Kampala International University, Uganda

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) POLICY

July 2023

Preface

ICT (Information and Communication Technology) plays an important role in universities as it helps to enhance teaching, learning, research, and administration. ICT tools, such as learning management systems, online databases, and video conferencing software, can facilitate distance learning and make education more accessible. Additionally, ICT can be used to support research by providing access to online journals and databases, as well as tools for data analysis and visualization. It can also be used to improve administrative processes and communication within the university. Overall, ICT can help to improve the effectiveness and efficiency of the university's operations. Hence, ICT resources remain central to university functions, activities and roles.

ICT policy in a university typically outlines guidelines for the use of technology within the institution. This can include rules for the acceptable use of computer systems and networks, guidelines for information security and data privacy, and policies for the use of social media and other communication tools. This policy will also help in addressing issues such as e-learning, online course management, and the use of mobile devices on campus. The goal of this policy is to ensure the responsible and effective use of technology to support the university's mission and goals.

The KIU has set out this ICT policy to ensure the efficient and effective use of technology in support of the university's mission and vision. This policy should serve as a guide for proper monitoring and control of ICT facilities, and outlines guidelines and frameworks for the integration of ICT into teaching, learning, research, and information management. The ultimate goal is to bridge the knowledge and technology gap within the university and provide access to global information for the entire university community.

Prof. Dr. Mouhamad Mpezamihigo
Vice Chancellor,
Kampala International University, Kampala.

Table of Contents

Definitions and Acronyms

KIU: Kampala International University.

Access Point: An access point (AP) is a device that allows wireless devices to connect to a wired network. It acts as a bridge between a Wi-Fi-enabled device and a wired Ethernet connection. An access point connects to a router, switch, or hub to allow multiple devices to share the same network connection. APs have a range of features, including support for different WiFi- standards, the ability to provide multiple SSIDs (virtual networks), and security options like WPA or WPA2 encryption. Access points are commonly used in homes, offices, and public places to provide Wi-Fi connectivity to users.

Centralized Distributed System: A collection of independent computers that appears to its users as a single coherent system. A distributed system consists of a collection of autonomous computers, connected through a network and distribution middleware, which enables computers to coordinate their activities and to share the resources of the system so that users perceive the system as a single, integrated computing facility.

CRU: Computing Resources Unit, refers to a standardized unit of measurement for computer resources such as processing power, memory, and storage. The exact definition of a CRU can vary depending on the specific system or application, but it typically represents a unit of computational capabilities that can be used to perform a specific task. The use of CRUs can help organizations manage and allocate their computing resources more effectively, by enabling them to quantify the computational requirements of their applications and allocate the appropriate amount of resources. By using CRUs, organizations can also more easily compare and evaluate different computing solutions, and make more informed decisions about their IT infrastructure.

Council: The KIU Governing Council

Data: The quantities, characters, or symbols on which operations are performed by a computer, which may be stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media. Data is distinct information that is formatted in a special way. Data exists in a variety of forms, like text on paper or bytes stored in electronic memory.

Department: A unit within the KIU.

DICT: Directorate for Information and Communications Technology is the hub (i.e. coordinating organ) for all ICT activities. It is a statutory organ of the University vested with the authority to acquire, develop, deploy, and manage all ICT infrastructure/resources within the University, and to ensure that, the provision of ICT infrastructure and services is aligned with the University's academic and administrative direction and priorities.

ERP: Enterprise Resource Planning refers to software for managing day-to-day activities such as accounting, procurement and project management.

Faculty: A unit within the KIU with more than one Department.

Fiber Optics: Fiber optics is a technology that uses thin, flexible, transparent fibers made of glass or plastic to transmit data as light signals over long

distances. This technology is used in many fields such as telecommunications, medicine, military, and others due to its advantages over traditional metal communications lines, including immunity to electromagnetic interference, higher bandwidth, and longer transmission distances.

Financial Data: Refers to data, which contain information on University financial profiles such as revenue, expenditure, budget, assets and facilities.

ICT: Acronym for Information and Communication Technology. Examples are Software, Hardware, work and Internet services.

ICT Policy and Guidelines: A formal document adopted by the constituted authority, detailing principles, plans and procedures to guide all and sundry on ICT utilization.

ICT Infrastructure/Resources: This refers to all of the University's Information and Communication Technology Resources and facilities including, but not limited to: desktop computers, Laptops, printers, scanners, access labs or other facilities that the University owns, leases or uses under License or by agreement, any off-campus computers and associated peripherals and equipment provided for University work or associated activities, or any connection to the University's network, or use of any part of the University's network to access other networks.

Information: Refers to all records, documents and data whether computerized or not and all software whether developed by the KIU or otherwise acquired, that is owned by the University or entrusted to it for any purpose or used in the course of or associated in any way with the KIU's business activities. \

Information Management: Information management (IM) is the collection and management of information from one or more sources and the distribution of that information to one or more audiences. This sometimes involves those who have a stake in, or a right to that information.

Internet Service Provider: An Internet Service Provider (ISP) is a company that provides customers with internet access. They offer various services such as broadband, Wi-Fi, and dial-up connections. ISPs connect customers to the internet using technologies like fiber optics, coaxial cables, or satellite, and usually charge a monthly fee for their services. Some ISPs also provide additional services such as email, hosting, and virtual private networks (VPNs).

Library Data: Refers to data, which contain information on University library profiles such as subscribed journals, available print collections available special collections.

Network: Local Area Network within KIU, as well as access to the Intranet, Internet and other networks using KIU's facility.

NOC: NOC stands for Network Operations Center. It is a central location responsible for monitoring, managing, and maintaining a company's communication and information networks. The NOC is typically staffed by network engineers and technicians who are responsible for ensuring the reliability and availability of the network. The NOC is equipped with tools and systems for monitoring network performance, identifying and resolving issues, and performing routine maintenance tasks. The NOC plays a critical role in ensuring the smooth operation of a company's network infrastructure

and is essential for maintaining business continuity and preventing outages.

OSS: OSS stands for Open-Source Software. It is software whose source code is made available to the public, allowing anyone to use, modify, or distribute the code. Open-source software is typically developed and maintained by a community of volunteers, with contributions from individuals and organizations. Some popular examples of OSS include the Linux operating system, Apache web server software, and the MySQL database management system. The open-source model allows for collaboration, transparency, and innovation, and has become a popular method for developing and distributing software, particularly in the enterprise.

Personnel Data: Refers to information relating to staff characteristics (qualification, rank, pension accrued, compensations, salary and so on) and staff demographics (state of origin, age, sex, religion, marital status, department, and so on).

Research Data: Refers to all outputs of creative work undertaken on a systematic basis in to increase the University knowledge base and information.

VPN: VPN stands for Virtual Private Network. It is a technology that creates a secure, encrypted connection between a device and a remote server over the public internet. VPNs are used to provide remote access to a private network and to secure internet traffic, protecting sensitive data from being intercepted by unauthorized users. When a device connects to a VPN, all data transmitted between the device and the VPN server is encrypted, making it difficult for anyone to intercept or access the data. VPNs are commonly used by businesses to provide secure remote access to their networks, by individuals to protect their internet privacy and security, and by users to access content that may be restricted in their region.

VSAT: VSAT stands for Very Small Aperture Terminal. It is a type of satellite communication system that allows users to send and receive data, voice, and video over satellite links. A VSAT system consists of a small dish antenna (typically less than 1 meter in diameter) and a modem, which is located at the user's location, and a satellite in geostationary orbit that provides the communication link. VSAT systems are commonly used for remote and rural areas where terrestrial communication options are not available, for disaster recovery and emergency communication, and for applications that require mobility, such as maritime and aviation communication. The main advantages of VSAT systems include their ability to provide communication services in remote areas, fast deployment times, and high-speed, reliable data transmission.

VoIP: stands for Voice over Internet Protocol and is a technology that allows voice calls to be made over the internet rather than through traditional telephone networks. In a VoIP system, analog audio signals are converted into digital data packets and transmitted over the internet to their destination. This technology enables users to make voice calls using a computer, smartphone, or special VoIP phone, as well as make video calls and send instant messages. The advantages of VoIP include lower costs, increased functionality, and greater flexibility compared to traditional telephone services.

1. INTRODUCTION

1.1. Preamble

Information and Communications Technology (ICT) development over the last few decades has led to the convergence of broadcasting, telecommunications, computing, and content. It has impacted the way business is conducted, facilitated learning and knowledge sharing, and generated global information flows, empowered citizens and communities, resulting in a global information society.

Kampala International University (KIU) encourages the use of electronic communications to share information and knowledge in support of the University's mission and to conduct the University's business. The University support and provide interactive electronic communications services and facilities such as electronic mail, social networking, publishing services and internet services.

However, access to sensitive University information by unauthorized persons could result in legal liability, substantial financial loss, violation of privacy and embarrassment to the University. The Campus network, which connects to the outside world through the Internet, is not isolated from the potential of unauthorized access. With an increasing use of computers and networks on Campuses and with people worldwide having access to the University network, KIU must put in measures to regulate and protect access to institutional information and data.

Hence, the University requires an effective ICT strategy to enhance the smooth functioning of the University. An integrated policy cannot anticipate all the new issues that might arise in the course of developing, using and managing ICT. One purpose of this policy is to provide a framework within which these new issues can be recognized and resolved institutional-wise.

This policy document, therefore, is a necessary guide for developers, users and managers of information and ICT resources on appropriate standards, that conform to recognized international standards and industry best practice for adoption by KIU for the acquisition, development, usage, and management of ICT resources to ensure availability and proper use and utilization of ICT in the executing KIU functions.

1.2. Obligation

The Director, ICT is saddled with the responsibility of been the custodian of this policy, including keeping it under review, while students, staff and visitors have to comply with the provisions of this policy. Therefore, any requests concerning this policy or conducts and suggestions on improving it shall be directed to the Director, ICT.

1.3. Vision

To be an international center of excellence in ICT by promoting the use of ICT in teaching, learning, research and service delivery.

1.4. Mission Statement

To provide Information and Communication Technology support services to academic and non- academic activities of the University and community through computer training and services.

1.5. Objectives

The overall policy objectives are:

- to certify that, processes and rules for the selection and use of ICT in the University are observed by staff, students and visitors alike;
- to deploy active control arrangements, to form and advance ICT infrastructure for optimum application in teaching, learning and research;
- to harvest ICT literate students;
- to leverage the use of ICT in promoting and facilitating learning for the benefit of both learners and teachers across the curriculum;
- to invest in our students and staff the skills of ICT in tandem with the current global digital trend; and
- to safeguard the University from any legal implications arising from unethical use of the University's ICT infrastructure.

1.6. Scope

The ICT Policy will be governing document for all ICT-related issues in all departments and support units of the university. The policy covers the following broad areas:

- Security And Privacy
- Technology
- Finances
- Personnel
- Software
- Web
- Creative Commons
- Open Software
- Research
- Management
- Partnerships
- Enforcement and Sanctions
- Disaster Management
- Related Policies

The scope of this policy is split into these fourteen (14) broad areas which are sufficient in the quest to implement the mission and vision of KIU. This categorization intends to highlight important milestones which need to be reached in the policy implementation. These shall be further developed into projects defined in detail in the ICT Master Plan which shall simplify monitoring the progress of the policy implementation.

2. SECURITY

2.1. Security and Privacy

IT resources must be protected from unauthorized access and natural disasters such as fire, flood, etc. The University should ensure the security of data and equipment through adequate measures.

Policy

To protect all resources managed by ICT, appropriate security measures must be implemented. The head of the unit/faculty/center is responsible for securing resources outside of ICT's control.

Objectives

- To ensure the safety of sensitive data.
- To prevent the misuse of private data or information.
- To protect the University from legal actions with regards to data.
- To prevent the loss of resources to the University.
- To ensure only the authorized personnel have access to data.
- To ensure the integrity of Information and the processing method.

Strategies

- All devices connecting to the University Network must be registered/authenticated with the DICT.
- The administrator account and password should only be used for system administration purposes.
- Service account passwords must be changed when a work group member who could have known the password leaves the work group.
- Internal Internet servers deployed at KIU must be managed by DICT.
- Approved Internet server configuration guides must be established and maintained by IT staff based on business needs, approved by the Director, and monitored for compliance.
- Any changes to the configuration guides must be reviewed and approved by the Director, ICT.
- University systems vulnerable to malware attacks must be protected by Antivirus Software.
- All KIU records and software must be backed up and recoverable using a combination of image copies, incremental backups, differential backups, transaction logs, or other techniques.
- A minimum of one fully recoverable version of all KIU Records must be stored in a secure off-site location.
- Backup and recovery documentation must be reviewed and updated regularly to account for new technology, business changes, and application migrations.

- The frequency of backups must be determined by the volatility of the data and the retention period must be determined by the criticality of the data. At a minimum, backups must be retained for 30 days.
- Recovery procedures must be tested annually.
- All critical servers must be housed in a secure data center with adequate power backup.
- Security-related events must be reported to appropriate Information Security personnel who will review logs and report incidents to management-level personnel in the DICT.
- Security audits must be carried out regularly.
- Software installation on University IT systems must only be approved by the DICT.

2.2. Password Policy

A password is a secret word or combination of characters used to verify a user's identity and grant access to a specific resource. It must be kept confidential from unauthorized individuals. An access code is one example of a password.

Policy

Access to information technology systems and resources is protected by requiring a password.

Objectives

- To verify the identity of users on personal and official systems in the KIU Network.
- To secure the systems in the KIU against unauthorized access by outside parties.

Strategies

- For all University accounts, password/passphrase standards require that the password:
  - Consists of a mix of letters, numbers, and special characters that don't match previous passwords
  - Has a minimum length of 8 characters but a passphrase of 15 or more characters is recommended
  - Incorporates at least one constraint, such as avoiding strings that match previous passwords, consecutive, repeated, or sequential characters (e.g. aaaa1111, abcd1234), or single dictionary words.

- For additional password/passphrase requirements:
  - Elevated Privilege System Accounts: Accounts with the authority to manage a system or application, such as system or database administrator accounts, should have their own unique elevated privilege system account, and not be shared. Where possible, these accounts should use a managed authentication service like Active Directory, LDAP, or RADIUS. When accessing remotely, multi-factor authentication is recommended.
  - Elevated privilege system account passwords/passphrases must:
  - Meet the minimum password standards
  - Be changed at least twice a year, every 180 days
  - Have a minimum length of 15 characters when feasible.

- Local Workstation Administrator Accounts: The elevated privilege account standards apply to local administrator accounts, where the password is stored on the workstation and not dependent on central authentication. Each computer must have a unique local administrator password for computers under this policy. The local administrator account and password should only be used for system administration.
- Service Accounts: These are accounts with passwords managed within a work group, including device passwords. They must comply with elevated privilege account password complexity but are exempt from the change requirement. They should be reviewed annually and changed when a work group member who may have known the password leaves the group.

Other Requirements:

- For password reset procedures: Assisted Password Resets: User account passwords will only be reset if the password administrator can verify the identity of the user requesting the change/reset using one of the following methods:
  - A secret key or verifying personal information
  - Verification by a supervisor or tech support person
  - A photo ID or biometric scan
  - Satisfactory challenge-responses in a self-service application

- Policy Exception Process: Applications or services that don't meet the minimum standards may be granted exceptions with approval. The approval process requires the system owner to provide a technical description and justification for the exception.

2.3. Antivirus Policy

Antivirus or anti-virus software sometimes known as anti-malware software, is computer software used to prevent, detect and remove malicious software.

Antivirus software was originally developed to detect and remove computer viruses, hence the name. However, with the proliferation of other kinds of malware, antivirus software started to protect from other computer threats. In particular, modern antivirus software can protect from: malicious Browser Helper Objects, browser hijackers, ransomware, keyloggers, backdoors, rootkits, Trojan horses, worms, malicious LSPs, dialers, fraud tools, adware and spyware.

Policy

All University systems, vulnerable to attack by malware must be protected by antivirus software wherever possible unless a specific exclusion has been granted and alternative measures have been taken to provide the same degree of protection. Any system that is infected shall be denied access.

Objectives

- To protect the University information systems against viruses, Trojans and other malware.

Strategies

- Monitor the infrastructures and generate regular reports to ensure University clients are protected and kept up-to-date.
- Test and deploy new updates, patches and fixes as they are made available from the Anti-Virus company.
- Ensure OS security patches are deployed to minimize vulnerabilities.
- Track and plan for specific threats, as and when they become known, to limit the impact on university systems.
- The University shall acquire educational licenses for commonly used software on the University network.
- Departments that manage their computers are responsible for virus protection on these computers. This includes installing antivirus products, keeping them up to date, giving advice on their use, removing any viruses found and applying any updates necessary to defend against possible threats.
- All staff and students are responsible for taking suitable measures to protect against virus infection and failure to do so shall constitute an infringement of the University's regulations governing the use of computing facilities.
- The use of pirated or illegal software shall not be allowed on the University network.

3. TECHNOLOGY

3.1. Bandwidth Usage Policy

Bandwidth refers to capacity of the data that can be transmitted in a fixed amount of time. It is the maximum data transfer rate a network or internet connection can handle.

Policy

KIU shall be responsible for regulating the usage of the university's internet bandwidth to prevent congestion and slow connections

.

Objectives

- Ensure all authorized users have fair access to the Internet.
- Prevent flooding of the network with unofficial requests.

Strategies

- Users must have an account to use the internet.
- Multiple users cannot use the same account at the same time
- Data volume/size is allocated to each user periodically after payment.
- Access to heavily used sites (e.g. Facebook) and downloading large files may be restricted between certain periods of the day to prevent congestion.
- Any account causing excessive traffic congestion after repeated warnings is automatically blocked for certain periods.

3.2. Equipment Procurement Policy

There is a need for the Information Technology and media equipment procurement process to follow existing rules and regulations governing the procurement of goods and services for KIU, while also satisfying the technical specifications of the department involved.

Policy

Any IT equipment or services to be procured shall meet certain technical specifications as recommended by DICT and the need of the department where such equipment is required**.**

Objectives

- To ensure that various departments follow the correct procedure for procurement of IT and media-related goods and services.
- To assist the departments with the preparation of technical specifications whenever the need arises.
- To ensure that projects for various departments are pursued diligently and efficiently.
- To ensure that the goods and services to be procured is/are satisfactory and timely.

Strategies

- All purchases shall have technical approval from the Directorate and financial authority approval from the budget holder to whom costs will be charged;
- The Financial Instructions which govern the procurement of all goods and services within the University must be met. For example,
  - All purchases shall be suitable for the purpose for which they are acquired;
  - All purchases shall be of acceptable quality;
- Purchasing shall be sufficiently flexible to allow rapid response to operational requirements and to enable the user to take advantage of opportunities arising from new IT products or services;
- All products or services purchased shall be on the approved products list unless specific permission is given to purchase non-approved products.
- In acquiring Non-Branded Equipment, Software and Services, a brief initial business case shall be submitted to the Director of DICT.
- Equipment to be donated shall ordinarily meet all necessary technical specifications.
- Refusal or rejection of any benefaction(s) on grounds of obsoleteness, inefficiency or incompatibility with existing hardware shall be done with diplomacy i.e. when equipment is donated to the university.
- An Inventory of all the IT and media goods and services procured by the various departments shall be forwarded to DICT for record-keeping purposes.

3.3. Equipment Maintenance Policy

Maintenance refers to repairing a malfunctioning electrical device and performing regular tasks to keep it functioning properly and prevent damage. This encompasses all technical and administrative, managerial, and supervisory actions.

Proper equipment maintenance is crucial for delivering high-quality IT services, achieved by timely servicing and repairing. Software maintenance encompasses a wide range of activities such as fixing errors, improving features, removing outdated capabilities, and optimizing performance.

Policy

- All Information Technology and Media equipment shall be regularly maintained. The equipment may be owned, managed, supported or operated by, or on behalf of, the University.
- All equipment shall be identifiable individually.

Objectives

- To ensure that users' PCs and related hardware are in serviceable order
- To specify the best practices and approaches in IT equipment maintenance
- To ensure the integrity and security of the network
- To ensure the currency of the licenses

- To allow departments/units to plan for replacement technology well in advance of the dates outlined

Strategies

- Maintaining a detailed log of maintenance activities
- Assisting in IT procurement for hardware to guarantee support by IT.
- Drawing schedules for maintenance and recognizing every piece of hardware.
- Carrying out preventive maintenance according to the recommendations of the manufacturer of the hardware, in terms of frequency and method of maintenance. However, where justified by the case, service shall be provided based on request.
- Declaring IT hardware connected to the University network obsolete according to the recommendations of the manufacturer.
- Conducting periodical maintenance by the hardware maintenance team to identify, retire and replace the hardware categorized as at "end-of-life."
- Selling of old systems to students and staff at subsidized prices. Facilitating the repairs and maintenance of equipment under warranty by maintenance staff at the IT Unit
- Keeping accurate records of warranty of individual items of equipment and using such information when needed to operationalize the warranty and/or guarantee for the equipment by the maintenance staff at the IT Unit
- Developing Equipment Age Repair and Maintenance Policy
- Making every reasonable attempt where possible to repair the technologies described in the terms of this policy based on a specified period of years from the date of manufacture

3.4. Local Content Development Policy

Information Technology and Media can enhance Local Content Development at KIU through a dual strategy of software and hardware development. The software sector is a multi-billion dollar market and the university can gain greatly by establishing its local software ecosystem in partnership with an industry expert to develop applications for various fields such as Agriculture (e-Agriculture), Business (e-Banking), Education (eLearning), Governance (e-Government), Health (e-Health) and more. This will benefit both the university and external organizations.

Policy

- IT local content (including software and hardware) is grossly underdeveloped in KIU and Uganda as a whole. This has resulted in over-dependence on foreign importation of software and hardware, and diminished opportunity for economic empowerment and capacity building.

Objectives

- To position KIU as a leader in software development
- To provide incentives for the growth of the software ecosystem;
- To promote software development education in the University;

- To ensure rapid indigenization and domestication of high technology IT and media products and services; and
- To encourage the attainment of a significant increase in local content of IT software and services.

Strategies

- Ensure that in-house software meets international standards;
- Provide incentives and initiatives that will significantly increase the number of software developers within the next five years;
- Build a strong interface between the software industry, academia and also the business world to improve the relevance of the end product;
- Promote collaboration amongst software developers;
- Ensure that security and privacy in the software information system are maintained;
- Ensure that intellectual property rights are protected;
- Promote international certification of indigenous software;
- Encourage the creation of major software projects as a platform for the indigenous software industry;
- Promote the patronage of indigenous software products and services;
- Promote Free and Open-Source Software (FOSS) development, education, and use
- Digitize local content in areas such as music, film, tourism, etc.
- Digitize and make available online local content.

3.5. Network Infrastructure Implementation Policy

A dependable network requires proper IT infrastructure deployment and solid network architecture. To establish a network that can handle the transmission of video, voice, and data for the university community, a well-organized strategy and plan for network design, deployment, operation, and support is necessary.

The campus network consists of three layers to guarantee efficient network support and phased network integration: I. Backbone network layer II. Access network layer III. Network Operating Center and network support layer.

The Backbone Network layer links local nodes with the central NOC can transmit video, voice, and data traffic via fiber optic connections with high reliability.

The Access Network layer interconnects local unit/node networks, including wired and wireless connections, serving as the final link to the optical backbone. The performance of the access network infrastructure has a significant impact on user experience.

The Network Operating Center and Network Support layer serve as the network control center, monitoring network performance daily. The Network Monitoring Center (NMC) offers support for all network services and integrations to the university community.

Policy

- KIU shall maintain three-tier network architecture for the provision of all Information Technology and media services to the community.

Objectives

- To Ensure that the University backbone network/master architecture is implemented
- To build a reliable, resilient and robust campus network for the University
- To regulate and advice on appropriate IT equipment deployed on the Campus network for the optic fiber, LAN, last-mile and wireless network implementations.
- To ensure standard Infrastructure and network architecture that can support the university network traffic and IT services are implemented.
- To enhance overall user experiences on the network.

Strategies

- Development of Backbone Infrastructure network
  - The university backbone network shall be implemented exclusively on optic fiber cable according to the network architecture
  - The backbone optic fiber hubs shall be passive hubs and central to a cluster of intended locations as designed, with a specific number of optic fiber.
  - Backbone network implementation shall conform to defined specifications
- Development of Campus Local Area Network and use of IT equipment in the Network
  - Node location network shall be terminated on Managed switches (POE) for local network distributions
  - Node location network shall be terminated on a Gigabit capacity router-board and Optical converter and each node shall have spares for each network equipment locally terminated
  - Node/Units LAN design and project supervision shall be done in conjunction with ITNH unit of the Directorate.
  - New building infrastructures within the University shall be e-ready buildings (local network design shall be implemented along in its construction phase)
  - The ITNH unit of the Directorate shall be consulted before the use/integration or replacement or purchase of any IT equipment into the local node network or network expansion plans for the node
  - Damaged and faulty IT equipment shall be replaced and restored by the person or unit involved as appropriate
  - Damages to University properties incurred during the implementation of IT projects shall be replaced and restored to originality by the contractor implementing the project
- Infrastructure deployment at the Central IT NOC/NMC
  - Servers on which network services are implemented shall be managed updated/extended servers with appropriate warranties.
  - Every Network service initiated at the central NOC shall be on resilience architecture (redundancy; in-case of hardware/software failure)
  - Restriction access and access/ activity log record details shall be implemented in the Server room for IT staff control.

3.6. Database/Enterprise Resource Planning Policy

Database is a collection of records that has been systematically organized for easy access. It is one of the core IT services in universities because of the huge amount of information being generated.

Policy

- KIU shall have a centralised database system managed by DICT.
- The database shall contain all relevant information about personnel, finances, projects etc.
- An ERP system shall be deployed to make access to the database useful for various tasks.
- Access to data stored in the database shall be on request.

Objectives

- To ensure accuracy in record keeping.
- To make access to information easy and simple.
- To allow automation and computerization of processes.

Strategies

- To acquire and/or modify an ERP system for use in KIU.
- To collect data once and digitally to ensure accuracy.
- To train users on the ERP system.

3.7. E-learning Policy

E-learning refers to technology-based education, delivered either remotely or in a traditional classroom environment, using computers and smart devices.

Policy

- The use of technology for teaching shall be encouraged.
- All staff and students shall be required to take prescribed introductory courses in computing as a requirement for E-learning.

Objectives

- To promote learning outside the walls of the classroom
- To prevent learning gaps even if the lecturers or students are not physically present

Strategies

- Adhere to the best e-learning practices and software packages.
- Make e-learning systems available to students.
- Make e-learning systems available to staff.
- Conduct trainings on using the e-learning tools for the staff.
- Encourage the teaching of e-learning tools to students as part of general studies course.

3.8. Local Area Network (LAN) Policy

A Local Area Network (LAN) connects one or multiple computers for sharing resources like files, programs, or devices (e.g. printers, scanners).

Policy

- The LAN is a property of the university
- DICT shall be consulted on the design and implementation of a LAN.
- Users cannot extend, modify or remove LAN components without prior written permission from DICT.

Objectives

- To ensure that standards are adhered to
- To allow maintenance of LAN irrespective of LAN builder

Strategies

- Keep copies of LAN diagrams at the DICT office.
- Publish network standards

3.9. Paperless Policy

As the trend is shifting towards eco-friendly, biodegradable materials and abandoning those that harm the environment. KIU recognizes this and aims to decrease its annual paper usage by exploring alternative communication and documentation methods.

Policy

- Use of electronic documentation systems shall be integrated into all activities of the University.
- Electronic documents shall have the same significance as paper documents.
- Electronic documents will be archived and preserved for referencing and use.

Objectives

- To promote environmentally sustainable operations.
- To encourage e-governance initiatives

Strategies

- Build a central data center for records and files.
- Implementation of a document management system.
- Documents will be in a format that is easily accessible by software applications.
- Document authenticity will be guaranteed by appropriate mechanisms.
- Access to documents shall be restricted and available when privileges are granted.

3.10. Mobile Devices Policy

A mobile device is a small computing device, typically small enough to be handheld (and hence also commonly known as a handheld computer or simply handheld) having a display screen with touch input and/or a miniature keyboard and weighing less than 1 kilogram. Mobile devices are pervasive in society today and their use has increased without a doubt in the university.

Policy

- Mobile devices shall comply with all existing policies related to information technology, information systems, communication technology and media technology.

Objectives

- To allow access to University resources using mobile devices

Strategies

- DICT reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to the network
- Staff and students using mobile devices and related software for network and data access will, without exception, use secured data management procedures. All mobile devices must be protected by a strong password
- DICT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and will be dealt with
- DICT reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the network

3.11. Remote Access Policy

This policy affects all authorized personnel including university faculty, staff, students, employees, and affiliates who access the university's IT network from a remote location using either university-owned or personal devices. This policy covers work-related activities performed through remote access, such as email and intranet web access. The policy applies to various remote access methods such as dial-up modems, ISDN, DSL, cable modems, etc.

Policy

- Authorized users with remote access privileges to the University Information Technology Network shall ensure that their remote access connection complies with the University Information Technology Policies and Procedures, and treat it with the same consideration as their on-site connection to the University.
- General access to the Internet through the University Information Technology Network, for reasonable recreational use by immediate household members of the university on personal computers, is permitted. Each Authorized user shall be responsible for ensuring that the family members comply with the University Information Technology Policies and Procedures, do not perform illegal activities, and do not use the access for outside business purposes. Each authorized user bears responsibility for any consequences of misuse.
- Authorized users must review applicable policies to determine how to protect information when accessing the University Information Technology Network via remote access methods, and for acceptable use of the University Information Technology Network.

Objectives

- To set guidelines for access to the University network when the user is not physically present in the campus

Strategies

- Secure remote access shall be strictly controlled. Control shall be enforced via one-time password authentication or public / private keys with strong Pass-phrases.
- Authorized users who, as a University employee or affiliates, with remote access privileges, shall ensure that University-owned or personal information technology resources are not connected to any other Network at the same time they are connected to the University Information Technology Network (with the exception of personal Networks that are under the complete control of the authorized user).
- Authorized users who, as a University employee or affiliates, with remote Authorized User access privileges to the University Information Technology Network must not use non-University Email accounts such as Hotmail, Yahoo, AOL or other external resources to conduct University business, thereby ensuring that official business is never confused with personal business.
- Routers for dedicated ISDN lines configured for access to the University Information Technology Network shall meet the minimum authentication requirements of the Challenge Handshake Authentication Protocol (CHAP).
- Reconfiguration of an authorized user's home equipment for Split-Tunneling or Dual Homing is not permitted.
- Frame Relay shall meet the minimum authentication requirements of Data-Link Connection Identifier (DLCI) standards.
- Non-standard hardware configurations must be approved by Information Technology Services personnel, and Information Security personnel must approve security configurations for access to Hardware.
- All Hosts that are connected to the University Information Technology Network via Remote Access technologies, including personal computers, must use the most recent corporate-standard anti-virus software.
- Personal equipment that is used to connect to the University Information Technology Network must meet the same requirements applied to university-owned equipment for remote access.
- Organizations or Authorized Users who wish to implement non-standard remote access solutions to the University Information Technology Network must obtain prior written approval from the Information Technology and Media Services Directorate.

4. FINANCE

4.1. Service Costing Policy

The cost of providing a service such as Internet access shall not be arbitrary but following acceptable practices.

Policy

- All services provided shall be offered to users at a price that covers the cost of the provision.

Objectives

- Services should be maintained based on the cost paid by the subscribers without needing the University to foot bills for those services.
- Services should be sustainable.

Strategies

- There are no free services.
- The cost of human effort, sunk costs, administrative charges and logistics will be included
- The cost shall not include taxes such as VAT (Value Added Services Tax).
- The cost of services can be changed when a constituent cost of the services change.

4.2. Payment Policy

There are multiple payment channels open to users in the case where payment to the University or any of its organs is required.

Policy

- Users of services provided by DICT shall pay for the services using acceptable payment methods

Objectives

- To provide an accountable way of tracking all revenue generate by the directorate
- To provide convenient payment channels

Strategies

- The Directorate shall endeavor to provide multiple payment platforms for users
- Payment for services shall be in the Local Currency except in circumstances related to international trade
- Payment for services shall be pre-paid
- Agents may be used for the collection of payments.

4.3. Investment and Funding Policy

Securing investment and funding is vital to the success of any information technology development plan and program. Funding can come from a variety of sources such as university management, private companies, and international organizations. University play a crucial role by providing an atmosphere that encourages investment and funding from multiple stakeholders.

Policy

- The University Faculties, Centers, Departments and Units shall invest in the provision of IT facilities and infrastructure.

Objectives

- To create an enabling environment and facilitate foreign direct investment as well as private sector investment in University DICT;
- To encourage public-private partnerships for the development of IT and Media;
- To provide funding for IT and Media projects through appropriate budgetary allocation;

Strategies

- Any investment shall be in line with section 3.2 of this document.
- Provide incentives to investors.
- Provide appropriate fiscal incentives to encourage local manufacture of IT and media equipment and the development of software.
- Streamline procedures and requirements for the purchase and use of IT and media. equipment;
- Adopt financing models that foster indigenous IT and digital media entrepreneurship.

4.4. Software Industry Economics Policy

The software industry is an ever-evolving and rapidly growing sector that is driven by advancements in technology and increasing demand for software solutions across a wide range of industries. The software industry operates under various business models, including licensing, subscription-based services, and cloud-based delivery, each with its unique economic characteristics.

Policy

- Information Technology and Media Services shall promote and encourage the growth of the economy through software development as a catalyst for revenue generation.

Objectives

- Promote software development as one of the major sources of revenue for the University.
- Provide and support the economic conditions that will enable the creation of a vibrant software ecosystem.
- Provide guidelines for the articulation of sectoral (defense, national security, education, agriculture, industry, finance, culture, media, sports etc.) software development and relevant

legislation such as intellectual property regime which shall enable a software innovation-led economy.

- Adopt a "user-driven" strategy that is based on the availability of software and its adaptation, dissemination and use tailored to the demands of the University and society at large.
- Information Technology and Media Services shall promote the development of indigenous software products and services for domestic, regional, and international markets.
- Information Technology and Media Services shall consider the development of an appropriate policy framework for the procurement and deployment of Open Source Software (OSS) solutions in the University.
- Ensure the use of OSS products for interoperability that support open standards and specifications in all IT projects.
- Providing a platform for advocacy for the development of the business of indigenous software products and services, as well as abuse of the use of internet resources.

Strategies

- Promoting investment in the software ecosystem through public-private partnership initiatives.
- Promoting the collaboration of software experts and students.
- Developing a benchmark for quality assurance of software products and services.
- Promoting the acquisition of software technology and stimulating research, innovation and development.
- Promoting the use of indigenous software products and services in the University.
- Encouraging other institutions/organizations to subscribe to indigenous software products and services.
- Providing a procedure for the classification, testing, measurement and certification of software products and services to ensure total adherence to global standards and best practices.
- Promoting collaborative initiatives amongst identified software investors, developers and solution providers to accelerate the growth of indigenous software products and services.
- Ensuring that the University Software Team is put to work before seeking Software Development firms
- Establishing innovation canters that can ably attract the available pool of expertise in software engineering.
- Encouraging the procurement of Software solutions in a manner that ensures the interoperability of solutions.
- Encouraging the development of a policy framework around the procurement and deployment of Open-Source software solutions.

5. HUMAN RESOURCE

5.1. DICT Staff Training Policy

The technical knowledge of DICT personnel contributes to the sustained growth and advancement of the university's ICT and technology services delivery.

Policy

- All DICT staff shall be trained regularly in related and relevant information technology and media solutions such as software, equipment, technology, concepts and application.

Objectives

- To enable staff to acquire the knowledge and skills that will enable them to perform effectively in their current roles
- To enable staff to enhance their performance in their current roles
- To enable staff to respond effectively to the demands placed upon them by internal and external change and development
- To enable staff to develop their careers effectively within the University

Strategies

- There shall be in-house training such as seminars, workshops, and webinars for all DICT staff
- Attendance at meetings of professional associations such as the Uganda Computer Society and Computer Professional Registration Council of Uganda shall be encouraged
- Hosting of training workshops so that more DICT staff can attend
- Paper presentations and Tutorial sessions at workshops and conferences
- Online training classes
- Individuals are responsible for reflecting at regular intervals upon their jobs and future career aspirations and identifying their needs for training and development
- Individuals are responsible for discussing (1) above with their Head of Department/Unit during their Performance and Development Review Meetings to establish priorities in relation to their unit and institutional objectives.
- The Directorate/Unit shall nominate individuals to participate in training programs
- The Directorate will rotate sponsorship of training every two years as follows:
  - Every senior staff shall be entitled to attend at least two local training events and one international training event
  - Every junior staff shall be entitled to attend at least one local training event
  - Deputy/Assistant Directors shall be entitled to attend at least three local training events and one international training event
  - The Director shall be entitled to attend at least six local training events and three international training events
- The Directorate will allow staff to attend unsponsored training events yearly as follows:

- Every senior staff can attend a maximum of two local training events and two international training events
- Every junior staff can attend a maximum of two local training events and one international training event
- Deputy/Assistant Directors can attend a maximum of three local training events and two international training events
- The Director can attend training events as the need arises

5.2. Digital Proficiency for All Staff Policy

The University recognizes its staff as its most valuable asset and is dedicated to supporting their growth through training and development. It is expected that all staff possesses literacy in information technology and media services within the University.

Policy

- All staff of the University shall be proficient in the use of Information Technology and Media Technology applications

Objectives

- To enable staff to acquire the knowledge and skills that will enable them to perform effectively in their current roles.
- To enable staff to respond effectively to the demands placed upon them by internal and external change and development.
- To enable staff to develop their careers effectively within the University.
- To ensure that the DICT training program shall lead to the use of IT for a significantly large group of new users and also change the working ethics of the existing users.
- Providing appropriate resources for training and development
- Training will focus on building skills in users making them effective in exploiting provided IT resources.

Strategies

- Ensuring that all staff shall have access to appropriate opportunities for continuing professional development in their jobs, in accordance with the university's equal opportunities policy.
- Ensuring equal opportunities in access to training and development is in accordance with the university's Equal Opportunities Policy.
- Identifying needs for training and development of staff arising from an internal and external change at Faculty and University levels
- Liaising with the Staff Development Unit in the provision of appropriate opportunities
- ICT Directorate will develop curricula for all trainings including the development of source material.
- ICT Directorate will release the training calendar at the commencement of each academic year.

- All trainees shall be subjected to a certification assessment. The Training Research and Development (TRD) unit of DICT shall issue certificates upon the successful completion of training and examination.
- The development of training materials and the administration of the training shall attract remuneration to staff and other personnel involved.

5.3. ICT Ethical Policy

DICT personnel are required to adhere to professional conduct guided by moral and ethical principles.

Policy

- DICT staff are obligated to abide by the code of ethics of their profession in their conduct.

Objectives

- The goal of the Directorate is to ensure that all business practices are both ethical and in accordance with the law.

Strategies

- Make the code of ethics of relevant professions available e.g., Computer Professionals Registration Council of Uganda, and Council for the Regulation of Engineering in Uganda.
- Encourage staff to join professional organizations/associations
- Run workshop on ethics, conduct and customer service
- Emphasize the vision, mission and core values of the Directorate.
- Promote the core values of the Directorate through placement on souvenirs, products, etc.
- Professionalism and ethics of IT Network Administrators
    - The network administrator can restrict a user account on the justification of a breach in usage procedure
    - Periodic maintenance of NOC and campus-wide IT deployments shall be carried out by the ITNH unit to identify, advice and replace items categorized at EOL (End-of-Life)
    - The IT administrator shall act with integrity, Respect, and readiness to support and observe great confidentiality
    - IT administrators shall resolve network complaints to the Network IT helpdesk within a WLA (Work Level Agreement) of 4-working hours
    - Each Faculty of the University shall have a resident IT Network support staff that will attend to all her network-related issues
    - Network administrator shall discharge their responsibilities within the ethics of his/her profession

5.4. DICT Personnel Policy

DICT consists of talented and innovative staff. When organized into units such as Network and Software, the staff benefit from a defined career path and a clear hierarchy.

Policy

- DICT personnel must possess qualifications in fields such as information technology, communication technology, network technology, and media technology. The hiring, training, advancement, and placement of staff with relevant ICT designations will be overseen by the Directorate.

Objectives

- Defining the roles and responsibilities of ICT personnel: A clear definition of the roles and responsibilities of ICT personnel helps to ensure that everyone understands what is expected of them and what they can expect from others.

Strategies

- The following cadre of staff will form the technical personnel of the Directorate:

Senior Staff

- Data Processing Officers Cadre
- Content Creator Staff Cadre
- Hardware Engineer Cadre
- Programmer Analyst Cadre
- Systems Analyst Cadre
- Telecoms/Network Analyst Cadre

Junior Staff

- System Administrator Cadre
- Computer Hardware Cadre
- Computer Operator Cadre
- Graphic Artist Cadre

- All DICT personnel in the University will meet annually
- The Directorate will ensure that personnel have defined career paths within the Scheme of Service
- Personnel records will be kept for all DICT personnel in the University
- Ensuring quality and consistency: By establishing standards and procedures for ICT personnel, an ICT personnel policy helps to ensure that the quality and consistency of services are maintained.

6. SOFTWARE

6.1. Software Development, Support, and Use Policy

Faculty, administration, staff, and students may develop suitable software for use on the University's IT systems, with support from the University. The University or the author may also publish or market the software for revenue generation.

Policy

- The University shall regulate the development, utilization, support, publishing, and marketing of any software created by members of the University community.

Objectives

- Ensuring clarity in the rights and responsibilities of all parties concerned with THE development of software and its documentation.

Strategies

- Securing the creation and dissemination of software products within the KIU community.
- The DICT will examine and assess all software produced or obtained before implementation.
- The DICT will establish a supportive setting for software development.
- The establishment of a technology incubator or innovation center will be encouraged.
- The establishment of a programming division within the DICT will be established.

6.2. Software Infrastructure Policy

To ensure the proper functioning of the software, necessary infrastructure like servers and electricity must be in place. It is important to make the necessary efforts to provide all the required infrastructure.

Policy

- Information Technology should support the ideation, creation, acquisition, implementation, management, assessment, and updating of essential infrastructure to advance the software applications of KIU in accordance with global standards and competitiveness.

Objectives

- Establish and safeguard vital infrastructure to foster the rise, expansion, and advancement of a resilient software environment.
- Create a plan for the supply of critical infrastructure to position KIU as a leading software center in West Africa, Africa, and the world market.
- Acknowledge and prioritize Critical Software Infrastructure (CSI) such as electricity, communication, and transportation to boost the software ecosystem at KIU.

Strategies

- Allocating appropriate funds for the creation and maintenance of software engineering labs in KIU.
- Guaranteeing the availability of functional software infrastructure such as energy sources, telecommunication services, fiber optics and internet connectivity to boost the software environment and facilitate collaborative learning and teaching (e-learning, distance learning, open-university systems, etc.).
- Ensuring the provision of necessary resources for supporting the growth and development of the mobile software development sector.
- Building a specialized software technology park for the creation of embedded systems, local software platforms, and interfaces.
- Fostering cooperation and coexistence between emerging software development platforms (proprietary software systems and open-source software systems).
- Formulating efficient procedures and technical guidelines for assessing the performance of Critical Software Infrastructure (CSI) at the University.
- Supporting various Public-Private Partnership (PPP) models for developing, nurturing, and safeguarding Critical Software Infrastructure.
- Re-establishing and re-positioning terrestrial LAN or fiber as backup communication infrastructure for continuous software services.
- Centralizing, monitoring, and controlling communication infrastructure to minimize costs and ensure software development service quality.
- Enforcing compliance with existing regulations for procurement of local software products and services among Faculties, Departments, and Units.
- Carrying out yearly surveys of software human capital and infrastructure in all Faculties, Departments, and Units to gather critical data for growth planning.

6.3. Software Usage Policy

KIU must prohibit any employee from utilizing software in a way that contradicts its relevant license agreement, including distributing or receiving software from clients, contractors, customers, or others.

Policy

- All software obtained for or by the university or created by university employees or contractors working on behalf of the university are considered to have been purchased and licensed exclusively for official use.

Objectives

- This policy governs the proper and improper usage of licensed software, both on and off campus, by setting standards for software copying, sharing, and utilization and informing university users of the consequences of software abuse.

Strategies

- Each individual using the software must read, understand, and follow all license agreements, notifications, and conditions associated with the software they acquire, copy, transmit, or

use. Unless specified in the license agreement or contract, duplicating copyrighted software, excluding backup and archival purposes, may violate federal and state laws.

- Master copies should not be used for daily operations and must only be used in case of computer problems such as virus infections or hard disk crashes that make the original or installed copy inaccessible or unusable.
- The creation and use of backup copies must comply with the software license agreement.
- No faculty, staff, or student may install software without obtaining the proper license.
- No user may sell, rent, sublicense, lend, transfer, or otherwise make software or any interest in it available to unauthorized individuals or entities.
- No user may decompile, disassemble, or reverse-engineer software unless permitted by the university's IT contracts administrator and all relevant software licenses and agreements.
- The university and its agents have the right to audit all resources to ensure compliance with the software policy, and the university may also allow software licensors and their agents to audit some or all resources to ensure compliance with license agreements, purchases, or other applicable agreements.
- Any user who suspects another user of not following the software policy must immediately inform DICT.
- This policy covers all software acquired by or for KIU, regardless of location, and all software used on KIU network, regardless of how it was acquired.

6.4. Software License Compliance Policy

The policy regarding compliance with software license agreements lays out the rules and guidelines for the use of software within KIU. It aims to ensure that the University has the necessary and valid licenses for all the software used and that its usage is in accordance with the conditions stated in the licenses. Failing to comply with the software licensing provisions can result in serious legal consequences and financial penalties for the University. Therefore, it is essential that the University has robust processes in place to guarantee compliance and minimize risk.

Policy

- Adherence to software licensing requirements is crucial for KIU as non-compliance can result in serious legal liabilities. It is imperative that the university implements effective measures to acquire the necessary licenses for all the software it utilizes and adheres to the conditions of use outlined in these licenses to avoid the risk of legal action and penalties.

Objectives

- To safeguard the University from potential lawsuits resulting from violations of software licensing agreements.
- KIU shall comply with all license agreements of software in use

Strategies

- DICT will keep a database of software licenses to help departments meet their obligations.
- The responsibility of ensuring software license compliance lies with the head of each unit in the university.

- Their specific responsibilities include maintaining a record of software purchases, disposing of software through resale, keeping a record of where licensed software is installed and tracking its movement within the department, and ensuring staff understand their own responsibilities with regards to license compliance.
- DICT should periodically conduct a software compliance audit.

6.5. Computer Software Purchase Policy

KIU is committed to the lawful and ethical use of the software. When a department or unit requires software not already licensed to the university, or additional copies of licensed software, the user should request their budget unit head or department head to make arrangements with the purchasing department or vendors for the acquisition of appropriate licensed copies. The software policy does not grant users the right to software, obligate the university to acquire software, delegate authority to individuals to purchase software on behalf of the university, or create liability for the University for a User's Non-compliance with the policy. Unauthorized duplication of software is illegal and goes against the university's standards of conduct. The university supports the ethical use of intellectual material and strives to avoid legal liability regarding software purchase and installation.

Policy

- The sole responsibility for purchasing all standard desktop applications and enterprise software licenses lies with DICT.
- All software obtained for the university or created by university personnel or contractors, must undergo review by DICT and must only be used in accordance with the relevant purchase and licensing agreements. This software is considered the property of the university.
- Requests for purchasing non- DICT software licenses must be referred to DICT for evaluation and authorization.
- No department or unit is allowed to make any purchases, sign contracts or arrange for software installation without prior written approval from DICT.

Objectives

- To establish an efficient process for acquiring necessary software applications at KIU that takes advantage of bulk purchasing and ensures adequate license coverage to meet the requirements.

Strategies

- The DICT will purchase necessary software licenses and/or provide annual maintenance for all standard desktop and enterprise software applications owned by the university.
- The DICT will not engage in or tolerate any unauthorized copying of software.
- The responsibilities of the DICT include serving as a central point for university-wide software licensing, maximizing the university's purchasing power through vendor agreements, assisting with the full life cycle of software agreements by coordinating license acquisition, tracking, and record management, evaluating options for site-licensing and volume procurement, providing a full-service approach to software acquisition to simplify the process for faculty, and negotiating SLAs for software and hardware equipment.

- The DICT will ensure a timely and sufficient supply of legally acquired software to meet the legitimate needs of the university.
- The DICT will comply with all license or purchase terms for the use of any software acquired by the university.
- The heads of units, faculties, and departments are responsible for ensuring the proper acquisition and use of software within their respective areas, and for taking recommended steps to mitigate legal risks.
- The DICT will enforce strict internal controls to prevent unauthorized copying, including measures to verify compliance and appropriate disciplinary action for violations.

7. RESEARCH

7.1. Software Research, Development, and Innovation Policy

The Software Research, Development, and Innovation (SRDI) policy outline the goals, procedures, and responsibilities for the development and deployment of software applications within KIU. It aims to ensure the development of high-quality software applications that meet the needs of the university and its users. The SRDI policy is critical for ensuring the effective and efficient development of software applications in the University. It provides a framework for software development that is aligned with the organization's goals and objectives and ensures the quality of the final product.

Policy

KIU shall foster growth in software Research, Innovation, and Development (RID) which is a crucial aspect of the knowledge economy, through Information Technology.

Objectives

- Encourage Research, Innovation, and Development (RID) in software engineering that is nationally oriented and marketable in local and global software markets.
- Fostering innovation in acquired technologies to produce globally competitive software products and services.
- Encouraging collaboration among experts, professionals, and students in software engineering and other areas within the university.
- Advocating for public and private partnerships in software development.
- Developing knowledge-based systems for a software evaluation, procurement, deployment, management, and performance evaluation of human capital, infrastructure, products, services, and markets.
- Re-skilling existing human resources with a focus on producing a large number of software engineers, developers, and solution providers for both domestic and international competitiveness.
- Establishing a framework to measure the impact of software development on the University.

Strategies

- The Training, Research and Development division of the DICT shall have the exclusive responsibility for establishing standards, conducting testing, measuring, and certifying software-related human capital, infrastructure, products, and services.
- The Training, Research and Development unit shall be empowered to create guidelines to grow the software ecosystem within KIU.
- Collaboration between the Training, Research and Development unit and key strategic sectors within the university shall be encouraged and facilitated.
- The Training, Research and Development unit shall strive to provide global best practices for the classification, testing, measurement, and certification of software products and services within the University.

- The performance of the Information Technology and Media Services Policy shall be monitored and evaluated regularly.

7.2. Plagiarism Policy

Plagiarism is the act of presenting someone else's work, ideas, or words as one's own without proper attribution or permission. It is considered a form of academic dishonesty and is strictly prohibited in many educational institutions. Plagiarism can take many forms, such as copying text directly from a source, paraphrasing information without proper credit, or submitting someone else's work as your own.

Policy

- The University has set a maximum plagiarism rate of 20% for any submitted publication.
- KIU will conduct plagiarism checks on individual submissions.
- The University will subscribe to plagiarism-checking software that will be accessible to all parties involved.

Objectives

- To advance ethical writing, academic work, and investigation
- To minimize instances of plagiarism and dishonesty
- To promote proper referencing of information sources.

Strategies

- Train stakeholders on the use of plagiarism software
- Maintain University access to the plagiarism software
- Allow multi-user access to the plagiarism software
- Allow access to the plagiarism software based on authentication and authorization e.g. username based on DICT record
- Encourage the development of local plagiarism checking software for students' projects and assignments.

8. PARTNERSHIPS

8.1. Policy

The potential for IT infrastructure project delivery, innovation, skill acquisition and outreach of University services to staff and students is huge through partnerships between the Directorate and the private sector. The Directorate recognizes the private sector as a driving force of economic growth and is committed to creating a favorable environment for successful, impactful, and sustainable Public-Private Partnership initiatives.

Policy

- The Directorate intends to fully leverage the vast potential offered by Public-Private Partnerships in IT and media development.

Objectives

- Enhance PPPs in IT and media to further the growth and development of the University.
- Ensure that PPPs bring about a significant and lasting impact, benefit both University and private sector stakeholders, and serve the ultimate beneficiaries effectively.

Strategies

- Ensure effective cooperation amongst Faculties, Departments, and units that are relevant for the proper operation of PPP
- Ensure a clear framework of Intellectual Property Protection and other terms of engagement with the private sector exist
- Ensure that all proposed PPP projects are subjected to viability and sustainability assessments
- Promote awareness of PPP opportunities to the private sector
- Ensure, where appropriate, incentive schemes to accelerate take off of IT projects

8.2. Web Content Creation Policy

A website is a group of web pages connected by hyperlinks that provide information on a location, object, or individual.

Policy

- The University's official website can be found at KIU.edu.ng
- All stakeholders in the University will contribute to the content of the website.
- The management of all websites will be handled by DICT.
- All websites associated with the university will be hosted on-site.
- The university will not be held accountable for any content created by stakeholders and published on its website.

Objectives

- To enhance the online presence of KIU.
- To enable stakeholders to create content for online distribution.

Strategies

- Create virtual servers to host websites from multiple units.
- Allow stakeholders to edit, change and modify the contents of their webpages.
- Provide website management training for stakeholders.
- Locate all webmasters in one unit under DICT.

8.3. Web Portal Policy

A web portal is a website that serves as a single point of access to information or services on the internet. It often includes a variety of content and features such as news, search engines, forums, and personalized content for registered users.

Policy

- KIU will create and possess its web portal.
- The portal will provide services and features as deemed appropriate by the university.
- The information generated by the portal will be under the control of the DICT.

Objectives

- To guarantee the provision of all required services to online users.
- To guarantee the preservation of user privacy.

Strategies

- The DICT will host vital data on-premises.
- The services will be organised into categories such as students, staff, alumni, and guests on the portal.
- Mobile device compatibility will be considered during the **design phase.**

8.4. Social Media Policy

Social media refers to computer-based technologies that enable individuals to produce, share, or exchange text, information, opinions, images, and videos in virtual communities and networks. It is described as "a category of Internet-based applications that draw on the principles and technologies of Web 2.0, enabling the creation and sharing of user-generated content." Examples of social media tools and platforms include Facebook, Twitter, Instagram, Google+, and Pinterest.

Policy

- The university will have a presence on relevant social media platforms, which will be managed and controlled by DICT.
- The university's social media presence must not be utilized for personal benefits or purposes.

Objectives

- To strengthen the university's message and image.
- To establish KIU’s reputation as a top-notch institution through an online presence.

- The platforms should be utilized to connect with digitally engaged young people, alumni, and students, while still utilizing traditional channels.
- To ensure that all communication channels are utilized for the dissemination of information.

Strategies

- Implement a social media strategy.
- The Social Media Manager should exercise discretion in accepting requests on behalf of the university or its departments.
- All social media accounts must have at least two administrators to provide a backup in case the primary administrator is unavailable during an emergency.

9. BACKUP, RECOVERY AND ARCHIVING

9.1. Policy

This policy outlines the proper ways to plan, prepare, manage, and reduce the impact of IT system disasters at KIU. It serves as a guide for creating, executing, and continually improving a disaster recovery plan for the systems and services overseen by the DICT department.

Policy

- In the event of a disaster, DICT will be accountable for restoring the IT and media systems under its management.
- DICT must have a comprehensive backup and recovery plan for all possible disasters.
- The backup and recovery plan will be funded by the university.

Objectives

- To establish a structured method for restoring the critical technology and information managed by the Information Technologies.

Strategies

- The Network Attached Storage appliance will undergo regular backup with the following schedule:
  - Daily incremental backups from Monday to Thursday with the data stored on-site.
  - Monthly full backups on the first Friday with the data stored off-site.
  - Weekly differential backups on all other Fridays with the data stored on-site.
- Regular backups for Windows Servers (not in DMZ) will follow the same schedule:
  - Daily incremental backups from Monday to Thursday with the data stored on-site.
  - Monthly full backups on the first Friday with the data stored off-site.
  - Weekly differential backups on all other Fridays with the data stored on-site.
- Linux Servers will undergo the same regular backup schedule:
  - Daily incremental backups from Monday to Thursday with the data stored on-site.
  - Monthly full backups on the first Friday with the data stored off-site.
  - Weekly differential backups on all other Fridays with the data stored on-site.
- The Backup Catalogue Database will undergo regular backups with the following schedule:
  - Daily full backups from Monday to Sunday with the data copied to tape and stored on-site.
  - Weekly backups on Friday with the data copied to tape and stored off-site.
- Backup tapes must be handled and stored according to the following guidelines:
  - Backups must be recorded on reusable LT01, LT02, and LT03 media with capacities ranging from 100-400 GB uncompressed (200-800 GB compressed) and transfer speeds of 15-60 MB/sec.
  - The media must be labeled clearly and kept in a secure area that can only be accessed by ICT staff or the contracted secure off-site storage vendor used by DICT.

- During transportation or transfer of media, it must not be left unattended.
- Daily backups must be stored in a fireproof safe that is physically secure and located in a separate building from the Data Centre. At a minimum, daily backups must be kept for one month.
- Weekly backups must be stored in a physically secure off-site location managed by a third party.
  - Weekly backups must be kept for at least four weeks.
  - Once the four-week period has passed, the tapes must be returned to DICT and either reused or disposed of.

- Before retiring and disposing of the media, the DICT must ensure:
  - The media does not have any active backup images, and
  - The contents of the media cannot be accessed or recovered by unauthorized individuals.
  - For all backup media, DICT must also make sure to physically destroy the media before disposing of it.
- Periodic backup verification is required:
  - The logs generated from each backup job will be reviewed daily to:
    - Detect and fix errors.
    - Monitor backup duration.
    - Improve backup performance where possible.
  - DICT will identify issues and take action to minimize risks in case of backup failure.
  - Weekly random test restores will be performed to confirm the success of backups.
  - CT will keep records of log reviews and test restores for audit purposes.
  - Data must be backed up frequently and stored securely for data recovery.
  - The DICT has policies for backup and restoration procedures.
- Data Recovery:
  - In case of a severe system failure, the users will have access to their backed-up data stored off-site within 5 business days after the damaged equipment has been replaced.
  - In case of a less severe system failure or user error, the users will have access to their backed-up data stored on-site within 1 business day, based on the amount of data to be restored.
  - The DICT will create a Disaster Recovery Plan to outline the emergency recovery of ICT systems.
  - An annual DRP simulation test will be conducted to assess the ICT Directorate's readiness.
- Restoration Requests:
  - In the event of information being accidentally deleted or corrupted, requests for restoration should be made to support@kiu.ac.ug
- Responsibilities:
  - The Network Operation Control Team is responsible for backups and data recovery.
  - The Networking Administrator is responsible for telephone system backups.
  - The Senior IT Operations will verify the data along with the data owners.