GREAT LAKES UNIVERSITY OF KISUMU

ICT POLICY 2016

Policy Identification: GLUK/ICT-Policy-02/09-2016

Table of Contents

1. INTRODUCTION

The ICT (Information Communication Technology) refers to technology that is used for processing and distribution of data/information using computer Hardware and Software, Telecommunication and Digital electronics.

The ever-increasing application of Information and Communications Technology is a welcome change being experienced for the past few decades. ICT enhances productivity, improves the work life of personnel and offers a better way of functioning to University Management, Staff and Students.

With the growth, the complexities have also increased and this offers many challenges. These challenges may severely impact the university's brand image and may involve significant social, legal and financial implications.

Therefore the ICT Support Unit of the University has taken an initiative to propose a Comprehensive ICT Policy to be implemented across entire University.

The Policy envisages covering five crucial aspects of ICT as follows:

- ICT Infrastructure
- Human and other resources
- Training - both to ICT related personnel and other Non IT personnel and
- Applications to enhance the utilization of ICT and overall productivity.
- Monitoring: This policy – once evolved and implemented, also presumes a continued monitoring along with periodic review and fine tuning based upon the implementation & operational experience.

This first draft of the Information & Communication Technology Policy of the Great Lakes University of Kisumu has been prepared by the University ICT Support Unit and put forth for consideration and approval of the University Authorities in September 2016. It shall be known as GLUK/ICT-Policy-02/09-2016 and shall be reviewed and updated every year from the date of its first implementation. However, it can be reviewed any time under exceptional circumstances.

This document seeks to evolve a policy regarding the development, upkeep & Operations of ICT Infrastructure, Resources, Training and Applications.

2. PREAMBLE:

2.1 Introduction

The Great Lakes University of Kisumu (GLUK) is an Interdenominational Evangelical Institution. It is a product of Tropical Institute of Community Health and Development (TICH) in Africa, a non-profit community based training, research and development trust which has been operating since 1998. The main aim of GLUK is to develop effective managers of health and development initiatives in the African Region and beyond. This is

achieved by bridging training with service delivery programmes, focusing on the needs of the most vulnerable communities in the society. It develops tests and disseminates hands-on innovative and effective models of development through action research. GLUK brings together regional and international academicians, professionals and practitioners in community health and development of diverse background to pool their skills, expertise and experience in addressing issues of livelihood for action and policy development. The educational experience at the University is enriched by the diversity of the student body. The students are a heterogeneous group, from different parts of Africa and beyond. They range in age and experience from recent high school to college graduate to mid-career managers.

2.2 Vision and Mission of the University

2.2.1 **Vision:** A university that is the centre of excellence in health systems and related fields in teaching, research and service provision, towards empowering communities in the Great Lakes Region of East Africa and beyond, for healthy, peaceful, prosperous and sustainable development.

2.2.2 **Mission:** To develop effective leaders and mangers through relevant programs, for the effective transformation of socio-economic development in the Great Lakes Region of East Africa and beyond.

2.3 Philosophy of the University:

Great Lakes University of Kisumu believes that all people and communities have capacities to undertake individual, collective and collaborative actions to solve their own problems. As partners we build on these capacities.

Rationale: Why ICT Policy?

The academic institutional networks are vulnerable to cyber-attacks world over and specifically in Kenya for two reasons. One, most universities have very limited budgetary provisions for network maintenance & security and two, the universities have weak/loose security mechanism in general, owing to the idea of academic freedom and autonomy on the campus.

In the Great Lakes University of Kisumu, it has become very essential to enact a useful ICT policy for the following reasons:

- ✓ To ensure smooth operations of ICT infrastructure and access to internet
- ✓ To protect its vital information like exam results data, accounts data etc. from unauthorized access
- ✓ To make available minimum internet bandwidth to each academic user to ensure the high availability of academic e-resources

- ✓ To standardize the ICT procurement and maintenance process
- ✓ To enforce and ensure minimum information & network security standards to prevent any misuse from its own users and outsiders
- ✓ To protect its ICT infrastructure from cyber-attacks and to prevent it from being used as a platform to create a cyber-attack somewhere outside the campus

Terms & Abbreviations

1. A "User" means any person, who is authorized to have access to ICT infrastructure of the university. It includes Registered Students of any academic program offered by the university and holder of the valid Identification Card issued by the respective authority of the university or with any other the authentication of the respective dean / head / director / coordinator of the faculty / department / School / institution under the university

   Administrators including Chancellor, Vice-Chancellor, Pro-Vice-Chancellor, Registrar & all executives/officers under the Registrar, Deans of the faculties, Heads of the Departments, Directors/Coordinators of any institution/Schools of the university & officers under them, if any, Members of the Senate.

   Teachers including permanent, temporary, visiting, part-time or any other who is assigned the duty to teach in any of the academic programs offered by the university on remuneration/honorarium

   Non-Teaching Staff including permanent, temporary, part-time, daily wagers, tenure based, on deputation, on-contract or any other who is assigned / hired to perform any non-teaching or technical duties on pay / wage / remuneration / honorarium

   Researchers including Project Assistants /Fellows, Research Assistants/Fellows or any other who is appointed/hired in any research work undertaken by any department/institution of the university

   Guests including visitors from other academic / research institutions / County or Central Government Bodies/Research Funding Agencies etc., delegates of regional / national / international academic seminar / workshop / conferences etc., Vendors, Bankers and other stake holders of Supply Chain Management (SCM)

2. "GLUK" represents The Great Lakes University of Kisumu
3. "University Community" includes Administrators, all categories of teaching & non-teaching staff as well as all categories of enrolled students
4. "User Department" means a Faculty, Department, Institution, Unit or Section of the university, which gives its staff and students access to its ICT resources and GLUK-Intranet
5. "GLUK-LAN" or "GLUK-Intranet" or "Campus-LAN" mean Local Area Network of all Information and communication devices, connected through one or more

communication medium – wired or wireless, across all campuses of the Great Lakes University of Kisumu interconnecting all faculties, departments, offices and institutions of the university

General Guidelines:

1. All users should be aware that several network usage issues are covered by the National ICT Policy, violation of which is an offence under national law.

2. The GLUK campus-LAN and Internet access resources are meant for official use arising from the academic/research activities and administrative responsibilities of the faculty, staff and students of the University. Use of network resources for personal purposes is discouraged.
3. Users should view the ICT & network resources with a sense of ownership and participation, and should actively help to prevent any misuse. Procedures laid down from time to time regarding the management of ICT & network resources, must be understood and followed meticulously by the user community.
4. The ICT Support Unit has the right to monitor and scan all information carried by the network for the purpose of detecting and identifying inappropriate use. As such the privacy of information carried by the network is not guaranteed. ICT Support Unit is authorized to break open a PC OR disconnect it from the network, if called for. However, specific scanning will be done only on approval / post facto approval by a competent authority. This is in accordance with the National ICT Policy.
5. Every user is expected to be aware of the contents of this policy document, and agrees to abide by its provisions. Once adopted, this policy should be publicly posted (for example, on the GLUK web site), and all individuals who use ICT & network resources of the university should be made aware of this policy.
6. Every effort will be made to aggressively publicize the policy and make it widely understood and accepted, by holding training sessions for end users, circulating training material, organizing personal meetings and so on.

3. INFRASTRUCTURE:

ICT Infrastructure comprises of Hardware, System and Application Software and Communications Infrastructure – wired and wireless, like cables and networking equipment etc. used in internal as well as external communications.

3.1. HARDWARE:

Hardware comprises of various items that are used by the end users as well as the items that are used to support the use of ICT by the end users. For example, Servers, Desktops, Laptops, Tablets, Mobile Phones, Printers, Scanners, UPSs, Network Switches etc. and various other equipment.

3.2. SOFTWARE:

System Software comprises of software that makes the system function and constitute an integral part of the system. For example, Operating System is a System Software and common applications like E-Mail Client can be considered to be an Application Software.

System Software are proprietary e.g. Windows OR in Public Domain e.g. Linux. Application Software include MS-Office, MS Outlook etc. are proprietary whereas Thunderbird E-Mail, Open Office Suite etc. are Open Source Software.

As far as it is practicable and consistent with the intended purpose, Users ought to prefer Public Domain Software which is available either free OR at a much lower cost.

Software for Common Usage should be identified and implemented across the university in order to achieve consistency of formats and ease of sharing common data.

3.3. COMMUNICATIONS INFRASTRUCTURE:

Covers the means of ICT based Communications – wired and wireless, both within the University as well as outside the University. It comprises of Cables, Junction Boxes, Switches, Modems, Routers, Access Points and similar networking equipment.

4. ICT PROCUREMENT & MANAGEMENT POLICY:

4.1. PROCUREMENT POLICY

1. ICT Support Office is responsible to define, review, revise, approve & circulate/publish on website the procurement policy for the ICT equipment once in every year.
2. All users/user departments must adhere to the policy guidelines published by the IIM Committee.
3. All users / user departments must take prior approval of IIM Committee for requirement and specifications of the ICT equipment they wish to procure.
4. The committee should meet once every month before the procurement committee meet

5. The committee shall strive to standardize the terms & conditions as well as the process for the procurement of ICT equipment and software in line with the Public Procurement Act.
6. It must perform the vendor evaluation and registration process every two years to identify & register the vendors for the general purpose ICT equipment and circulate the same to all user departments
7. The procurement process should also be in accordance with accounting & auditing provisions and guidelines of Commission of University Education.
8. Bulk procurement by combining the requirements of similar equipment should be encouraged to achieve optimum cost benefits. Procurement of equipment / software from Original Equipment Manufacturer (OEM) vendor must be preferred.

The following aspects must get a consideration, as a part of ICT Procurement Policy:

Feasibility: If an item / technology does not already exist and is being introduced, an appropriate justification for introducing new item / technology must be prepared. It must also consider the alternate technologies explored and the reasons why the choice for the selected technology was made.

Cost Benefit: The initiator of the proposal must submit a statement of the cost – benefit expected from the procurement. In case the benefits are subjective, a subjective assessment in terms of the underlying criteria and their rankings from points 1 to 10 must be submitted. This will help the technical staff to match the requirement with the technology being procured.

Plans and Budgets: It is desirable that all Faculties and Departments plan their ICT requirements in advance and provide for the same in their budgets. The budgets must cover Capital Investments as well as recurring, operational expenses. This will help in controlling the monetary outflow while enhancing the ICT Resources. The specifications and configuration submitted for procurement must be consistent with the intended usage and should be derived in consultation with members of the ICT Infrastructure Management Committee.

Financing: Appropriate means for financing must be available for ICT Procurement. Experts in Finance at the University may appropriately suggest leasing and other means for funding the procurement appropriately. It is also desirable that a common pool is available such that in case a procurement having merit is falling short of the budget, it can supplement the budget.

Accounting: Entire ICT Infrastructure including Hardware, Software and Communications Equipment comes at a cost and certainly needs to be accounted for accurately. These items must be treated as assets and their procurement, transfers and disposals must get reflected in the Accounts Books of Assets at any given time.

Insurance: There must be a policy for Insurance for ICT and each item must get covered either in general Insurance Policies OR - for specific items - must get covered under specific policies related with Electronics Items. For example, Servers must get covered in Policy for Electronic Items with Data Restoration. Insurance against loss of data and cost of recovery also should be considered.

Systems Audit: There must exist a system of cross checks and physical verifications of ICT Assets to ensure that all assets exist; they are functioning as expected, are technically fit and not obsolete. Such audit help in determining in advance the items that need replacements over

a period of time and so, can be well planned. This activity will prevent any degradation of efficiency in the ICT Services.

Information Security: There are different aspects of Information Security. They are broadly classified as Digital and Physical. Security related to Digital Devices is related with Passwords, Access Rights, Backups, Anti-Virus Measures, use of external media and so on. Physical Security involves securing parts of physical location to regulate its access, to restrict only authorized personnel, to provide for smoke detectors and fire alarms, to enable monitoring through CCTV Cameras and so on. On the other hand, Physical Security covers classification, storage and upkeep of documents, regulating access to classified documents and arranging for their safe custody, sharing of confidential information, inadvertent leakage of classified information and so on.

Outsourcing: In the modern world, outsourcing is beneficial and cannot be avoided but there are many aspects that need to be considered while outsourcing activities or while having external staff working within University premises. These concerns are related with providing information related with outsourced jobs, getting certain repairs done, disposing off items / equipment and so on – all of which must be carefully carried out considering ICT Security and safety in mind. Similar care should be taken while executing any turn-key projects in the area of ICT implementation.

Best Practices: There must be personnel earmarked to keep abreast of the developments in Technology, who must be assigned the identification of appropriate avenues wherein new technology / products may be profitably deployed. They must also keep themselves aware about the Best Practices desirable and / or being followed elsewhere, which may be beneficial to the university.

4.2. MAINTENANCE/UPGRADATION POLICY

1. On procurement & installation of any new ICT device/equipment, User department must allocate a unique dead-stock number (Asset Identification Number) in the dead-stock/Asset Register. The same number must be written on the front side of the device/equipment, which can be used for physical verification. The same must be appropriately updated while transferring out OR disposing/writing off such assets.
2. User department must be vigilant about warranty checks and must take appropriate action if the performance of the device/equipment deviates from the expected performance.
3. After the completion of the warranty period, User Department may implement the Annual Maintenance Contract (AMC) for the device/equipment depending on the criticality of its usage, with the approval of the ICT Support Office& following the standard procedure laid down by the university from time to time.
4. The ICT Support Office shall define, review, revise, approve and circulate/publish the guidelines & procedure for up-gradation of outdated ICT devices/equipment/components or to improve the performance of existing ICT devices/equipment/components and software. The upgradation of devices/equipment can be through increasing the performance capacity by adding/replacing some components, like memory, HDD, Graphic card etc. or by replacing the whole device/equipment through a buy-back mechanism depending on the specifications and performance parameters of the device/equipment. A prior approval of specifications and requirement by the IIM Committee is essential.
5. Necessary budget provisions must be made by the respective user departments for the maintenance and up-gradation of its ICT equipment and software.

4.3. POLICY FOR WRITING-OFF ICT EQUIPMENT

ICT Support Office is responsible to define, review, revise, approve and circulate/publish the guidelines & procedure to scrap and write off the non-functional, non-operable, non-repairable and obsolete ICT devices/equipment.

It must perform the vendor evaluation and registration process to identify & register the vendors specialized in disposal of e-scrap or digital scrap.

5. ICT USAGE POLICY

5.1. FAIR / ETHICAL USAGE GUIDELINES

1. All users are expected to make use of the ICT resources accessible to them with sensibility and awareness.
2. The GLUK-Intranet and Internet access will not be used for commercial activity, personal advertisement, solicitations, or promotions, such as hosting or providing links of commercial websites or email broadcasts of commercial promotions to the users.
3. Any part/component of the ICT infrastructure of the university shall not be misused for Anti-University, Anti-State or Anti-Government activities.
4. As such, non-GLUK organizations (such as commercial outlets operating on the GLUK campus) will not be connected to the GLUK-Intranet, and cannot be a part of the GLUK domain space.
5. The downloading of audio and video files is to be done strictly for official purposes.
6. Each user must preserve & maintain the confidentiality of the password used by him/her. No user must try to access the ICT resources using other user's password, either knowingly or otherwise.
7. Access to sites that are banned under law or that are offensive or obscene is prohibited. This is also an offence under the National ICT Policy and attracts severe punishment.
8. Use of the network to tamper with information on other computers, to deliberately spread harmful/pirated programs, compromise other systems, or to cause damage of any kind using the intranet/internet is prohibited, and is an offence under the National ICT Policy. The user is liable for any civil losses caused, in addition to criminal prosecution under the National ICT Policy.
9. No equipment/user other than those registered with the University, can be used to connect to the intranet.

5.2. CENTRALIZED AUTHENTICATION OF USERS

1. ICT Support Unit is responsible to devise a mechanism for management of registration and access policy for all users using, for example, LDAP or Active Directory or any other appropriate software. It should provide a GUI based platform for user administration through which user departments can administer their users in the centralized database of users in LDAP or Active Directory.
2. The head of every user department is responsible to add/modify the information about its users and their access rights on centralized user database managed by ICT Support Unit. The head may designate a staff member, preferably a permanent staff member, to assist him/her for the user information management of its users on the central user

database and inform the ICT Support Unit about the same. ICT Support Unit shall provide necessary training to all heads and designated staff members to manage the user information of their respective user department.

3. The user department shall update information of its students after finalization of admissions once every year. The modification of user data for teaching/non-teaching staff and any other user must be updated immediately by the user department with the change in the user status. Individual user is not responsible for updating of his/her information in the user database.

5.3. INTERNET & INTRANET APPLICATION SOFTWARE USAGE ONLY BY REGISTERED USERS

1. Registered users will be allowed access to internet facilities and audio and video downloads depending upon their access rights.
2. Users with selected privileges will be allowed access to Intranet Application Software of the university. For example, only staff of the academic and examination section and faculty shall be given role based access to add/modify/delete relevant data in the Student Management Information System (university ERP).
3. Every Application Software deployed in the university, whether developed in-house or through outsourcing or readymade or cloud based, shall have one administrator user designated by the university. It is the responsibility of the administrator user to manage user access rights. However, non-IT administrators must take guidance and assistance of the ICT Support Unit in resolving technical issues of the software.
4. Access of non-academic websites, download of music/movies and non-academic videos etc. must be restricted for all users.
5. Faster access to e-journals subscribed through academic consortia, National Digital Library & other such projects should be ensured.

5.4. SHARING OF HARDWARE RESOURCES LIKE DESKTOPS, PRINTERS, SCANNERS ETC. BY EMPLOYEES & STUDENTS

1. ICT resources are limited and users are more. Hence, the resources have to be shared sensibly and effectively.
2. Use of network Office equipment like Network Printers and Network Scanners should be encouraged.
3. Minimum computer-student ratio of 1:2 in every teaching department offering IT programs / courses and a ratio of 1:4 to 1:6 in non-ICT programs/courses is desirable.
4. A desirable Computer-staff ratio of 1:2 should be maintained in research departments/institutions. A desirable Computer-staff ratio of 1:3 should be maintained in all other non-teaching / administrative departments/sections/offices.
5. Due care should be taken not to overwrite / delete other users' data on shared resources. In case of any difficulty, guidance and support can be taken from the ICT Support Unit.

5.5. UNDERTAKING FOR FAIR USAGE BY ALL REGISTERED USERS (Legal Requirement)

ICT Infrastructure Access Agreement

Please Read the following the ICT Usage Policy of the Great Lakes University of Kisumu CAREFULLY before accepting/rejecting the policy.

The Great Lakes University of Kisumu, ICT Support Unit Undertaking with respect to the ICT Usage Policy Whom this Document Concerns All Users of ICT infrastructure (Computers and the Network) at GLUK

Reason for Policy

This policy outlines the responsible use of the Information & Communication Technology Infrastructure at GLUK.

Statement of Policy

All users of the ICT facilities of GLUK will be subject to the following Acceptable Use Policy

1. [Content] I shall be responsible for all use of this network. In case I own a computer and decide to connect it to GLUK network, I will be responsible for all the content on it, especially that which I make available to other users. (This provision will also apply to any computer or device for which I am responsible, and is included in the meaning of "my computer".) In case I do not own a computer but am provided some ICT resources by GLUK, I will be held responsible for the content stored in the designated workspace allotted to me (examples: file storage area, web pages, stored/archived emails, on ICT Support Unit or Department machines).

2. [Network] I will be held responsible for all the network traffic generated by "my computer". I understand that network capacity is a limited, shared resource. I agree that physically tampering with network connections/equipment, sending disruptive signals, or making EXCESSIVE USE of network resources is strictly prohibited. Repeated offenses of this type could result in permanent disconnection of network services. I shall not share the network connection beyond my own use and will not act as a forwarder/ masquerader for anyone else.
3. [Academic Use] I understand that the ICT infrastructure at GLUK is for academic use and I shall not use it for any commercial purpose or to host data/network services for other people or groups. Also, I shall not host or broadcast information that might harm others or may be otherwise considered objectionable or illegal as per provisions of Indian law.
4. [Identity]I shall not attempt to deceive others about my identity in electronic communications or network traffic. I will also not use GLUK ICT resources to threaten, intimidate, or harass others.
5. [Privacy] I will not intrude on privacy of anyone. In particular I will not try to access computers (hacking), accounts, files, or information belonging to others without their knowledge and explicit consent.
6. [Monitoring]I understand that the ICT resources provided to me are subject to monitoring, with cause, as determined through consultation with the GLUK

administration, when applicable. The monitoring may include aggregate bandwidth usage to effectively manage limited ICT resources as well as monitoring traffic content in response to a legal or law enforcement request to do so. I authorize GLUK administration to perform network vulnerability and port scans on my systems, as needed, for protecting the overall integrity and efficiency of GLUK network.

7. [Viruses] I shall maintain my computer on this network with current Antivirus/Internet Security/Endpoint Protection software and current updates of my operating system, and I shall attempt to keep my computer free from viruses, worms, Trojans, bots, malware and other similar programs.
8. [File/Data Sharing] I shall not use the ICT infrastructure to engage in any form of illegal file/data sharing (examples: copyrighted material, obscene material).
9. [Security] I understand that I will not take any steps that endanger the physical or logical security of the GLUK network. Specifically, I will not attempt to bypass firewalls and access rules in place. This includes not setting up servers/communication devices (including wireless) of any kind (examples: web, mail, proxy, router, managed or unmanaged switch, smart phones) that are visible to the world outside the GLUK campus. In critical situations, GLUK authorities reserve the right to disconnect any device or disable any account if it believed that either is involved in compromising the information security of GLUK.
10. [Penalties] I understand that any use of ICT infrastructure at GLUK that constitutes a violation of GLUK Regulations or provisions of Kenyan Cyber Law could result in administrative or disciplinary or legal procedures. Your access will be automatically suspended/BLOCKED completely, if the ICT Infrastructure Access Policy is not ACCEPTED by you.

6. ICT SECURITY POLICY

6.1. DESKTOP SECURITY POLICY

6.1.1. PHYSICAL SECURITY OF SERVERS, DESKTOP, LAPTOP, THIN CLIENT, PORTABLE DEVICES ETC.

1. The user department where the ICT equipment is installed and used, either temporarily or permanently is responsible for the physical security of it.
2. It is responsible for allowing the physical access to the ICT resources only to authorized users.
3. It is also responsible to ensure proper power supply with effective grounding (earthing), proper furniture as well as cleanliness of the equipment and environment including air-conditioning machines.
4. The user department must ensure proper load on electricity meter before installing additional ICT equipment or other allied equipment like air-conditioning machines etc. The user department must get the power load on electricity meter checked by KPLC every 2 years. The power load on electricity meters must be calculated and increased taking into account requirements of next 2 years.
5. Users of a user department can access the network via desktop/laptop computers on the campus network. Users are responsible and accountable for the usage of the systems allocated to them.

6. Users must take adequate & appropriate measures to prevent misuse of network from computer systems that they are responsible for.
7. Individual users as well as User departments should take reasonable care of the vulnerability of systems attached to the campus network. In particular, users must apply appropriate service packs, browser updates and antivirus and client security solutions in their MS Windows machines, and necessary upgrades, OS patches, browser updates etc. for other systems.
8. If a user department wishes to set up its own Internet access facility, then it should be done under support and monitoring of the ICT Support Unit and ensure that deploying such an access facility does not jeopardize the security of the campus network. The user department must completely adhere to the provisions of this ICT Policy for such facility.

6.1.2. USE OF LICENSED SOFTWARE

1. Software programs are covered by copyrights and a license is required for their use.
2. Legal, free and compatible alternatives are available for a large number of applications / software and users must evaluate them, rather than straightway going for software having a cost.
3. Users / User departments must ensure that they have either an academic, commercial or public license (as in the case of 'free' software) for any software they install on the systems that they are responsible for.
4. Use and exchange of pirated / illegal software over the GLUK-Intranet is prohibited. It is the responsibility of the head of the user department to ensure compliance.
5. The downloading and use of software that is not characterized as public domain or 'free' is prohibited.
6. Use of Open Source Software is encouraged to avoid financial burden and legal complications arising out of license management. For example, use of King soft Office or Open Office must be preferred over MS-Office, Thunderbird E-Mail Client as against MS Outlook.
7. ICT Support Unit should arrange for the training of general purpose Open Source Software for all the users

6.1.3. USE OF ANTI-VIRUS & INTERNET/ENDPOINT SECURITY/PROTECTION SOFTWARE

1. The user department is responsible for installation and maintenance of proper Anti-virus or Internet/Endpoint Security/Protection Software or any other security software as prescribed by the ICT Support Unit.
2. In case of detection of any issues in the security, the compromised computer/equipment must be disconnected from the GLUK-Intranet failing which ICT Support Unit shall disable the respective network connection.
3. Strict action may be taken by the ICT Support Unit against users who deliberately prevent installation of such security software OR disable such software OR prevent them from running.

6.1.4. STATEMENT OF RESPONSIBILITY

1. User Department is responsible for security of ICT infrastructure & resources under its control and usage. One permanent staff member shall be designated to supervise and help maintain the ICT security through coordination, guidance and training with the ICT Support Unit.
2. ICT Support Unit is responsible to provide guidance and training to all user departments in maintaining due security of ICT infrastructure. It is also responsible in monitoring the implementation of ICT policy on GLUK campus.
3. University Administration is responsible to provide necessary administrative and financial support to ensure the ICT infrastructure and resources required for implementation of ICT policy.
4. In the eventuality of cyber-attack/crime/fraud or any other cyber security incident on or using ICT infrastructure of the university, affected department/section/institution shall perform technical/legal procedure in technical coordination with ICT Support Unit and guidance of Legal Unit of the university. In case of national level cyber security issue, full cooperation of the user department, ICT Support Unit shall be extended to the Cyber Crime Cell of the Government, NIS and other agency authorized by the county or central government.

7. INFORMATION SECURITY POLICY

7.1. DEFINITION OF CRITICAL INFORMATION

Critical Information Classification is the classification of information based on its level of sensitivity and the impact to the University should that information be disclosed, altered or destroyed without authorization. The classification of information helps determine what basic security controls are appropriate for safeguarding that information. All institutional information should be classified into one of three sensitivity levels, or classifications:

Restricted Information, which is highly valuable and sensitive. The unauthorized alteration, disclosure or loss of this information can cause significant damage (devastating) to the university, for example, examination results under process, accounts etc. This information must be highly protected as it cannot be easily recovered or brought to its original state easily.

Private Information, which is of moderate importance and sensitivity. Its unauthorized alteration, disclosure or loss of this information can cause moderate damage to the university. Generally, the information which is not classified in other two classes falls under this. Reasonable and effective security is required for this information, as recovery of its original state may take sizable amount of resources.

Public Information, which is of low importance and sensitivity. Its unauthorized alteration, disclosure or loss of this information can cause little damage to the university. Public information includes press releases, circulars, notifications, course information and research publications, published results on website etc. While little or no controls are required to protect the confidentiality of Public information, some level of control is required to prevent unauthorized modification or destruction of Public information.

All information created, processed, generated, maintained and deleted by the university must be classified into these categories and different levels of user privileges must be defined for each function. Only authorized users can get access to the category of information he/she is authorized to access.

7.2. BACKUP POLICY

1. Every user and user department should manage & maintain backup of data stored on the computers under their control based on its level of criticality. Daily/twice a day / thrice a day backup of Restricted Information must be taken depending on its frequency of updates. The backup of server data must be maintained on designated desktop computers by increasing its storage capacity, on regular basis to prevent any data loss in certain incidents.
2. Backup of official data on laptops, external hard drives or any other mobile/removable media should be discouraged.
3. Backup or temporary storage of official data on free public cloud storage facilities like Drop Box, Google Drive, OneDrive etc. is unsafe and prohibited.
4. No user/user department should take official data outside the GLUK campus without necessary authorization.
5. ICT Support Unit should provide Centralized storage facility for all user departments to store backup of their official data only on GLUK-intranet. No access to this backup shall be allowed from internet outside the campus. User departments can store ONLY OFFICIAL AND CRITICAL information using the centralized backup solution. A backup of Critical / Confidential Information SHOULD BE stored in the local Hard Disk as well as on removable media which may be stored in fire-proof/water-proof safes at different locations to protect critical data from manmade or natural calamities.
6. Periodicity of the backup should be decided based on the level of criticality of information.
7. Information should be classified based on its level of criticality. Users with special privileges should have the accessibility of different levels of critical information.

7.2.1. STATEMENT OF RESPONSIBILITY

1. ICT Support Unit is responsible to facilitate guidance, support and training to user departments in managing their backup of data.
2. ICT Support Unit should provide a network based storage solution like NAS to automatically obtain backup of their Central Repository including restricted/private information.
3. It is the ultimate responsibility of the user / user department to manage the backup of their data.

8. NETWORK MANAGEMENT & SECURITY POLICY

8.1. STRUCTURE OF GLUK-INTRANET – WIRED & WIRELESS

The GLUK-Intranet consists of about 300 nodes connected through UTP semi-structured cabling with a layered architecture of L3, L2 and EDGE switches with wireless radio backbone to its campuses. Campus-Wi Fi is implemented across the campuses.

The ICT Support Unit is the nodal agency responsible for establishment, maintenance and management of the campus-LAN. All the technical aspects of network related activity like, defining specifications of network components, establishment, maintenance and management

of wired and wireless LAN, strategic planning for expansion of LAN, management of internet bandwidth and gateway, Network Security Management is the sole responsibility of the ICT Support Unit.

1. ICT Support Unit is responsible for the core GLUK network (includes Internet facilities: email, web etc.).
2. ICT Support Unit will provide connectivity to each User Department, to the backbone, and also the necessary IP addresses, proxies, email relays etc.
3. If any node or part of GLUK-Intranet "misbehaves" and causes problems for any other user department or the entire campus, or disrupts services, ICT Support Unit will notify the concerned Head and disconnect the node or part of GLUK-Intranet from the core network until the problem is fixed satisfactorily.
4. ICT Support Unit will decide which web sites can be accesses through the campus internet and, shall disallow access to other sites and maintain a mechanism suitable to enforce such a purpose.
5. University is receiving25Mbps internet connectivity through Access Kenya. This will eventuality be upgraded on need basis. There is no backup connectivity.

8.2. METHODOLOGY OF IMPLEMENTATION & EXPANSION OF LAN INCLUDING CAMPUS WI-FI

ICT Support Unit should define and implement the best methodology for optimum implementation and effective utilization of the campus-LAN. It should define the standard specifications for laying of OFC, structured UTP cabling and Wi-Fi for optimum network performance.

1. Standards and specifications for laying OFC (to be defined)
2. Standards and specifications for structured UTP cabling (to be defined)
3. Standards and specifications for campus-Wi-Fi (to be defined)

8.3. MAINTENANCE OF GLUK-INTRANET INCLUDING ROUTERS, SWITCHES, CABLING, AP ETC.

Maintenance of active & passive network components is very important for the health and performance of any network.

Routers, core switches are costly components and need to be taken care of well.

Only manageable switches and components including APs should be used. Use of unmanaged network components is strictly prohibited.

Proxy Servers and DHCP servers shall be configured and maintained by the ICT Support Unit only. However, any user department wanting to configure its own DHCP server and use its own range of IP addresses must use the IP range other than GLUK-Intranet and communicate all the configuration details of its VLAN to the ICT Support Unit.

Use of open proxy servers or any other mechanism to bypass the defined security configurations at any level without prior permission from the ICT Support Unit shall be treated as breach of policy and dealt with strictly.

Any user department wishing to use live IP addresses for its applications shall obtain a written permission from ICT Support Unit who then shall allocate live IPs in writing to the user department. It shall be the sole responsibility of the user department to ensure that no security or operational difficulties/threats are created in GLUK-Intranet. ICT Support Unit shall maintain the records of all live IP addresses.

ICT Support Unit should be given separate budgetary provisions for network maintenance

Wired and wireless networks should be kept separate for more efficient network management.

User departments must cooperate in providing necessary space and power supply for installation of network components/devices at technically appropriate place defined by ICT Support Unit in their premises.

ICT Support Unit will evaluate, procure and deploy and appropriate Network Management Software Application to ensure its uptime, security, efficiency and effectiveness.

8.4. BANDWIDTH MANAGEMENT

Network Management is one of the core functions of the ICT Support Unit. University has 25 Mbps Internet bandwidth through Access Kenya (ISP). Distribution of the bandwidth across the campus-LAN is a very important aspect of bandwidth management. The bandwidth management should give priority to academic contents, Application Software implemented by the university, research projects, University Website & E-mail facility etc. over general Internet browsing and other utilities.

8.5. INTERNET GATEWAY SECURITY

Securing Internet Gateway is a very challenging task. ICT Support Unit is solely responsible to ensure effective security of the gateway. Enterprise Firewall or Unified Threat Management Solution must be implemented effectively with strong policy definitions in line with ICT policy of the university. University Administration must provide an active administrative support to secure the internet gateway by the ICT Support Unit.

8.6. LAN (GLUK-INTRANET) SECURITY INCLUDING SWITCHES, UTP CABLING, POWER SUPPLY & WI-FI

ICT Support Unit is solely responsible for the maintenance of campus-LAN. However, the respective user departments must take care of network components installed in their premises and ensure physical security of them. The user department should also provide adequate power supply for network devices in stalled in its premises.

8.7. STATEMENT OF RESPONSIBILITY

1. ICT Support Unit is responsible for physical as well as operational security of internet gateway and other network components and the operational security of network components – Active or Passive, up to EDGE switch level.
2. User Departments are responsibility for security of all Network Components – Active or Passive, installed in their premise as part of GLUK-Intranet.

9. APPLICATIONS SOFTWARE:

Applications in the current context cover the software procured / developed and deployed to carry out a given function of the university.

With the increasing usage of the technology, it is worthwhile introducing new applications to profitably utilize the available infrastructure and derive the benefits of enhanced productivity as a result.

The Applications may be custom developed as per the specific requirements of the functional area. The development may be carried out by internal resources or may be outsourced to Application Development Agencies. The students undergoing various courses, who are required to undertake live projects, also constitute an attractive talent pool which can be harnessed towards this objective.

An alternate to Custom Development of applications is to procure and implement a readymade application. With the advent of Web and Cloud based computing, various cost effective and rich applications are increasingly available that can meet the requirements of given function(s). Depending upon the size and complexity of the application, the investment varies from being free / nominal to multiple millions of shillings.

Looking at the benefits, more and more applications must be deployed for various functions across the University. Preferably, the applications must be centralized, developed/procured by a central authority and deployed as needed. All the implementation and installations of such Application Software must take place under the guidance, supervision and support of the ICT Support Unit. Such Application Software must comply with the provisions of the ICT Policy.

To keep it very brief, the Applications can be introduced with the following methodology:

1. A brief outline of requirements by the User Department to the Head of Software Development Team / ICT Support Unit
2. Elaboration of the requirements in consultation with the proposer, by the Head of Software Development Team / ICT Support Unit
3. Discussion between them and modifications in the requirements, if needed
4. Finalization of mutually agreed Functional Requirements, Specifications Document
5. Decision whether to look for a readymade product / solution OR to develop a turn-key solution as per the requirement
6. Procurement / Development of the Application
7. Testing of the application to ensure fulfillment of the requirements
8. Training to the users to operate the application
9. Deployment, Implementation, Support for the Application
10. Standard Operating Procedure (SOP) for various user application software must be clearly defined and strictly adhered to.

10. TRAINING:

The University is a long existing establishment and people from diverse academic and social backgrounds and difference age groups work in various positions. Not all of them can be expected to be IT Savvy. Moreover, new technologies and tools are being introduced and it is essential that not only the people who operate these, but even the others who are impacted by it and those who are responsible for implementation, must be appropriately trained. Therefore Training is a very important activity and it must be an ongoing activity in the University.

Training does not necessarily mean classroom training. It can be imparted by publishing Training and Reference Material on Intranet, by circulating printed material, through E- Mails and such other means as appropriate.

Therefore the Training Activity must aim to cover each employee in at least one Training Program in one year.

Elaborate requirements for Training can be determined by the ICT Support Unit based upon the current status of deployment of IT Infrastructure and the awareness of the people but nevertheless, the need for continued training as an important activity cannot be emphasized more.

After all, whatever may be the merits of different tools and gadgets being deployed, until the people who utilize them are knowledgeable enough, the value derived from such investments will be negligible.

So the proposed ICT Policy recognizes and appreciates the criticality of Training and suitable actions will be taken to execute it on an ongoing basis from a long term perspective.

11. RESOURCES:

The ICT Policy proposes to attach considerable importance to optimal utilization of Resources. Various resources needed to implement IT based activities must be consistent with the objectives of the activities. Resources needed must not be disproportionate to the objective for which they are being made available.

It is from this angle that the Policy proposes Planning and Budgeting on the part of all Faculties and Departments, especially ICT Support Unit such that the resources required can be planned for and made available on time when needed.

Those submitting Purchase Indents OR various proposals for investment, must try to assess their needs, available options and must finalize the requirements keeping the investment requirements to the minimum possible. For example, if the job can be effectively carried out by using LINUX Operating System with Kingsoft Office / Open Office Products, one must assess these options against Windows & MS Office Options so as to minimize Investment Requirements.

Such Financial Plans / Budgets must also take into account the recurring operational expenses, besides the capital investments. For example, if a new printer is purchased today, the expenses for its Ink/toner Cartridge also must be provided in the budget.

As in case of Financial Resources, the Faculties and the Departments – more so, the ICT Support Unit, must also plan out their activities for a new year and thereby, plan for Human Resources well in advance. This will help in getting suitable personnel meeting the requirements, orienting and training them to take up the envisaged responsibilities effectively.

12. VARIOUS COMMITTEES

12.1. ICT POLICY ADVISORY COMMITTEE

ICT Policy Advisory Committee (ICTPAC) is responsible for creating, reviewing and recommending the ICT Policy for the university.
The main functions of the committee shall be as follows.

- To define, review and recommend ICT policy and modifications in the policy
- To define the standard formats to collect data/feedback of various ICT functions of the university quarterly/half yearly, which can be useful to analyze and review various ICT functions, including Information & Network Security.

Proposed Constitution of the Committee as under.

i. Vice Chancellor – Chairperson
ii. ICT Support Officer – Member Secretary
iii. Registrar Administration – Member
iv. HoD IT - Member
v. Quality Assurance Manager – Member
vi. Chief Accountant – Member
vii. Any three Invited Experts nominated by the Vice-chancellor preferably with expertise in the field of Cyber Law / Information System Audit / Networking – Member

The committee can co-opt additional members for specific purpose.

12.2. ICT INFRASTRUCTURE MANAGEMENT COMMITTEE (INCLUDING PROCUREMENT)

ICT Support Office is responsible to define, approve & circulate the specifications of all ICT equipment requirements once in every year or an need arise. The committee should meet once every month before the Procurement committee.

The principal functions of the committee shall be as follows.

1. To define, approve and circulate Standard, minimum, generic specifications of commonly used ICT equipment
2. Vendor Registration & Evaluation
3. Standardization of procurement process – quotation & tender documents with

   uniform and consistent terms & conditions in concurrence with the purchase policy of the university

4. To define guidelines for maintenance of separate Dead Stock register (Asset Register) for ICT equipment

5. To define guidelines for management of licenses of various software – Procurement, licenses, Record Maintenance, upgrades agreements etc.
6. To define guidelines for management of Memorandum of Understanding (MoU) / Service Level Agreement (SLA) with hired IT solution providers, Annual rate Contract (ARC), Annual Maintenance Contract (AMC), Campus Agreement etc. related to ICT Software, Applications &Equipment.
7. Software procurement policy & use of Open Source Software
8. To define guidelines for document tendering or e-Tendering process for ICT equipment/solutions
9. To define guidelines for writing off obsolete/outdated ICT hardware & software
10. Annual Internal Audit for verification of regular upkeep of the ICT infrastructure by the User Departments under their control, Network Performance and Security Audit and Information Security Audit

As regards procurement of Materials related with IT, the following standardizations should be considered:

i. Identification of Items generally being purchased regularly – for example, servers, Desktop PCs, Laptops, Printers, consumables etc.
ii. Identification of a few selected Brands of these items
iii. Identification of a few selected vendors who supply these brands
iv. Working out (preferably three) sets of configurations from bare minimum to the highest possible level, against which the specific requirements may be matched and the appropriate configuration meeting the requirements may be identified.
v. The procurement may be carried out from the identified vendors for the selected configuration.
vi. This will help in procurement of items that fulfill the requirements with desired level of performance without unnecessarily increasing the investment due to an unduly higher configuration.

ICT equipment & software procurement sub-committee and ICT equipment & software write-off sub-committee can be constituted from the members of the IIM committee.

Primary responsibility of Implementation of all aspects of ICT Policy should be of ICT Support Unit under the supervision of ICT Policy Advisory Committee and with necessary administrative and financial support of the University.