# KILIMANJARO CHRISTIAN MEDICAL UNIVERSITY COLLEGE

**(A Constituents College of Tumaini University, Makumira)**

# INFORMATION COMMUNICATION TECHNOLOGY POLICY

**February 2022**

## Policy Indexing Information

| **Policy Name** | **Information Communication Technology Policy** |
|---|---|
| **Approving Authority** | College Governing Board |
| **Approval Date** | 25th February 2022 |
| **Policy status** | 1st Revision |
| **Date of Revision** | January 2022 |
| **Custodian** | Department of Information Communication Technology |
| **Owner** | College Governing Board |
| **Policy Index Number** | ICTP/004/CGB44/21/2.31 |
| **Date of Next Review** | January 2025 |

## 1.0 BACKGROUND

The KCMUCo ICT Policy was first formulated in 2016 to guide the identification, promotion and appropriate utilization of ICT resources and ensure that ICT applications are integrated into the planning and operations of the College. The use of ICT provides opportunities for the College to cope with the challenges of training increased numbers of competent health professionals during these times of knowledge society. It is thus imperative for the College to acquire the appropriate and adequate human resources, infrastructure, hardware, and software to facilitate optimal deployment of ICT services to accelerate the College growth through improved outputs of its core functions. To achieve this and in the light of increasing recruitment of faculty, expansion of teaching programmes and therefore expansion of enrolment, which heavily depends on an efficient ICT network, the College needed to review its ICT policy to match technological advancements and take care of worsening cyber security.

Through this policy, the College will ensure that its ICT resources and facilities are used solely for their intended purposes. Thus, the formulation of this policy is driven by the need to guide proper planning, development, deployment, and use of ICT services at the College.

ICT is fundamental in facilitating KCMUCo core functions, i.e., teaching, research, and service. The importance of ICT in innovation for knowledge generation and technology transfer geared at enhancing national development as a component of education for life has been embraced in the College strategic plan. KCMUCo, therefore, reaffirms its commitment to adopt and operationalize e-government standards, ensure availability of Internet bandwidth, improve ICT Infrastructure, and ensure that best security measures are in place through the revised ICT policy.

KCMUCo understands that the vast choices of ICT for the holistic development of Education can be built only on a sound policy. The initiative of ICT Policy in KCMU College Education is inspired by the tremendous potential of ICT for enhancing outreach and improving the quality of education.

## 2.0 PURPOSE OF THE POLICY

This Policy provides the commitment of the KCMUCo to effectively manage the ICT functions, assets, and the obligations of the College community in protecting and guiding the ICT resources into good use. The policy ensures that the College ICT-related investment, operations, usage, and maintenance processes are well-directed while preventing ICT-related risks and discharging its core functions efficiently. In compliance with accepted best practices, KCMUCo shall provide the security and privacy of the data stored on, redirected through, or processed by its technology resources. Therefore, the purpose of this Policy is to: -

(i) Ensure KCMUCo users can access, observe best practices, identify, protect, and manage ICT resources available.

(ii) Provide cost-effective information communication technology facilities, services and automation.

(iii) Improve clients' satisfaction.

(iv) Identify priority areas for ICT development.

(v) Encourage innovations in technology development, use of technology and general workflow.

(vi) Help clients adapt to new circumstances and provide tools and models to respond rationally to challenges posed by ICT.

(vii) Promote information sharing, transparency and accountability and reduce bureaucracy in operations.

(viii) Use technology as a platform to meet KCMUCo strategic goals.

## 3.0 POLICY JUSTIFICATION

The College needs to achieve its Vision, Mission, and core functions and improve the quality and efficiency of its services using technologies. Thus, KCMUCo has over the years invested in ICT to facilitate its teaching, research, and public services, making the College operations increasingly dependent on ICT. Regulated ICT policy in the College is crucial for the efficiency of its operations. However, the expansion of ICT use comes with unexpected consequences of vulnerability to ICT related risks. To prevent the exposure of ICT-related risks, the College, therefore, must develop and operationalize a robust ICT Policy that takes oversight of ICT development, adoption, and usage within KCMUCo.

## 4.0 SCOPE OF THE POLICY

The Policy applies to all College staff, contractors, consultants, agents, students, collaborators, and any other person who uses or will be given access to email or files, software applications and the Internet during their employment or business dealings with the KCMU College, whether such use takes place on the KCMU College premises or elsewhere.

## 5.0 UNDERPINNING PRINCIPLES

The following fundamental principles shall guide this Policy: -

(i) Mainstreaming of ICT services in the College.

(ii) Seamless integration of ICT.

(iii) Inclusion, flexibility support to all stakeholders in the College and management system.

(iv) Adherence to best practices & policies.

(v) Economies of scale and customer value propositions.

## 6.0 DEFINITION OF TERMS.

In this policy, unless the context requires otherwise: -

**"Business Continuity Plan (BCP)"** means a document that outlines how a business will continue operating during an unplanned disruption of service. It is more comprehensive than a Disaster Recovery Plan (DRP). It contains contingencies for business processes, assets, human resources and business partners and every aspect of the business that might be affected.

**"Business Systems"** means any Information System that is critical to the ongoing operations of the KCMUCo and would cause losses to the KCMUCo if data integrity is compromised or if the system becomes unavailable.

**"Business System Owner"** means the nominated custodian responsible for the security of the data and application component of the ICT Asset and is also accountable for those aspects of the Information System. Business System Owners for each of the KCMUCo Information Systems shall be identified.
Note: Systems owners for each system shall be identified, and the list should be attached to the Policy.

**"College"** means Kilimanjaro Christian Medical University College.

**"College Clients"** means staff and students of the College as well as third party college clients.

**"Cost Centre Manager"** means the most senior officer or member of staff responsible for the management of a Faculty/Directorate/Institute or management or support service or administrative area or sub-section specifically identified for allocation of funding within the College's budget framework.

**"Data recovery plan (DRP)"** means a formal document created by the College that contains detailed instructions on how to respond to unplanned incidents such as natural disasters, power outages, cyber-attacks and any other disruptive events.

**"Information technology (IT)"** means all equipment, processes, procedures, and systems used to provide and support information systems (both computerized and manual) within an organization and those reaching out to customers and suppliers. Information and communications technology (ICT) was coined to reflect the seamless convergence of digital processing and telecommunications.

**"Information Communications Technology (ICT) Asset"** means all software, hardware and data used to manage the related KCMUCo information resources. This may include non-ICT resources, such as printed records.

**"ICT Steering Committee**" means one of the management organs formulated with a charter to help govern all issues related to ICT financially and technically accountable to the Management Human Resource and Students Affairs Committee (MHRSAC).

**"Information Classification"** means categorizing an ICT Asset to identify the security controls required to protect that asset.

**"Information System"** means an electronic system that manages information and data related to the ICT functions.

**"Proprietary System"** means an Information System developed by an individual(s) outside the College's IT development guidelines (e.g., LEO, OSIM).

**"Segregation of Duties"** means a separation of responsibilities in undertaking a task to minimize the likelihood of compromising security

**"Third-Party KCMUCo Clients"** means contractors, consultants, adjunct appointments and other individuals who are not College staff or students but require access to KCMUCo Information Systems.

"**User**" means a full-time or part-time staff, consultants, students, interns, retirees, suppliers, other College clients and stakeholders, and affiliated third parties who access

## 7.0 ABBREVIATIONS OF TERMS

| | |
|---|---|
| **BCP** | Business Continuity Plan |
| **CCTV** | Closed-Circuit Television |
| **DICT** | Directorate of Information Communication Technology |
| **DPA** | Deputy Provost Administration |
| **DPAA** | Deputy Provost Academic Affairs |
| **DRP** | Disaster Recovery Plan |
| **E-Learning** | Electronic Learning |
| **HEIs** | Higher Education Institutions. |
| **HRASC** | Human Resource and Students Affairs Committee |
| **ICT** | Information Communication Technology |
| **ICTSC** | Information Communication Technology Steering Committee |
| **ISP** | Internet Service Provider |
| **IT** | Information Technology |
| **KCMUCo** | Kilimanjaro Christian Medical University College |
| **KRA** | Key Result Area |
| **MDGs** | Millennium Development Goals |
| **NIDC** | National Internet Data Centre |
| **OSIM** | Online Student Information Management |
| **PC** | Personal Computer |
| **VPN** | Virtual Private Network |
| **VTC** | Video Tele-Conference |

## 8.0 POLICY STATEMENTS

The policy statements are presented in a number of approaches to policy issues followed by the operational procedures under each policy statement.

## 8.1 ICT GOVERNANCE

### 8.1.1 Administration

Effective ICT Governance practices impact how securities of information assets are achieved at the KCMUCo. This includes how risks are identified and managed; resources are allocated to implement several security measures, and KCMUCo management commitments to achieve the notable goal of operating in a secure, universal environment. Thus, the KCMUCo shall:

(i) Use ICT Steering Committee that is chaired by DPA.

(ii) Ensure ICT security practices are implemented on discharging its core functions while maintaining visions and mission highlighted in the strategic objective.

(iii) Ensure ICT security measures are addressed in all ICT related projects.

(iv) Allocate sufficient funds for ICT security and ensure capacity building on updated security issues to ICT staff.

(v) Ensure changes to the organization, business processes, information processing facilities and systems that affect ICT security shall be controlled.

(vi) Ensure the entire community comply and abide by security measures, which will be put in place.

(vii) Ensure a consistent and practical approach to managing risk and implementing a Business Continuity Plan (BCP).

(viii) Ensure sustainable management of the College ICT resources by creating appropriate policy guidelines and regulations, advisory and operational organs that will cater to the broad interests of all users.

### 8.1.2 ICT Assets Inventory and Protection

Inappropriate use of ICT assets may expose the KCMUCo to risks including but not limited to loss of these resources, malware attacks, compromising investment, compromise network systems and services and legal implications. Assets Management and Controlling involve asset acquisition, storage, usage, maintenance, and disposal activities. To ensure asset protection, KCMUCo shall: -

(i) Put into the record all ICT-related hardware/software into KCMUCo ICT inventory within five working days once purchased and received in the store.

(ii) The ICT Directorate, Accounts, and procurement shall keep the ICT inventory and;

  (a) update DPA, DPAA, Provost regarding the status of the College ICT assets as shall be deemed feasible.

  (b) Ensure that ICT assets are protected physically and logically for the asset's entire lifecycle.

  (c) Ensure user entitlement of ICT assets are well documented and bonded in their tenures, meaning that all terminated users shall retire to Head of ICT all ICT related resources given to them during tenure ship.

  (d) Ensure that ICT assets are disposed-off securely when no longer required.

  (e) Ensure that any lost ICT related resources/assets are reported immediately to DICT and accounted for by finance in the inventory and register.

  (f) Ensure continued job and external training to ICT staff on all aspects of ICT technologies, including security matters for effectiveness and efficiency on security measures implementation and custody of ICT assets.

  (g) Ensure regular training to KCMUCo staff and students on ICT matters.

### 8.1.3 ICT Budgeting

Proper accountability of ICT resources and compliance with financial regulations complement the streamlining of quality ICT services. Unplanned budgeting tends to disrupt the timely provisioning of ICT services. Therefore, the ICT Department shall: -

(i) Comply with Finance and Procurement policy, procedures, and regulations on proper utilization of resources and appropriate forms for requesting, purchasing, and retiring.

(ii) Ensure legal contracts, including a Non-Disclosure Agreement stipulating terms in which service will be rendered for all services from external vendors or consultants.

(iii) Assess, plan and implement ICT annual procurement plan across all KCMUCo Faculties, Departments, and Units for proper resource planning.

(iv) Allocate sufficient funds for adequate ICT security and ensure capacity building to ICT staff on updated security issues.

## 8.2 SECURITY AND ACCESS

In a community where there is a diversity of individuals, proper control is required to ensure safety measures are enhanced at all levels to protect the core ICT infrastructure and users. Thus, security and access at the ICT department shall be categorized as follows: -

### 8.2.1 Server Room Access

The server room hosts the KCMUCo ICT infrastructure; only authorized personnel can enter. Therefore,

(i) The server rooms shall have Biometric entry access and a CCTV camera to monitor all activities.

(ii) All individuals accessing the IT Server Rooms must sign in and out of the IT Server Room(s) Access Log, always including visitors, accompanying IT staff.

(iii) Tailgating other staff to enter the IT Server room(s) is not permitted, and non-compliance will lead to disciplinary action.

(iv) In case of emergence, The ICT Personnel in charge shall isolate access to the server room.

(v) Inventory register of all items inside should be placed in the visible area within and record in/out movements of equipment/items.

### 8.2.2 Computer Access

Misuse of computers because of mishandling of user access may result in legal consequences, loss of reputation, leak of sensitive information and more. Therefore, the College shall: -

(i) Enforce the use of passwords by users to access College computers and screen lock on all idle computers.

(ii) Install and update antivirus software on all servers and client computers.

(iii) Grant and revoke user access as per ICT security policy.

(iv) Authorize, document and monitor the use of remote support from external consultants.

### 8.2.3 Network Security

Safety is critical to any network environment; cyber security risks can catastrophically impact the College. Therefore, KCMUCo shall: -

(i) Ensure all servers are placed behind firewalls,

(ii) Ensure controlled access to and from the external environment by authorization.

(iii) Use an Intrusion Detection System (IDS) to fight against cyber-attacks proactively.

(iv) Establish support contact from the Tanzania Computer Emergency Response Team (TzCERT) in case of a major cyber-attack.

### 8.2.4 System Access

An uncontrolled ICT resource environment exposes all users to malicious attackers' data breaches and privacy violations. To mitigate this, the College shall: -

(i) Provide different access levels to limit or grant users' access according to their roles, responsibilities, and specialty.

(ii) have proper identification process for entry and exit of staff, visitors, students and third part to gain and terminate access from the systems including but not limited to:

(a) CCTV

(b) File system

(c) Students Management System.

(d) Accounts/Finance Systems.

(e) Human Resource Management System.

(iii) Fix security cameras in critical areas such as server rooms, computer venues/labs/library, and the administration floor.

### 8.2.5 Physical Environmental Protection

The physical environment includes but is not limited to the room, cabinets where ICT resources are hosted. The environment is subjected to a number of risk exposure from electricity problems, high environmental temperature, fire and loss of property due to physical theft.

To prevent any of the above, College shall:

(i) Use Uninterruptible Power Supplies (UPS) and other surge protectors against electricity

(ii) Protection from excessively high temperatures and fire by temperature control and fire alarm.

(iii) Install and monitor Security cameras within the premises with critical ICT infrastructure.

## 8.3 MULTIMEDIA (WEBSITE, DISPLAY SCREENS, SOCIAL MEDIA)

It is important to continue updating the community on the College's ongoing activities and their relationship with the College vision and mission through multimedia platforms, which can reach out to the local and international communities. Therefore, the College shall monitor and control the use of the following platforms: -

### 8.3.1 Website

The College shall ensure availability, reliability, visibility, and moderate the content presented on the website to reflect its vision and mission. For this reason, KCMUCo shall:

(i) Pay domain subscription of <https://kcmuco.ac.tz> to the registrar of companies.

(ii) Pay hosting service of the website and items related to the website such as security certificates and themes.

(iii) Update and continue to moderate the website's content to reflect the College core activities.

### 8.3.2 Social Media.

There is an exponential growth of social which send information to the community, and if not moderated, it may lead to the conveyance of wrong information. The College shall moderate the posting of social media content and ensure that: -

(i) The information posted is from an authentic and authorized source

(ii) The information portrays the mission, vision, values, and core functions of the College.

### 8.3.3 Display Monitors

Screen monitors located at various places in the College buildings inform the public about current issues or news of common interest. To ensure relevance, appropriateness and conformity to vision mission and values, KCMUCo shall: -

(i) Moderate all contents through an approval process.

(ii) The Public Relation Office shall finally vet the information content before it is posted.

## 8.4 CONNECTIVITY (NETWORK & INTERNET, EMAIL)

Enabler environment for college core business activities is supported through ICT reliable connectivity, to safeguard and ensure reliable, adequate and sustainable service is the key.

### 8.4.1 Network integrity

The College ICT infrastructure is built by fibre-optic connections to buildings where students and staff are housed. Protection of the ICT infrastructure is vital for smooth daily operations. To ensure the integrity of the infrastructure of the College: -

(i) Prohibits removing, cutting, or causing any form of damage to the fiber optic cables connections to different buildings.

(ii) For any new connections to a new office or building that require fiber termination, the Head of ICT and the officer in charge of the Network shall be involved in the process to safeguard the interest of the College.

### 8.4.2 Use of Email

All official communications via emails within and outside the College shall require KCMUCo official email address. This measure may serve as a defence against an allegation that the user has intentionally violated this Policy by inadvertently disclosing the College information. Regarding the use of personal use of College emails and the Internet: -

(i) Users can make reasonable personal use of College email and Internet facilities outside regular working hours. However, such use must be consistent with this Policy.

(ii) The College reserves the right to discontinue the entitlement for any employee if it is of the views that the use of email and Internet facilities is excessive or inappropriate.

(iii) Any personal use of the College email can be considered private and subject to monitoring through this Policy.

(iv) Users must make arrangements to save electronic or paper copies of their emails. The College does not accept any responsibility for the safe storage of personal emails, which may be deleted at any time.

### 8.4.3 Internet

Improper or inappropriate Internet use can harm the KCMUCo operation, lead to serious legal consequences or disrepute.

(a) To ensure a safer environment, KCMUCo shall: -

(i) Ensure cost recovery strategy for Internet and other ICT services and facilities is incorporated in the University Strategic Plan for sustainability purposes.

(ii) Ensure all projects within the KCMUCo community contribute Internet and ICT service fees to create sustainable, robust services.

(iii) Filter contents as it deems fit according to the law of the country and institutional views provided under vision and mission.

(iv) Ensure provision of better, quality service of the Internet from reliable and affordable ISP.

(b) KCMUCo shall not allow the following uses of the Internet: -

(i) To access, review, upload, download, store, print, post, or distribute pornographic, obscene, or sexually explicit material.

(ii) For political activities and campaigning.

(iii) To transmit obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually explicit language.

(iv) To access, review, upload, download, store, print, post, or distribute materials that use language or images inappropriate to the work environment or may disrupt the work atmosphere.

(v) To post information or materials that could cause damage, danger, or disruption of the system and harmony.

(vi) To access, review, upload, download, store, print, post, or distribute materials that use language or images that advocate violence or discrimination toward other people or that may constitute harassment or discrimination.

(vii) To knowingly or recklessly post false or defamatory information about a person or organization, harass another person, or engage in personal attacks, including prejudicial or discriminatory attacks.

(viii) To engage in any illegal act or violate act as applicable in the country's laws.

(ix) To gain unauthorized access to information resources or to access another person's materials, information, or files without that person's implied or direct permission.

(x) To post private information about another person or to post personal contact information about themselves or other persons including, but not limited to, addresses, telephone numbers, work addresses, identification numbers, account numbers, access codes or passwords, and will not repost a message that was sent to the user privately without permission of the person who sent the message.

(xi) To attempt to gain unauthorized access to the system or any other system through the KCMUCo system, attempt to log in through another person's account, or use computer accounts, access codes or network identification other than those assigned to the user.

(xii) To violate copyright laws, or usage licensing agreements, or otherwise to use another person's property without the person's prior approval or proper citation, including the downloading or exchanging of pirated software or copying software to or from any KCMUCo computers.

(xiii) Unauthorized commercial or financial use or gain that is not part of the official business of the KCMUCo.

(xiv) To offer or provide goods or services, products, advertisements, other than for work purposes.

(c) If a user unintentionally accesses inappropriate materials or an unacceptable Internet site, the user shall immediately delete or report to the appropriate authority for further action.

## 8.5 TRAINING, SUPPORT AND MAINTENANCE

As part of a plan to ensure KCMUCo users have sufficient knowledge and skills to maximize utilization of existing ICT resources, ICT support and scheduled maintenance are vital.

(a) The College ICT department shall therefore provide the following support: -

(i) Office Support – For administrative, teaching, and research employees assigned with ICT working tools such as desktop or laptop computers.

(ii) Venues (offices, classrooms and conference rooms, laboratories) - includes the students as the primary users of the physical and virtual spaces for meetings and teaching platforms.

(iii) Train users in the college on best practice usage of ICT resources, useful resources and security matters related to their roles.

(b) The ICT management shall: -

(i) Promote the use of ICT in all offices, and depending on availability and cost containment, resources sharing will be promoted. This applies to lecturers, researchers, administrators, managers, secretarial, and clerical staff.

(ii) Enhance and streamline financial management processes and reporting by implementing an integrated financial information management system.

(iii) Support and enhance the e-learning initiatives to diversify teaching and learning practices to a broader community of potential scholars within and outside the country.

(iv) Ensure all administrative and academic buildings are provided with access to facilities as well as training.

(v) Enhance and streamline Education related administrative, managerial processes and improve academic reporting by implementing an Integrated Academic Records Information Management System that will reduce costs related to paperwork and stationery.

(vi) Actively involve the Head of ICT in the review, approval of space related to ICT, including but not limited to software, hardware and renovations of ICT equipment buildings that require prior safely removal of equipment.

(vii) Plan scheduled maintenance of ICT equipment and other facilities/resources.

(viii) Promote the use of an online service desk to identify recurring challenges and efficiency in resolving matters raised.

## 8.6 DATA PROTECTION

All data collected through research and field activities that involve a member of the College is a property of KCMUCo unless explicitly specified in the MoU with the Funding Agency. Therefore, this policy is hereby declaring that: -

(i) Access and release of data require authorized privileges and a need-to-know basis according to the information hierarchy.

(ii) Sensitive information shall not be stored on external storage systems (e.g., Dropbox, un-encrypted USB memory sticks, and external hard drives) or similar devices.

(iii) Even with protective measures in place, data saved on such systems is vulnerable. In case external storage is an operational necessity, proper sensitivity classification must be specified, approval obtained from the Head of the department/unit, and the repository should be utilized for data transfer only – with immediate deletion following completion of the transfer.

(iv) Cloud storage shall only be used for KCMUCo data if an official agreement or contract exists between KCMUCo and the third-party service (e.g., NIDC). The problem with individual users engaging the third parties to house their data is that there are no contractual controls on who has access to the data or any knowledge of the "due diligence" used by the third-party service in protecting the data. Thus, users could be inadvertently revealing sensitive data to unauthorized persons.

(v) The Internet should not be used for illegal purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g., spreading computer viruses).

(vi) Individuals must limit their personal use of the Internet. The College allows limited personal communication with family and friends, independent learning, and public service. Still, it prohibits, among other things, its use for unsolicited mass mailings (Sending spam), access for non-users to College resources or network facilities, uploading and downloading of copyrighted files without legal rights, access to pornographic sites, peer to peer sites, illegal drugs, weapons, gaming, competitive commercial activity, and the dissemination of information to cause a public disturbance.

(vii) Users remotely accessing KCMUCo' corporate Network shall ensure that their remote access connection is given the same consideration as the user's on-site connection (e.g., an updated antivirus system is running). Users shall abide by and be aware of all policies and laws applicable to computer system use.

(viii) All staff' report IT security violations to the ICT Officer or designee and cooperate fully with all investigations regarding the abuse or misuse of KCMUCo IT resources.

(ix) In an event that a security incident arose, in whole or in part, due to user non-compliance with applicable regulations, rules, policies, or procedures may result in forfeiture of the privilege to use technology resources or, depending on the severity of the incident, administrative, disciplinary, or other legal action may be taken.

## 8.7 DATA BACKUP

Backup procedures, ensuring that both data and software are regularly and securely backed up, are essential to protect against loss of that data and software. Backing up of the user files is the responsibility of the user and user units. However, ICT staff shall undertake all possible measures to ensure that backing up user files is accurately undertaken and proper operations of the baking up system are guaranteed through**:**

(i) ICT team members shall ensure a daily incremental and a weekly backup to the backup servers to ensure the system's continuity in the event of failure.

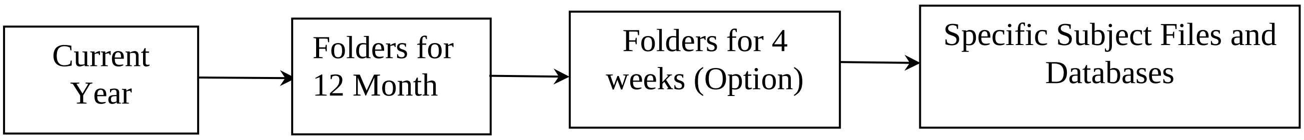
(ii) In the absence of assigned ICT staff, another ICT personnel should take responsibility for backup.

(iii) In case of a disaster strike, BCP shall be invoked.

(iv) Users are required to backup data periodically (daily/weekly/monthly) basis, depending on how data are generated, currently, all data are synchronized to

KCMUCo domain storage.

(v) Proper tree structure for backup document needs to adhere as follows: -


Current Year
Folders for 12 Month
Folders for 4 weeks (Option)
Specific Subject Files and Databases

## 9.0 POLICY IMPLEMENTATION, MONITORING AND EVALUATION.

### (i) Policy Implementation

The responsibility for monitoring the implementation of this Policy is vested in the College Management. However, the ICTSC shall have the oversight mandate for all matters concerning and affecting ICT services on behalf of the College Governing Board. The responsibility for implementing specific operational aspects of this Policy is integral to the Provost, Deputy Provosts, Deans, Directors, Heads of Departments through the Head of ICT.

### (ii) Policy Monitoring and Evaluation

This policy will be monitored and evaluated through appraising the increased performance and elimination of ICT risks, assessment of the level and quality of staff engagement and understanding ICT functions, and degree of compliance with this policy, documenting the progress of the whole policy cycle from its development, endorsement, and timely review, and ensuring the policy is put into practice through dissemination, implementation planning, and planning for its following review.

## 10.0 OWNER OF THE POLICY

The owner of this Policy shall be the KCMUCo College Governing Board.

## 11.0 CUSTODIAN OF THE POLICY

This Policy shall be under the Custody of the Head, Department of ICT, through the following address: -

P.O. Box 2240, Moshi<br>
Kilimanjaro.<br>
Telephone: +255272753616 Ext#62

## 12.0 RELATED LEGISLATIONS

(i) KCMUCo Staff Regulations and Condition of Services (2015).

(ii) KCMUCo Intellectual Property Policy (2015)

(iii) KCMUCo Co-operate Strategic Plan (2020/21 - 2025/26).

(iv) KCMUCo Charter and Rules (2010).

(v) Tanzania's National ICT Policy (2016)

(vi) The Education and Training Policy (2014)

(vii) The Universities Act (2005)

(viii) Tanzania Cybercrimes Act (2015)

## 13.0 REVIEW OF THE POLICY

The Policy shall be reviewed after every three years.

## 14.0 APPROVAL

Approved by the College Governing Board during its 45th Meeting Held on 25th February 2022**.**