The Mico University College

1A Marescaux Road, Kingston 5

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) POLICY

Office of Accountability:	VP, Administration
Office of Administrative Responsibility:	ICT Department
Document Number	Mico.Adm. Po.13.006
Effective Date of Policy	September, 2013
Date of any Policy Revision	
Policy Prepared by:	Junior Martin, Stephen Megoo and Selvin Bailey
Date Policy Created:	August, 2013
Date Accepted by Executive Management Com. :	
Authorized by:	
	President and Chairman of Executive Management Com.
	VP Administration
Date Approved by the Board of Directors:	
Authorized by:	
	Pro-Chancellor and Chairman of the Board
	Chairman of the Sub-Committee
Version	01

Draft

Table of Contents

A.   Information Communication and Technology

1.0   Introduction

Information and Communication Technologies play a vital role in supporting all day-to-day academic and non-academic functions of The Mico University College. With the expansion of the technology services and the population of users, the need arises for the development and implementation of policies to govern the management of ICT. The institution therefore seeks to establish a system of management of all technology systems and users in an efficient and effective way to improve and maximize the outputs The Mico community. The ICT policy therefore defines a set of principles relating to the application and use of ICT to inform strategies and methodologies adopted for learning, teaching, research, administration and management. The policy seeks to establish standards and competencies required by all users who interact with the equipment and technology services provided by The Mico University College.

2.0   Scope

This policy applies to persons within the University College Community who access / develop and/or use the institution's information and ICT resources which are owned, managed, supported or operated by, or on behalf of, the University College, wherever these resources are located. This shall include all University staff and students; any other organizations accessing services over University College's ICT resources; and suppliers of outsourced ICT services. This policy is binding on all users of the University College's ICT resources.

3.0   Goals and Objectives

This policy seeks to guide developers and users of information and ICT resources on appropriate standards to be adopted at the University College. Its objectives include to:

i) provide guidance in developing a pervasive, reliable and secure technology infrastructure conforming to recognized International standards supporting all services in line with the priorities of the University College;

ii) provide a framework for development and management of ICT network services that shall ensure the availability, enhanced performance and security of running the ICT infrastructure;

iii) establish and implement security requirements across the University's ICT infrastructure;

iv) guide the management of information/data within the University by ensuring compliance with applicable statutes, regulations, and mandates for the management of information resources; and thereby establishing prudent practices for Internet and the University Intranet use;

v) manage the use of ICT services and resources to guide the process of enhancing user utilization of ICT resources through training**;** outline the rules and guidelines that ensure users' PCs and other hardware are in serviceable order; specify best practices and approaches for preventing failure.

4.0   Policy Statements

The Mico University College shall -

i)   Respect all computer software copyrights and will adhere to the terms of all software licenses to which the institution is a party. The University College shall take all steps necessary to prohibit users from duplicating any licensed software or related documentation for use either on its premises or elsewhere, unless expressly authorized to do so by the licensor.

ii)   Commit to ensuring that its ICT systems support direct, secure, convenient, and easy access to information, as appropriate.

iii)   Protect, adequately, its existing ICT investments while ensuring that the it maintains the opportunity to adopt new technologies

iv)   Ensure that technology platform decisions will be based on application and information needs.

5.0   Definitions

ICT Resources   refers to all of the University College's Information and Communication Technology Resources, facilities and infra-structure, including, but not limited to: personal computers including internet access – Mico-mail, the intranet, the internet; telephony including - telephones, mobile phones, voice mail, SMS, facsimile machines, email; regular mail; other equipment including - printers, scanners, access labs or other facilities that the University College owns; leases or uses under Licence or by agreement; system software and the physical network.

User(s)   refers to all employees, including temporary employees, any person enrolled in an award course of study at the University College and any person registered to attend short courses, seminars or workshops in any unit of the University College.

Application Software   Includes but not limited to – Mico-mail, Student Management Systems (SMS), Accounting software (ACCPAC), Microsoft suite, Educational Software (SPSS etc.), Human Resource Software (Orange HR)

Data   Refers to all of the University Colleges, which includes – student data, i.e. application, acceptance, progress reports, transcripts etc.; staff data, application, contracts, leave, etc.; and Programme / Course data.

6.0   Roles and Responsibilities

The President

The President shall have the responsibility for considering the recommendations of the ICT Steering Committee on matters of information, communication and technology and for authorising the necessary resources for implementation as necessary.

The Chief Information Officer (CIO)

The Chief Information Officer shall –

....

HOD ICT

The Head of the ICT Department shall –

....

Senior Systems Administrator

Senior Systems Administrators shall –

....

<u>Systems Administrators</u>

Systems Administrators shall –

....

<u>Specialists</u>

Specialists shall –

....

<u>Staff Members</u>

All staff members shall

i)   Be aware of and comply with the policies, procedures and regulations regarding ICT

ii)   Ensure that all information systems, telecommunication networks and confidential information belonging to or entrusted to the University College shall be protected unauthorised or accidental disclosure, modification, destruction or use.

iii)   Report any incident of actual or potential misuse of the institution's assets (hardware or software) to the ICT Department.

The proposed organizational Structure is at <u>Addendum I.</u>

<u>Students</u>

All students at the Mico University, whether enrolled full time or part time, whether on campus or off campus shall -.........

7.0 ICT Steering Committee

7.1 Statement

The purpose of the ICT Steering Committee is to oversee and manage the implementation of the institution's ICT systems.

7.2 Organisation of the ICT Steering Committee

i) A ICT Steering Committee shall be established at the institution, with the VP Administration having the overall responsibility for the Committee.

ii) The composition of the Committee shall not exceed 12 persons, with the membership including the HOD of the ICT Department, who shall be the Chairman of the Committee, the Chief Information Officer, the Librarian, the Registrar, the Bursar, the HR Director, the Director of Records Management, the Deans who shall be rotated every year, the Plant Manager, the Senior System Administrator and a representative of ITER/Graduate School.

iii) The Committee shall hold regular meetings, the frequency to be determined by the Committee. The Committee shall maintain minutes of its meeting, as well as, records of correspondence and activities.

iv) The Committee shall establish a system by which it obtains ICT-related suggestions and reports directly from staff and students.

v) The Committee shall ascribe to itself any other duties it sees fit.

7.3 Committee Procedures

i) Schedule
The Committee shall meet regularly, the frequency to be determined by the Committee. The Committee shall maintain minutes of its meeting, as well as, records of correspondence and activities.

ii) Agenda
Any member may place items on the agenda for discussion at a Committee meeting. Relevant papers shall be circulated in advance to allow members adequate time for preparation.

iii) Minutes
Minutes shall be sent to each Committee member, and may be posted for all employees, where it is deemed necessary to advise personnel of decisions taken. Minutes may be retained for three years.

iv) Conduct of Meetings
Meetings shall be conducted by the Chairperson. In the absence of the Chairperson, the members in attendance will select a member as Acting Chair, who will conduct the meeting.

v) <u>Quorum</u>
At regular meetings, a quorum shall be one half of the appointed members. In the absence of a quorum, a Committee meeting may continue except that no formal votes shall be conducted.

vi) <u>Sub-Committees</u>
Sub Committees may be formed to carry out tasks on behalf of the Committee as required.

vii) <u>Reporting</u>
The Committee shall provide bi-annual reports to the Academic Board on its activities, its observations and evaluations and its recommendations.

8.0   Guidelines

8.1 Infrastructure

The University College shall

i) Institute processes and guidelines to ensure that only authorized users have access.

ii) Formulate a development plan to ensure the adequacy of the University College's ICT infrastructure to achieve its strategic objectives and take into account, usage, demand patters and technological change.

iii) Ensue that its network provisions shall be in accordance acceptable standards.

iv) Ensure that there are no external network connections without the prior written authorizations.

v) Develop protocols for the location, security and operation of the servers and its connectivity.

8.2 Security

The University College shall

i) Ensure the physical security for its computers and other ICT equipment in areas which can be locked and shall institute a key management policy to ensure that only authorized users have access.

ii) Develop and implement standard procedures for control over diskettes, tapes and other media:

iii) Ensure that Password Security is administered user IDs and passwords are applicable, to ensure that:

- New users obtain IDs and passwords as needed

- Users who are no longer members of the University community have their IDs and passwords revoked immediately.

- Passwords are kept confidential and users are held accountable for their password.

iv) Conduct training for all employees in the use and observance of the system, and ensure training for new employees at orientation.

8.3 Application Software

i) All software to be acquired by the University College must be justified by the Users and must have received the requisite approvals

ii) All software shall be installed by the ICT Department or under their supervision. Once installed, the original information shall be kept in a storage maintained by ICT. User manuals, if provided, shall either reside with the user or reside with the ICT as necessary.

iii) The personal computers are owned by the University College and only software purchased through the University College shall be used. Users are not permitted to bring software external to the institution for loading onto the institution's computers; nor shall be the software purchased by the University College be taken away to be used in a personal capacity.

8.4 Internet Resources

The University College shall –

i) Ensure that all software used to access the Internet shall be part of the University College standard software suite.

ii) Make the necessary provisions for the software to incorporate the latest security updates provided by the vendors and that all files downloaded from the Internet shall be scanned for viruses using the University College's virus detection system.

8.5 Data Retention, Archiving and Restoration

Electronic messages sent or received on behalf of the University and which provide evidence of an activity, transaction or event must be regarded as official University records. Such records must be retained in an official repository. Their disposal must be in accordance with approved retention and disposition schedules. Records relative to matters subject to on-going or threatened legal action or any investigation must be retained and should not be disposed of, even if the retention period has been met on the records retention schedule, except as advised by the University Legal Counsel.

In additions, The University College shall –

i) Make the necessary arrangements for all electronic records that would normally be saved if they were paper documents to be retained on the same basis. Individual users shall be ultimately responsible for backing up their data files using the appropriate drives.

ii) Develop procedures for complete data reconstruction and resumption of the system operations. These procedures shall be documented and suitably stored and shall include retention periods etc.

iii) Be obliged to maintain archives of data of critical University College systems for a time frame that is beyond the normal backup retention period, for future needs.

8.6 Strategic Application and use of the Technologies

The University College's technologies shall be used to support the institutions strategic objectives including but not limited to:

i) Teaching
- a) Integration of technology in teaching
- b) Training (lecturers)
- c) Supporting technologies (resources)
- d) Technical support

ii) Administration & Operations
- a) Finance
- b) HR
- c) Registry
- d) Administration
    1. IT Dept.
    2. Physical plant, and Admin. Services

B.   E-MAIL PROTOCOL

1.0   Purpose

The Mico University College's email services support the educational and administrative activities of the University and serve as a means of official communication by and between users and the Mico University College. The purpose of this policy is to ensure that this critical service remains available and reliable, and is used for purposes appropriate to the University's mission.

All users of the email systems are required to comply with the rules and regulations governing the email systems.

2.0   Scope

The Email policy applies to all members of The Mico University College community who are entitled to email services and their related email records managed by the university's email system.

The Mico University College provides email services to faculty, staff and students, and to other affiliated classes of individuals as approved by the University. Use of The Mico University College's email services must be consistent with University's educational goals and comply with Jamaican law and university policies.

3.0   Email Account Ownership and Authorized Users

3.1   Users

The electronic mail systems and services are university facilities. All e-mail addresses and accounts maintained by the system are the property of The Mico University College.

i)   **Faculty and Staff**

Email services are available for faculty and staff to conduct and communicate University business. Incidental personal use of email is allowed with the understanding that the primary use be job-related, and that occasional use does not adversely impact work responsibilities or the performance of the university's systems or network.

Email services are provided only while a user is employed by the University and once a user's electronic services are terminated, employees may no longer access the contents of their mailboxes.

Faculty and staff email users are advised that electronic data (and communications using the University network for transmission or storage) may be reviewed and/or accessed by authorized University officials for purposes related to University business. The Mico University College has the authority to access and inspect the contents of any equipment, files or email on its electronic systems.

ii)   **Students**

Email services are available for students to support learning and for communication by and between the University and themselves. The services are provided only while a student is enrolled in the University and once a student's electronic services are terminated, students may no longer access the contents of their mailboxes.

Student email users are advised that electronic data (and communications using the University network for transmission or storage) may be reviewed and/or accessed in accordance with the Mico University College's Acceptable Use Policy. The Mico University College has the authority to access and inspect the contents of any equipment, files or email on its electronic systems.

iii)   **Other Users**

Individuals with special relationships with the Mico University College may be granted limited email privileges, including an email address, commensurate with the nature of their special relationship. The Mico University College is free to discontinue these privileges at any time.

iv)   **Personal Use**

Although the University's electronic messaging system is meant for university business use, the University shall allow the reasonable use of its electronic messaging systems for personal use once the applicable guidelines are adhered to:

- Personal use of the electronic messaging system should not interfere with work.
- Personal emails must conform to these policies and accompanying guidelines.
- Personal emails are advisedly kept in a separate folder and deleted regularly.
- Users should restrict the number of personal emails sent within working hours.
- Mass mailing is not allowed.

3.2   Copyright Laws

All users of the email system shall observe all applicable copyright laws and license agreements applicable to the University and the laws of Jamaica.

3.3 Acceptable Use under University Policies

Email users have a responsibility to learn about and comply with the Mico University College's policies on <u>acceptable uses of electronic services</u>. Violation of the Mico University College policies (including this one) may result in disciplinary action dependent upon the nature of the violation. Examples of prohibited uses of email include:

- Intentional and unauthorized access to other people's email;
- Sending "spam", chain letters, or any other type of unauthorized widespread distribution of unsolicited mail;
- Use of email for commercial activities or personal gain (except as specifically authorized by University policy and in accord with University procedures);
- Use of email for partisan political or lobbying activities;
- Sending of messages that constitute violations of the Mico University College's handbook.
- Creation and use of a false or alias email address in order to impersonate another or send fraudulent communications;
- Use of email to transmit materials in a manner which violates copyright laws.

Senior management, Deans and Heads of Departments are responsible for enforcing the application of the email policy throughout the University.

Abuses of the Mico University College's email services should be directed to the Information Technology Department.

3.4 Security and Privacy of Email and Passwords

The Mico University College attempts to provide secure, private and reliable email services by following sound information technology practices. However, the Mico University College cannot guarantee the security, privacy or reliability of its email service. All email users, therefore, should exercise extreme caution in using The Mico University College email to communicate confidential or sensitive matters. Users must not give their passwords to other persons.

The university reserves the right to monitor ALL electronic messages and to protect itself from any liability due to the unlawful use of the services provided. Further, users should be aware that during the performance of their duties, network and computer operations personnel and system administrators, may need to, periodically, observe certain transactional addressing information to ensure proper functioning of the university e-mail services, and on these and other occasions may inadvertently see the contents of email messages.

3.5 Best Practices in Use of Email

1. **Confidential Information**
   When sending the Mico University College restricted information, the user must encrypt the message as advised the University's Information Technology Department.

2. **Viruses and Spyware**
   The Mico University College email users shall be careful regarding unexpected attachments from unknown or even known senders, and shall not open such attachments nor follow web links within an email message unless the user is certain that the link is legitimate. Following a link in an email message executes code, which can also install malicious programs on the workstation.

3. **Identity and Theft**
   Forms sent via email from an unknown sender should never be filled out by following a link. Theft of one's identity can result..

4. **Password Protection**
   The Mico University College's policy requires the use of strong passwords for the protection of email. A strong password should contain digits or punctuation characters as well as letters.

5. **Departmental E-mail Boxes**
   Departments that provide services in response to email requests should create a shared mailbox to help support departmental functional continuity for managing requests sent via email.

6. **Forwarding Email**
   The Mico University College email users may choose to have their email forwarded to another mail repository. However, a non University College forwarding address should not be used if there is a reasonable expectation that confidential information will be exchanged. Email is not considered a secure mechanism and should not be used to send information that is not considered public.

   Staff email users on an extended absence should create an Out Of Office message, which should include the contact information for another staff member who can respond while the user is away from the office.

Staying Current
Official University communications such as urgent bulk email and course email must be read on a regular basis since those communications may affect day-to-day activities and responsibilities.

4.0   Email Content

The content of electronic messages qualifies as recorded material and is subject to the same rules and regulations as any other type of record created, used, or received and retained by the University throughout the course of business.

4.1   Creation of Messages

The same rules governing good sociable behaviour applying to face-to-face communication or to traditional written communication, apply also to electronic communication. Messages should reflect careful, professional and courteous drafting, particularly since they are easily forwarded to others. It is advised that every user of university email systems assume that others than the addressee[s] may read a message.

4.2   University Records

4.3   Offensive Electronic Content

It is strictly prohibited to send harassing, abusive, intimidating, discriminatory or other offensive electronic messages. It is a misuse of the facilities, and may in certain cases, be illegal for a user to receive, transmit, display or store such offensive material using University equipment. Such misuse may result in disciplinary or legal action being taken against those responsible.

C. ACCEPTABLE USE

1.0 Background: ICT Acceptable Use Protocol (AUP)

An acceptable use protocol (AUP), also known as an acceptable usage policy or fair use policy, is a set of rules applied by the owner or manager of a network, website or computer system that restrict the ways in which the network, website or system may be used.

AUP documents are written for corporations, businesses, universities, schools, internet service providers, and website owners, often to reduce the potential for legal action that may be taken by a user, and often with little prospect of enforcement.

Acceptable use policies are an integral part of the framework of information security policies; it is often common practice to ask new members of an organization to sign an AUP before they are given access to its information systems. For this reason, an AUP must be concise and clear, while at the same time covering the most important points about what users are, and are not, allowed to do with the IT systems of an organization.

It should refer users to the more comprehensive security policy where relevant. It should also, and very notably, define what sanctions will be applied if a user breaks the AUP. Compliance with this policy should, as usual, be measured by regular audits.

2.0 Purpose

This policy defines what constitutes acceptable use of the Information and Communication Technology (ICT) resources of the Mico University College.

The mission of The Mico is to support National and Regional development through well-educated populations by equipping students locally, regionally and internationally with the required Teacher Education knowledge, skills, attitudes and values.

The University's ICT resources are provided for the use of members of staff, registered students and other authorized persons in pursuit of the goals and objectives of the Mico. Users of the University's ICT resources have access to valuable resources, sensitive data and networks. Consequently, it is important that they use these resources in a responsible, ethical and legal manner.

In general, "acceptable use" means an accountable and appropriate exercise of the opportunity to use, while respecting the rights of other computer users, the integrity of the University's Information and Communication Technology (ICT) resources and all pertinent licences and contractual agreements.

3.0 The Mico's (ICT) Resources

The ICT resources of the Mico include, but are not limited to, all items of

1. Hardware
2. Software
3. Networking equipment, services and facilities
4. Communication equipment, services and facilities
5. Data and information
6. Processes and Procedures

That are owned, leased, or loaned, by the Mico or its agents, irrespective of where these items may be located. Access to the Mico's ICT resources is conditional on the compliance to this policy.

Examples of these ICT resources include, but are not limited to:

1. ALL computing infrastructure under the responsibility of the Mico.
2. The Student Management System (SMS)
3. Financial and other enterprise applications
4. The University's Local and Wide area networks (LANs and WAN)
5. Electronic mail
6. Internet access
7. Web pages ·
8. Public computing facilities
9. Voice telephony systems
10. Wireless network systems
11. Human resource data and Student data
12. Learning and teaching platforms and systems

4.0 Guidelines on Usage

4.1 Acceptable Use

University information systems are to be used solely for University-related business, inclusive of the teaching and learning processes. However, personal use of computers may be permitted if, and only if, such conforms to the general university regulations and do not:

a. Interfere with University's operations,
b. Adversely affect the operations of the computing infrastructure
c. Negatively impact on any aspect of the University
d. Hinder the intended learning outcomes of students or
e. Retard the performance of duties by employees.
f. Incur any unapproved cost

4.2   Unacceptable Use

Use of the Mico's ICT resources is a privilege extended by the University to its staff, registered students and approved others. Any use of the ICT resources of the Mico will be considered an unacceptable use if it:

1. Conflicts with the aims and objectives of the University or
2. Breaches any statute or ordinance of the University or
3. Could result in legal action being taken against the University or
4. Violates national laws.
5. Is deemed legally, morally or ethically or otherwise inappropriate by the management of the University

Examples of unacceptable use include, but are not limited to:

a. Intentionally circumventing or compromising the security controls or integrity of the Mico's ICT resources or any other computer or communication network resource connected to it.

b. Intentionally denying access to or interfering with any network resources, including spamming, jamming and crashing any computer.

c. Using or accessing any of the Mico's ICT resource information or data, without proper authorisation, or in a manner inconsistent with the authorisation.

d. Using the University ICT resources to attack computers, accounts, or other users by launching viruses, worms, Trojan horses or other attacks on computers in the University College or elsewhere.

e. Conducting commercial activity not duly approved in writing by the University.

f. Using the University's ICT resources to misrepresent or impersonate someone else.

g. Using the University's ICT resources for any purpose which the University deems obscene or offensive.

4.3   Penalties for Unacceptable Use

Where there is evidence of unacceptable use, the University will restrict or prohibit the use of its ICT resources and as well take any other action that may be deemed appropriate. Violations of this policy shall be treated in accordance with applicable University Rules, Policies and Regulations and the laws of Jamaica.

D.   REFERENCES

The Laws of Jamaica
i)   Copyright Act, 1999
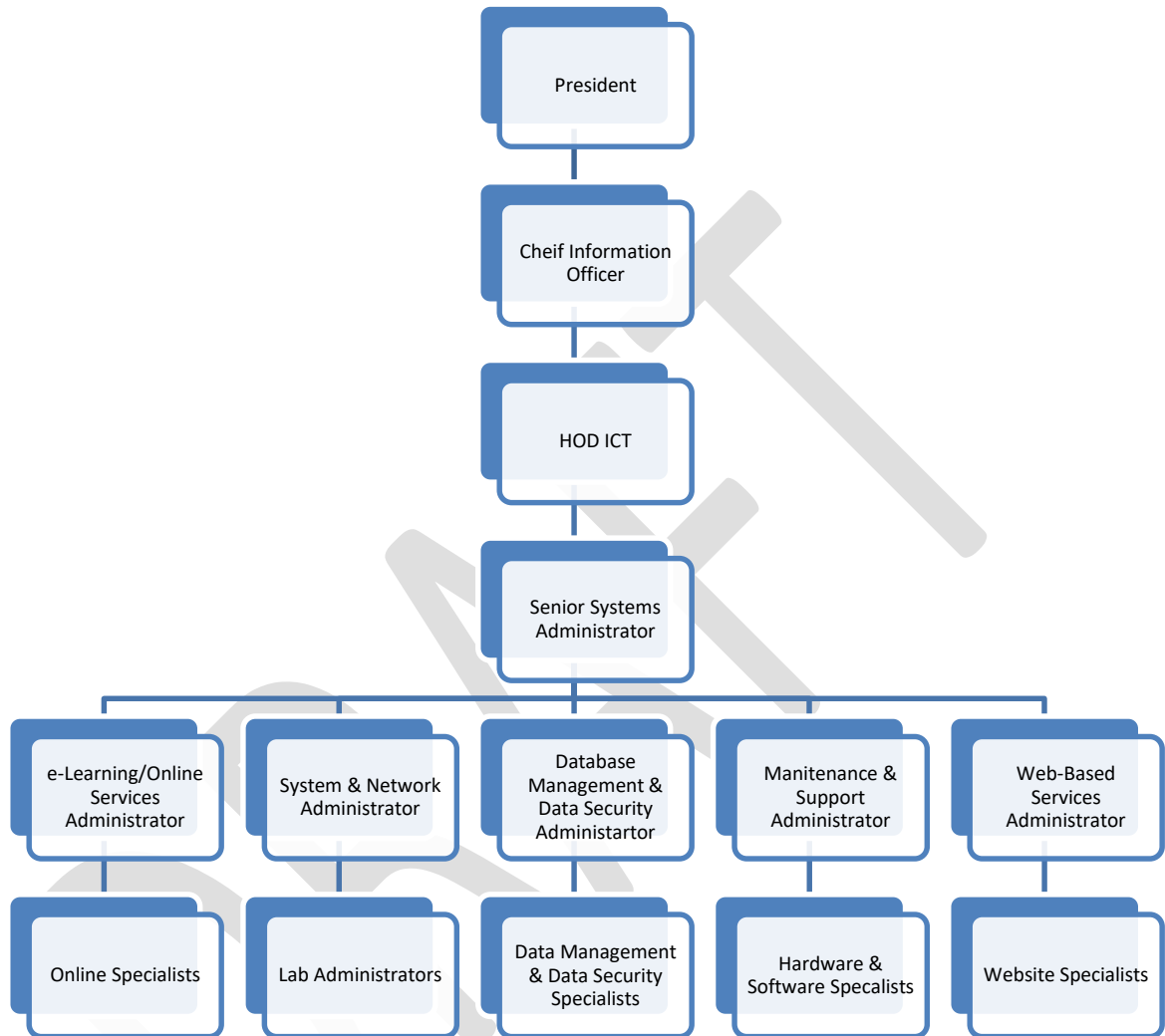ii)   Government of Jamaica, ICT Policy, 2011

The Mico University College's Policies, Codes, Guidelines
iii)   Record Management Policy
iv)   Code of Conduct

E.   ADDENDUM

Addendum I – Recommended Organizational Structure for the ICT Department

The proposed structure seeks to reflect best practices within the industry and to facilitate efficiency. With the CIO reporting directly to the President, matters related to ICT will be given direct priority. The new structure seeks to broaden the scope of services and expertise provided by ICT department to the institution. The structure also seeks to expand the support of ICT to the all the operations of the institution by addressing the future developments in ICT. The aim of the structure is to integrate quality staff as the platform to dive the implementation of ICT as a major tenet of the institution's growth and development.

Addendum II – User Agreement for E-mail service

User Agreement and Acceptance

All users of the ICT resources of the Mico are required to sign this document. This signifies your acceptance of this policy, and commitment to comply with its provisions. This document covers all the ICT resources of the Mico University College, which include, but are not limited to :

1. Hardware;
2. Software;
3. E-mail;
4. Networking equipment, services and facilities;
5. Learning and teaching platforms and systems;
6. Communication equipment, services and facilities;
7. Data and information.
8. Processes and Procedures

I.   I understand that the Mico provides, operates and maintains its ICT resources to support its instructional, research, and administrative activities. I understand that my assigned access credentials (including user names, passwords and other security facilities) identify and allow my access to the Mico's ICT resources and that I am accountable for the secrecy of my access credentials. I agree that I am responsible for all actions and consequences of my actions committed through the use of my access credentials.

II.   I agree that the Mico has the right to access, impound and search any of its ICT resources at any time and for any reason, including determining compliance with University, Campus or other information security requirements.

III.   I agree to comply with the Mico's Acceptable Use Policy and accept that as a user of the Mico's ICT resources I have a responsibility for the security of those resources. To the best of my ability I will protect the Mico's ICT resources from unauthorized use, modification, destruction or disclosure, whether accidental or intentional. I agree to be bound by the current version of the Mico's Acceptable Use Policy, which will be freely available to the University community.

IV.   I understand that abuse of these requirements, and others which may be declared in the future, may result in disciplinary and/or legal action.

V.   I hereby acknowledge that I have read, understood and agreed to the terms of The Mico's E-mail Protocol and Acceptable Use Policy. I agree to be bound by the conditions herein and understand that failure to comply might result in disciplinary or legal action being taken against me by The Mico University College.

Signature: _____

Print Name: _____

Date: _____

Student/Staff ID No: _____

Position: _____

Office/Faculty: _____

Department/Unit: _____

DRAFT