types of needs, rights and vulnerabilities associated with the new data types and technologies. For secure electronic transactions to occur, an environment of trust must be created and sustained through the legal and regulatory apparatus, taking cognizance of constitutional rights as well as the provisions of criminal, civil and commercial law. Meanwhile, cyber-criminals around the world are constantly

seeking loopholes through which to perform malfeasance such as transacting illegal or illicit businesses, perpetrating fraudulent affairs, propagating computer viruses, or gaining unauthorized access into networked systems. Any University which has inadequate cyber-law is essentially providing a safe-haven for cyber-criminals to act with impunity, a situation which is detrimental to Tansian University on the basis of trustworthiness of all of its electronic transactions. Therefore, Tansian University urgently needs to create and sustain a secure cyber-law environment, in addition to Intellectual Property Law, before any significant new developments can emerge in service areas. Therefore, the Legal and Regulatory Framework is emphasized in the context of the Tansian University ICT policy.

A.3 HUMAN CAPITAL

Tansian University like other Universities are not so blessed with skilled and experienced experts in ICT and in other professions that rely on ICT. It is therefore necessary to view Tansian University's human capital needs in the global context, wherein the brain drain is a fact of life in all professions and fields that rely on, or are enabled by, ICT competence. Hard choices must be made between either rapidly importing needed skills, or slowly nurturing them within our own University – even at the risk of a subsequent "loss" into the Nigerian Diaspora. Other choices are needed on the priorities in the composition of competencies that are most urgently needed and on realigning the educational and vocational training pipelines to provide appropriate exit-points that satisfy the current needs of the University.

In addition, we cannot afford to ignore the new opportunities for applying ICT to enhance education opportunities for self-improvement, life-long learning, distance learning, etc., for teaching not only about ICT, but for all courses and specialisations. If embraced appropriately and supported at all levels, these could transform the Tansian University's human capital. With the increasing need for professional versatility arising from convergence, our traditional education and training institutions are otherwise going to be hard pressed to meet the growing demand for multi-skilled operatives, knowledge workers, and the so-called "hybrid managers". Therefore, Human Capital is central to the Tansian University ICT policy.