Kilimanjaro Christian Medical University College
(A Constituent College of Tumaini University Makumira)

DATA SECURITY POLICY

1:-Introduction

The purpose of this policy is to outline essential roles and responsibilities within the KCMU College community for creating and maintaining an environment that safeguards data from threats to personal, professional and institutional interests and to establish a comprehensive data security program. This policy is also designed to establish processes for ensuring the security and confidentiality of confidential information and to establish administrative, technical, and physical safeguards to protect against unauthorized access or use of the confidential information.

2:- Scope

This policy applies to all KCMU College faculty and staff, whether full- or part-time, paid or unpaid, temporary or permanent, as well as to all other members of the KCMU Collage community. This policy applies to all information collected, stored or used by or on behalf of any operational unit, department and person within the community in connection with KCMU Collage operations. In the event that any particular information at KCMU College is governed by more specific requirements under other Collage policies or procedures (such as the policy concerning students' education records) the more specific requirements shall take precedence over this policy.

3:-Definitions.

In this policy, unless the context requires otherwise:

"Information Resource" An Information Resource is a discrete body of information created, collected and stored in connection with the operation and management of the KCMU Collage and used by members of the Collage having authorized access as a primary source. Information Resources include electronic databases as well as physical files. Information derived from an Information Resource by authorized users is not an Information Resource, although such information shall be subject to this policy.

"Sponsors" Sponsors are those members of the KCMU Collage community that have primary responsibility for maintaining any particular information resource.

"Data Security Officers" Data Security Officers are those members of the KCMU-Collage, designated by the Provost, who provide administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.

"Users" Users include virtually all members of the KCMU- College community to the extent they have authorized access to Collage Information Resources, and may include students, staff, contractors, consultants, temporary employees and volunteers.

"Data Security Committee" The Data Security Committee shall be chaired by the Provost and shall include the following or their representatives: the Deputy Provost Administration, the College Bursar, the IT manager for Information Technology, Human Resources Office, and the Legal Officer.

"Computer System Security Requirements" Computer System Security Requirements shall mean a written set of technical standards and related procedures and protocols designed to protect against risks to the security and integrity of data that is processed, stored, transmitted, or disposed of through the use of KCMU-Collage information systems, and shall include computer system security requirements that meet or exceed the requirements of regulations promulgated under the relevant laws. The Computer System Security Requirements establish minimum standards and may not reflect all the technical standards and protocols in effect at the KCMU-Collage at any given time.

"Data Security Directives" Data Security Directives shall be issued from time to time by the Data Security Committee to provide clarification of this policy, or to supplement this policy through more detailed procedures or specifications, or through action plans or timetables to aid in the implementation of specific security measures. All

Data Security Directives issued by the Committee shall be deemed incorporated herein.

"Specific Security Procedures" Specific Security Procedures are procedures promulgated by a KCMU Collage Provost or Dean to address particular security needs of specific Information Resources sponsored within their area of responsibility, not otherwise addressed by this policy, or any Data Security Directives.

"Data Security Working Group" The Data Security Working Group shall be chaired by the ICT in-charge and shall consist of those Data Security Officers as may be assigned to the group from time to time by the Data Security Committee.

"Security Breach" A Security Breach is any event that causes or is likely to cause Confidential Information to be accessed or used by an unauthorized person.

4:-Data classification.

1) All information covered by this policy is to be classified among one of three categories, according to the level of security required. In descending order of sensitivity, these categories are "*Confidential*," "*Internal Use only*," and "*Public*."
   a) *Confidential* information includes sensitive personal and institutional information, and must be given the highest level of protection against unauthorized access, modification or destruction. Unauthorized access to personal confidential information may result in a significant invasion of privacy, or may expose members of the KCMU-Collage community to significant financial risk. Unauthorized access or modification to institutional confidential information may result in direct, materially negative impacts on the finances, operations, or reputation of KCMU College. Examples of personal confidential information include information protected under privacy laws, information concerning the pay and benefits of KCMU Collage employees, personal identification information or medical/health information pertaining to members of the Collage community, and data collected in the course of research on human subjects. Institutional Confidential information may also include KCMU Collage financial and planning information, legally privileged information, invention disclosures and other information concerning pending patent applications.
   b) *Internal Use Only* includes information that is less sensitive than confidential information, but that, if exposed to unauthorized parties, may have an indirect or possible adverse impact on personal interests, or on the finances, operations, or reputation of KCMU College. Examples of this type of data from an institutional perspective include internal memos meant for limited circulation, or draft documents subject to internal comment prior to public release.
   c) *Public* information is information that is generally available to the public, or that, if it were to become available to the public, would have no material adverse effect on individual members of the Collage community or upon the finances, operations, or reputation of KCMU College.
2) All Information Resources, whether physical documents, electronic databases, or other collections of information, are to be assigned to a security classification level according to the most sensitive content contained therein.
3) Where practicable, all data is to be *explicitly classified.*
4) In the event information is not explicitly classified, it is to be treated as follows: Any data which includes any personal information concerning a member of the KCMU Collage community (including any health information, financial information, academic evaluations, or other personal identification information) shall be treated as Confidential. Other information is to be treated as Internal Use Only, unless such information appears in form accessible to the public (i.e., on a public website or a widely distributed publication) or is created for a public purpose.
5) It is hereby established Data Security Committee. The Data Security Committee may from time to time provide clarifications relating to the security classifications, and may, through issuance of Data Security Directives establish more detailed requirements concerning the classification of Information Resources or specific data.

5:- Role of the data security working group.

1) The KCMU Collage has established the Data Security Working Group to aid in the development of procedures and guidelines concerning the collection, storage, and use of data by the Collage community, and to assist the Data Security Committee in the implementation of this policy.

2) In consultation with the Office of the Corporate Counsel, Internal Auditor, the Data Security Working Group shall:
   a. Ensure compliance with the local legislation concerning privacy and data security;
   b. Stay abreast of evolving best practices in data security and privacy in College, and assess whether any changes should be made to the Computer System Security Requirements.
   c. Establish data privacy and security training and awareness programs for the KCMU Collage community and periodically assess whether these programs are effective.
   d. Periodically reassess this policy to determine if amendments are indicated or if Data Security Directives should be proposed to the Data Security Committee.
   e. Discuss any material violations of this policy and Security Breaches, the KCMU Collage's actions in response, and recommend any further actions or changes in practice or policy to the Data Security Committee.

6:- Role of the data security Committee.

1) The KCMU Collage has established the Data Security Committee to formulate Collage-wide procedures and guidelines concerning the collection, storage, use and safekeeping of data, to update as necessary this policy, and to direct the responsive actions in the event of any material violation of this policy or any Security Breach.
2) The Data Security Committee shall from time to time liaise with representatives of the Data Security Working Group to review the implementation of this policy and compliance with the Computer System Security Requirements and Data Security Directives.
3) The Data Security Committee shall periodically review identifiable risks to the security, confidentiality, and integrity of data, and shall review this policy and the scope of Computer System Security Requirements at least annually to assess its effectiveness and determine whether any changes are warranted.
4) The Data Security Committee is authorized to:
   a. Issue Data Security Directives.
   b. Promulgate amendments to this policy, including the Computer System Security Requirements.
   c. Take actions to ensure compliance with this policy, which may include, without limitation, the commissioning of internal audits and investigations.
   d. Take actions in response to violations of this policy or any Security Breach.

7:- ROLE OF THE director of Computer Policy and Security.

a) The ICT In-Charge shall, with input from the Data Security Working Group, identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of KCMU Collage data. This identification and risk assessment shall include adopting means for detecting security system failures and monitoring the effectiveness of the Computer System Security Requirements.

b) The Director shall, in conjunction with the Data Security Working Group, oversee the implementation of the Computer System Security Requirements and recommend changes to address risks, failures, or changes to business practices to the Data Security Committee.

c) The Director shall work with other KCMU Collage administrators to investigate any violation of this policy and any incident in which the security or integrity of KCMU Collage data may have been compromised, including taking the steps set forth below in response to a security breach.

d) The Director shall work with other KCMU Collage administrators to develop and review training materials to be used for employee training under this policy.

8:-Security responsibilities.

1. It is the policy of the KCMU Collage that all confidential and other sensitive information be safeguarded from unauthorized access, use, modification or destruction. All members of the KCMU Collage community share in the responsibility for protecting the confidentiality and security of data. This section of the policy assigns specific duties to each of the roles of Provost and Deans, Sponsors, Data Security Officers, Users, and the Human Resources officer. However, it is likely that an individual will have responsibilities reflecting multiple roles with respect to certain information.

2. *Provost and Deans*. KCMU Collage Provost and Deans are responsible for promoting institutional awareness of this policy and for ensuring overall compliance with it by their staff. In particular, Provost and Deans are

responsible for:

a. Ensuring that all staff have the training and support necessary to protect data in accordance with this policy, all Data Security Directives, and any Specific Security Procedures applicable to such data.
b. Designating and managing the efforts of one or more Sponsors and Data Security Officers for all Information Resources maintained in their area of responsibility.
c. Approving access authorization of all Users of Information Resources maintained in their area of responsibility having a data classification of Confidential.
d. Promulgating Specific Security Procedures.
e. Ensuring that Confidential or Internal Use Only data within their area of responsibility are not provided or accessible to, or created or maintained by KCMU Collage vendors or other third-parties without (i) assistance from the ICT In- Charge and the Director of Internal Audit, verifying that the third party has the capability of adequately protecting such data; (ii) review and approval of the relevant contract and the underlying terms and specifications by the ICT Director and Security and the Office of the Corporate Counsel; and (iii) unless approved otherwise by the Office of the Corporate Counsel, verifying that the third party has executed the KCMU Collage's standard form of Privacy and Security Addendum.

3. *Sponsors*. A Sponsor has primary responsibility for overseeing the collection, storage, use and security of a particular Information Resource. In cases where a Sponsor is not identified for any Information Resource, the Provost or Dean shall be deemed the Sponsor. A Sponsor is responsible for the following specific tasks associated with the security of the information:

a. Ensuring that the Information Resource is assigned a security classification and that such data is marked where appropriate;
b. Identifying authorized Users of the Information Resource, whether by individual identification of by job title, and obtaining approval for such access from the Provost or Dean;
c. Proposing to their Dean Specific Security Procedures for the handling of data under their sponsorship, consistent with this policy and other applicable KCMU Collage policies and procedures.

4 *Data Security Officers*. A Data Security Officer works with Information Technology and other appropriate KCMU Collage functions in consultation with a Sponsor, to support the implementation and monitoring of security measures associated with the management of Information Resources. Data Security Officers shall be responsible for:

a. Ensuring adequate security technology is applied to Information Resources in keeping with their classification and to comply with this policy and all Data Security Directives, and Specific Security Procedures;
b. Monitoring for indicators of loss of integrity;
c. Promptly reporting to the ICT In-Charge any incidents of data being accessed or compromised by unauthorized Users, and any violations of this policy, Data Security Directives or Specific Security Procedures;
d. Monitoring for risks to data security and reporting any known or reasonably foreseeable risks to the Data Security Working Group.

5. *Users.* Users are responsible for complying with all security-related procedures pertaining to any Information Resource to which they have authorized access or any information derived there from that they possess. Specifically, a *User* is responsible for:

a. Becoming familiar with and complying with all relevant KCMU Collage policies, including, without limitation, this policy, and all Data Security Directives contemplated hereby, the policy on Professional conduct and Business ethics and other policies related to data protection, technology use and privacy rights.
b. Providing appropriate physical security for information technology equipment, storage media, and physical data. Such equipment and files shall not be left unattended without being locked or otherwise protected such that unauthorized Users cannot obtain physical access to the data or the device(s) storing the data.

c. Ensuring that Confidential or Internal Use Only information is not distributed or accessible to unauthorized persons. Users must not share their authorization passwords under any circumstances. Users must avail themselves of any security measures, such as encryption technology, security updates or patches. Users must log off from all applications, computers and networks, and physically secure printed material, when not in use.

d. To the extent possible, making sure that any KCMU College data accessed by the User is stored only on secure servers maintained by the Collage and not on local machines, unsecure servers, or portable devices.

e. KCMU College Confidential or Internal Use Only data, when removed from the campus or when accessed from off-campus, is subject to the same rules as would apply where the data on campus. Sponsors and Users will comply with this Policy and all relevant Data Security Directives irrespective of where the KCMU College data might be located, including, for example, on home devices, mobile devices, on the Internet, or other third-party service providers.

f. When access to information is no longer required by a User, disposing of it in a manner to insure against unauthorized interception of any Confidential or Internal Use Only information. Generally, paper-based duplicate copies of confidential documents should be properly shredded, and electronic data taken from confidential databases should be destroyed.

g. Immediately notifying his or her responsible officer any incident that may cause a security breach or violation of this policy.

6:-*Deputy Provost Administration (DPA).* The Deputy Provost Administration shall be responsible for:

a. Working with the Data Security Working Group to educate incoming employees (including temporary and contract employees) regarding their obligations under this policy and to provide on-going employee training regarding data security;

b. Ensuring that terminated employees no longer have access to KCMU Collage systems that permit access to Confidential or Internal Use Only information; and

c. Carrying out any disciplinary measures against an employee presumed to have violated this policy as shall be deemed necessary and equitable.

7:-Security Breach Response.

As provided above, Users and Data Security Officers must report any known Security Breach or any incident that is likely to cause a Security Breach. These incidents include thefts of computer devises, viruses, worms, or computer “attacks” that may lead to unauthorized access to confidential information.

Immediately upon becoming aware of a likely Security Breach, the ICT In- Charge shall notify the Office of the Corporate Counsel and the Internal Auditor. The Corporate Counsel shall determine what, if any, actions the Collage is required to take to comply with applicable law.

The Corporate Counsel shall work with other administrators as appropriate to ensure that any notifications and other legally required responses are made in a timely manner. If the event involves a criminal matter, the Police shall be notified and shall coordinate its response with the Office of the Corporate Counsel.

8:- Enforcement sanctions

The KCMU Collage reserves the right to monitor network traffic, perform random audits, and to take other steps to insure the integrity of its information and compliance with this policy. Violations of this policy may lead to appropriate disciplinary action, which may include temporary or permanent restrictions on access to certain information or networks. Willful or repeated violations of this policy may result into termination.

9:-KCMU College Computer system Security requirements.

The KCMU Collage maintains a computer security system that provides at a minimum to the extent technically feasible:

1. Secure user authentication protocols including:

a) Control of user IDs and other identifiers;

b) A reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;

c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;

d) Restricting access to active Users and active User accounts only; and

e) Blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system.

2. Secure access control measures that:

   a) restrict access to records and files containing Confidential information to those who need such information to perform their job duties; and

   b) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls.

3. Encryption of all transmitted records and files containing KCMU College that will travel across public networks, and encryption of all data containing KCMU College data to be transmitted wirelessly.
4. Reasonable monitoring of systems, for unauthorized use of or access to KCMU Collage data source.
5. Encryption of all KCMU Collage data stored on laptops or other portable devices.
6. For files containing KCMU Collage data on a system that is connected to the Internet, reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the KCMU Collage data.
7. Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.
8. Education and training of employees on the proper use of the computer security system and the importance of data security.

10: Policy approval

This policy was approved by the College Governing Board in its meeting held on………Day of ……………………………………………………………………2017