University of Kisubi

ICT POLICY

August 2020

Table of Contents

DEFINITION OF TERMS

ANTI-VIRUS: Also known as anti-malware is a computer programme used to prevent, detect, and remove malware.

ANTI-SPAMMING: The phrase anti-spam refers to any software, hardware or process that is used to combat the proliferation of spam or to keep spam from entering a system.

Cyber Security: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation.

UniK: University of Kisubi

DICT: Department of ICT

Management System: Set of inter-related or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives.

Quality Policy: Intentions and direction of an organization related to quality performance, as expressed by its top management.

ODeL: Open distance and e-learning.

Objective: Result to be achieved (strategic or operation) and can apply at different levels e.g., organization-wide, project, product, service and process.

Monitoring: Determining the status of a system, a process or an activity.

1.0 The University of Kisubi and its context

The University of Kisubi (UniK) was established in 2004 as Kisubi Brothers Centre of Uganda Martyrs University. It was started to provide quality training to teachers in Uganda. UniK became a Constituent college of UMU in 2009. The university was conceived by the Brothers of Christian Instruction (BCI) to be a centre of excellence in teacher education management and other disciplines. It is inspired by the words of the founder of the Brothers of Christian Instruction and follows the Mennaisian Spirituality and service for GOD ALONE in the spirit of shared mission to cater for the youth and less privileged in society. The University was conceived as a critical component of the educational transformation and development, for strengthening the education management capacities of various institutions. The constituent college attained autonomous status with the grant of a provisional licence as University of Kisubi (UniK) in 2015 with a mandate to offer degrees, diplomas and certificates as a University. The University is sponsored by the Brothers of Christian Instruction with the Provincial Superior as Chancellor. The University Council, Management, staff and students are oriented regularly to understand and appreciate the history, pedagogy and mission of the Brothers of Christian Instruction in order to evangelise the youth, and the poor through university education.

UniK aspires to become a center for excellence in ICT comparable in standard to the very best in the world. Its niche is in the promotion of innovation in business and technology.

The UniK's ICT Policy is a guide on how ICT shall be used to achieve the University goals and aspirations. It highlights how the usage of ICTS shall be implemented, their development and maintenance, the optimal distribution of resources (hardware, software, data and human resources) as well as the safe and healthy utilization of ICT and the environment. This policy seeks to enumerate the rules necessary to ensure the existence of the highest levels of consistency, control and harmonious interaction with ICT technologies.

1.1 The University Structure

The University is governed by a Council whose members represent key stakeholder organizations and students. The Chief Accounting Officer is the Vice Chancellor; who is appointed by the Chancellor on recommendation of the Council. The Vice Chancellor works with the Deputy Vice Chancellor(s), Faculty Deans, Directors of schools, Dean of Students, Heads of Department, and Heads of various units to ensure the effective strategic and operational management. The University has a Senate that regulates all the academic activities of the University.

1.2 Policy Statement

Information and Communication Technology facilities are simply electronic and mechanical tools that facilitate the storage, manipulation, analysis and transfer of information.

UniK is committed to providing safe, effective and efficient usage of ICT facilities by its stakeholders (Academic and Administrative Staff, students, and Visitors).

UniK is committed to training graduates to develop innovative ICT technologies that provide more secure, efficient and effective solutions to the contemporary global challenges.

1.3 Vision and Mission Statements

1.3.1 The University Vision

A dynamic University that nurtures pragmatic professionals of integrity

1.3.2 The University Mission

To provide a holistic education through teaching, innovation, and research for social transformation

1.4 The Core Values

UniK attaches great importance to the integral nature and development of the human person. The University is propelled by the following core values:

- Service
- Creativity
- Responsibility
- Integrity
- Professionalism
- Teamwork

(SCRIPT)

2.0 THE GUIDING PRINCIPLES FOR THE IMPLEMENTATION OF THE POLICY

The ICT Department, demonstrates an on-going commitment to mainstreaming ICT usage by ensuring that the relevant policies, practices, and metrics are in place. Frequent and consistent communication will be issued by the ICT department about tips on how to execute safer, more secure and efficient operations. This will be broadcast to the affected or target audience(s).

2.1 Mainstreaming Diversity

UniK supports diversity and does not discriminate against minority entities based on age, gender, race, religion, political affiliation, etc. Diversity is encouraged in the different spheres like educational preferences, research interests, funding preferences, work-life-balance, performance management, and career management and other inclinations or variations.

2.2 Objectives of the ICT Policy

The Policy addresses itself to several sections of the discipline and each of these is given specific objectives and strategies. The sections are listed below:

1. Acceptable Use
2. Electronic Mail
3. Anti-virus and Anti-Spam
4. User Password
5. Data Backup & Restoration
6. Software Use
7. Internet Bandwidth
8. Computer Lab and equipment
9. E-Learning
10. Monitoring and evaluation

2.2.1 Acceptable Use

The purpose of this section is to ensure the proper use of the ICT facilities, software, services and systems by its employees (academic and administrative), guests and students in an appropriate, responsible, and ethical manner. This section also applies to the use of privately-owned computers or notebooks connected to the University network.

(a) Objectives

The acceptable use section has the following objectives:

i. To encourage the use of both the Internet and hardware as a conduit for free expression without infringing the rights of others;

ii. To protect and preserve the privacy of individual users and the public at large;

iii. To discourage the irresponsible use of hardware and network resources, which use may result in the degradation of service;

iv. To ensure the security, reliability and privacy of UniK's system and network infrastructure;

v. To avoid situations that may result in the occurring of any form of civil liability;

vi. To propagate the image and reputation of UniK as a reliable and responsible University.

(b) Strategies

i. The UniK community as a whole must be warned that they must not use the ICT facilities, software, services and systems in any illegal, or otherwise unauthorized manner as will be defined by the University authority.

The University reserves the right to monitor and record all activities related to University activities using ICT facilities, software, services and systems.

(c) The Department for ICT is responsible for the following:

i. Monitoring of network traffic and activities related to the University

ii. Recording of all activities related to the University

iii. Putting in place measures to ensure security, reliability, fair use and free expression of users without infringing the rights of others.

iv. Ensuring availability of measures to protect and preserve the privacy of individual users and the public at large.

v. To disseminate information in order to sensitize users on irresponsible acts in the use of hardware and network resources, that may result in the degradation of service

vi. To promote the safety of users and network infrastructure.

2.2.2 Electronic Mail

The University commits to provide the members of her community with an electronic communication infrastructure that includes computing resources, network connectivity, and software tools for electronic communication (e-mail). The University community shall use email service to send out information and the system shall automatically disable this service as soon as one is no longer considered to be a member of the community.

(a) Objectives

i. To ensure the proper use of the University's electronic communication infrastructure system by its employees (academic and non-academic), guests and students.

ii. To support academic (teaching and learning), research and administrative functions of the University

(b) Strategies

All e-mail communications (and associated attachments, objects, graphics, videos) transmitted or received by the network are subject to the provision of this policy, regardless of whether the communication was sent or received on a private or University owned computer.

(c) The Department for ICT is responsible for the following:

i. Creating email addresses for new members of the UniK community. This also includes access rights e.g. passwords, biometrics, and secret questions.

ii. Disabling email addresses for persons who have ceased to be members of the UniK community. In order to allow smooth transition, this will be done after a period of three months.

iii. Monitoring the electronic mail management usage by its users in a regular or systematic manner. Such monitoring may include tracking addresses of e-mail sent and received, accessing in-box messages, accessing messages in folders, and accessing archived messages. Please note that the Department reserves the right to monitor such usage from time to time and without prior notice.

iv. Minimizing any misuse or illegal use of email communications.

(d) The mailbox owners are expected to:

i. Be responsible and liable for all messages sent from their e-mail account and ultimately responsible for all activity performed under the account.

ii. Keep his/her password secret e.g. by not disclosing it out to another person, frequently changing it, not writing passwords down or using any other processes that facilitate automatic log-on

iii. Use only their authorised e-mail accounts.

iv. Use email accounts for legal, moral and authorized activities.

(e) The mailbox owner is expected to regularly carry out some activities to manage email accounts and documents. These include:

i. Reading all the new e-mail messages at least once in every 1 or 2 days and replying as soon as possible;

ii. Not letting messages build up in the Inbox and deleting messages as soon they are no longer needed;

iii. Opening the 'Sent messages' folder at least once a week and deleting old messages that are no longer needed;

iv. Saving messages that they want to keep onto the hard disk or removable disk;

v. Logging out of the email account before exiting the application.

(f) Mailbox owners are expected to adopt practices that increase privacy and confidentiality of their email communications. They need to be aware of the following:

i. E-mail messages are saved indefinitely on the receiving computer.

ii. Copies of e-mails are forwarded electronically or printed on paper.

iii. It is possible for other people to read or change messages that one sends by forwarding it to others.

iv. New e-mail shall be prevented from coming in to the mailbox once the mailbox has reached the maximum allowable storage space.

(g) UniK expects members of its community to exhibit acceptable ethical conduct in the use of computing resources. Users are expected to exercise good judgement to ensure that their electronic communications reflect the high ethical standards of the academic community and display mutual respect.

2.2.3 Anti-virus & Anti-spamming

(a) Objectives

The objective of this section is to ensure that the University provides its community with adequate protection from computer viruses, unsolicited and unwanted emails. The university shall invest and deploy anti-virus and anti-spamming software on ICT facilities owned or leased by the University as well as on ICT services outsourced by the University.

(b) Strategies

The Department of ICT shall be responsible for the following:

i. Installing anti-virus software to ensure that all networked computer servers, computers and notebooks used by the University users are protected against virus infections.

ii. Installing Anti-Spam software that automatically separates suspected spam from regular mail.

iii. Minimizing any misuse or illegal use of email communications.

iv. Protecting the community against other malicious attacks like denial of service, spy ware, phishing.

Users of the University resources are expected to act in the following way:

i. Report any case of virus, spam or other security risks.

ii. Refrain from creating or initiating virus and spam attacks.

iii. Use the existing technologies to minimize effects of virus, spam and other attacks.

2.2.4 User Password

The section ensures that the user has the minimum standard applied to their user password to support the confidentiality, integrity and security of the University ICT resources. This section refers to users of the University resources that require passwords.

Objectives

The objectives are:

to ensure access control to the ICT resources,

ii. to communicate the needs to have protection against unauthorized access and

iii. To establish an ICT environment that will encourage data sharing and exchange without sacrificing security.

Strategies

The Department of ICT is responsible for providing passwords for access to sensitive or controlled environments like email accounts, tests and examinations, restricted rooms, sensitive files and folders as well as various gadgets.

Password holders are expected to act in the following ways:

i. To treat all passwords as private and confidential and not to be divulged, shown or given to any party other than the user.

ii. To change passwords on a regular basis

iii. To create passwords based on numeric and alphabetic combinations with a minimum length of 8 characters.

iv. To create hard-to-guess passwords

v. First time users are expected to change the password immediately after they have been issued the initial default password.

2.2.5 Data Backup & Restoration

Objectives

The objective of this section is to define the backup and restoration of data and information associated with the University operations. This applies to only staff of the University who create, process and store data and information using the ICT resources. With this policy in place, we can ensure copies of critical data are retained and available in case of disaster,

software or hardware failures.

(b) Strategies

The Department of ICT is responsible for:

i. Performing daily back up for the entire critical corporate database for the entire University.

ii. Ensuring safety of backup information by uploading it on cloud

iii. Clearly marking all back up folders with a name and creation date. This will ease identification.

iv. Providing the necessary storage and backup support to staff.

v. Periodically testing the backup disks to ensure they are recoverable.

The Individual users shall be responsible for backing up their own data which is on their own computers and notebook computers.

2.2.6 Software Use Policy

(a) Objectives

The objective of this section is to ensure that the software the University adopts provides the service as expected. This includes the financial management software, human resources, academic records and any other software that may be procured to solve a management problem.

(b) Strategies

The Heads of units shall:

i. Initiate the procurement / adoption of a given software.

ii. Report any bugs or mal functions observed on the software.

The Department shall:

i. Procure the software after approval from the relevant organs.

Procure software licenses after approval from the relevant organs

iii. Install the software on authorized computers or notebooks and record all installed software in a software directory.

iv. The software users shall:

   a. Adhere to the rules and regulations set aside for the proper usage of the software.

b. Report to the ICT Department, any bugs or malfunctions observed on the software.

c. Not manipulate software for whatever purpose

Install copies of personally owned or free software on University machines, and then report such software to the Directorate of ICT and Quality Assurance for recording in the software inventory.

2.2.7 Internet Bandwidth Policy

(a) Objectives

The objective of this is to manage bandwidth use to avoid degradation and ensure network efficacy. Management of Bandwidth resources shall be entrusted to the Department of ICT and Library services.

(b) Strategies

Bandwidth usage shall be subject to the following:

i. Internet Bandwidth will not be over utilized as to prevent access to critical information, research and online educational material.

   Bandwidth allocation shall be made in the following order:

   UniK applications

   e-mail

   internet research

ii. Unauthorized persons/users shall not be allowed to access internet facilities within the campus network

iii. To ensure efficiency and optimal usage by all the users, ICT resources shall be monitored from time to time by the Department of ICT.

2.2.8 Computer Laboratory Policy

(a) Objective

The main objective is to manage use of the computing lab and to maintain its security.

(b) Strategies

In order to keep computer equipment safe, lab users shall abide by the following regulations

i. Any form of eating, drinking, or smoking shall be done outside the lab premises

ii. Lab users are advised to report any problem promptly to the Department

iii. Users are expected not to alter the configuration of hardware or software to suit their need because the set up is intended for a variety of users

iv. Computer labs shall be accessed by only staff and students, any other user must seek authority from the Deputy Vice chancellor

v. The Department staff reserve the right to schedule the users in order to ensure equity in use of the facilities

vi. Only the University, through the Department has the authority to install software of any University equipment

vii. Watching of pornographic material is strictly prohibited

viii. University computer resources shall be used for only legally acceptable business

ix. Users shall only use material where they have access

2.2.9 Personal Computing Devices/Bring Your Own Device (BOYD)

The University shall allow the usage of personal devices on the University network as long as such complies with the University policies and offers a similar level of protection as specified by ICT Technical Department. Such usage shall be subject to the following:

a) The University has the right to access information stored on personal devices where necessary as long as it's used to conduct University business

b) The University is not responsible for the safety of personal devices. All security is the responsibility of the individual owner

c) The University shall have the right to investigate/ audit personal devices in case of any malicious activity, cybercrime or fraud that affects the University

d) Personal devices shall be registered with ICT Technical Department before use on University network

2.2.10 Computer Equipment Policy

(a) Objectives

Due to the variety and nature of work performed by staff and students across the entire University, it is not practical and easy to define a standard operating environment for all equipment. This section provides a guide to what is expected of the equipment used by the University community.

(b) Strategies

i. The Department of ICT is responsible for providing the minimum standards for all equipment used by the University community. Below is a range of equipment with the recommended minimum standards:

Processor: 5th Gen Intel Core i3+ or equivalent

Front Side Bus: 2.7 GHz

RAM: 8GB+, NON-ECC, 1600MHZ DDR3, 2DIMM. Systems developers and power users may need computers with larger RAM

Hard Disk: 500GB+ 7200rpm (Keep Your Hard Drive, 3 Year)

CD-ROM: 16X DVD+/-RW

External Ports: 4 USB 2.0/ 3.0 Graphics: Integrated, up to 256MB shared

Sound: Integrated

Monitor: 21" WXGA LCD Keyboards: 101 key-enhanced keyboard

Mouse: 2 button digital mouse with scroll

Operating System: Windows 10 Professional (64 bit)

Network Capability: Integrated 10/100/1000 Ethernet card

Certification: Must be certified for compatibility with Windows 8 Professional, Windows 8.1 or Windows 10 Professional 64-bit Operating Systems

Warranty: 3 Years onsite (next business day recommended)

Brands: Dell OptiPlex, Hewlett-Packard. Actual brand selection depends on cost, availability of service and maintenance facilities in the country.

Recovery CD to be produced 'after' PC is configured UPS with 'User Replaceable' battery

Minimum Standards for Personal Computers – Notebooks

Processor: 4th Gen Intel Dual Core or More

RAM: 2GB+ DDR3+. Systems developers and power users may need computers with larger RAM Hard Disk: 5000 GB 7200rpm (Keep Your Hard Drive, 3 Year)) or 512 GB SSD/PCIe drive

CD-ROM: Optional/8X DVD+/-RW

External Accessories:1 SD Card Slot; 2 USB 2.0/3.0;21" WXGA LCD, in conjunction with docking station; 101 key-enhanced keyboard;2 button digital mouse with scroll

Graphics: Integrated

Sound: Integrated. Light Sensitive Webcam and Noise Cancelling Digital Array Mic

Display: 13" WXGA Active Matrix / Touch Screen

Modem: Optional

Network Capability: Integrated 10/100/1000 Ethernet card

Wireless Capability: Integrated 802.11b/g/n

Battery: Lithium-Ion 6-cell Power Supply: Universal, auto-sensing (100-240 Volts/50-60Mhz)

Operating System: Windows 10Professional (64 bit)

Warranty: 3 Years onsite / accidental damage coverage

Brands: Lenovo, HP, Dell, Toshiba, and Sony. Actual brand selection depends on cost, availability of service and maintenance facilities in the country/city

Personal Computer Software

Operating System: Windows 8.1, 10 Professional with latest

Service Pack

Bootable Recovery CD for each computer (desktop/notebook) supplied. Recovery CD to be produced 'after' each computer is configured

Recovery CD from manufacturer.

Additional software products and licenses may be required depending on the planned configuration of the PC.

Printers

Hewlett Packard printers, plotters and scanners are the standard. The model purchased will depend on the requirement, either for portable computing, desktop printing or group printing.

Standards for Software

i. **Operating Systems**
   Microsoft Windows 8, 8.1 and 10 Professional

Windows Server (File Server, Application Server)

UBUNTU Open Source

ii. **Office Suite**

MS Office 2007/2010/2013/2016/2019 Professional

Open Office

iii. **Databases**

MS SQL Server, MS Access , Oracle.

iv. **E-mail Server**

MS Exchange Server.

v. **E-mail Client**

MS Outlook 2003/2007/2010

vi. **Browser**

Mozira Firefox, or greater with latest Service Pack

Google Chrome

vii. **Compression utility**

WinZip

viii. **Anti-virus (Desktop, Fileserver**)

KasperSky Antivirus

ix. **Backups (Desktop, Fileserver)**

Veritas BackupExec (Enterprise)

2.2.11 E-Learning

Reference to the UniK E-Learning Policy

2.3 POLICY VIOLATIONS

a) The procedure that follows after a violation of this policy is reported or noticed is that:

i. The HOD ICT will set up a team to investigate the allegation or suspicion. If it is a student being investigated, The Dean of the Students shall be part of the team. If it is a member of staff being investigated, the Deputy Vice Chancellor must be part of the team.

ii. The Head of Department ICT will temporarily suspend or block access to an account, prior to the initiation or completion of such procedures, when it reasonably appears

necessary to do so in order to protect the integrity, security, or functionality of the University or other computing ICT resources or to protect the University from liability.

iii. After investigations are complete, the findings will be forwarded to the UniK management, which will decide whether the suspect is guilty or not, and which will determine the disciplinary action to be taken.

b) Users who violate this policy may be denied access to University ICT resources and may be subject to other penalties and disciplinary action, both within and outside the University. Violations will normally be handled through the University disciplinary procedures applicable to the relevant user.

2.4 IMPLEMENTATION AND EVALUATION

2.4.1 Players

The ICT Department is composed of the Head of Department, ICT Manager, ICT System Administrator, Support desk/ ICT technician, E-learning Coordinator, Web Master, Librarian and Quality Assurance Manager.

2.4.2 Implementation, Evaluation of the UniK's ICT policy

The Implementation and evaluation of the of the UNIK's ICT policy is performed by the Directorate of ICT and Quality Assurance in consultation with the University management.

2.4.3 Monitoring and Review Progress of the UniK's ICT policy

The monitoring and reviewing progress of the UniK's ICT policy is performed by the Department of ICT in consultation with the University management.

2.4.4 Institutional and Regulatory Frameworks

The implementation of this policy shall be operationalised through the existing University institutional structures. Council as the governing body of the University shall ensure that all its organs and officers abide by and implement all provisions of this policy.

2.5 MONITORING AND EVALUATION

Regular and timely monitoring of the progress of this policy shall be carried out **by the Academic Boards of faculties, under the oversight of the Quality Assurance office.** This Quality Assurance Office, on an annual basis, shall review and evaluate progress on implementation of this policy and report to Management.

References:

The UniK Human Resource Manual (2019)

UniK Quality Management Manual (2019)