UGANDA MARTYRS UNIVERSITY

ICT Policy Framework

February 2025

Contents

Definition of Key Terms

Cloud: A global network of remote servers designed to store and process data for other devices and computers

Data Breaches: A data breach is any security incident in which unauthorized persons access sensitive or confidential information, including personal data e.g. Social Security numbers, bank account numbers, healthcare data etc. and corporate data e.g. customer records, intellectual property, financial information etc.

Demilitarized (DMZ): sometimes referred to as a "demilitarized zone" functions as a subnetwork containing an organization's exposed, outward-facing services. It acts as the exposed point to an untrusted network, commonly the internet.

Encryption: The process of converting information or data into a code, especially to prevent unauthorized access.

Abbreviations/Acronyms

BCP&DR	Business Continuity Plan and Disaster Recovery
BYOD	Bring Your Own Device
CCTV	Closed Circuit Television
ICT	Information and Communication Technology
NDA	Non-Disclosure Agreement
OSS	Open-Source Software
SDLC	Software Development Life Cycle
SLA	Service Level Agreement
UMU	Uganda Martyrs University
USB	Universal Serial Bus
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity

1.0 Introduction

Uganda Martyrs University's ICT Policy aims to create a comprehensive framework that governs the responsible and effective use of ICT resources across the institution. This policy aims at ensuring that all students, faculty and staff engage with ICT systems in a way that promotes academic integrity, improves the learning experience and protects sensitive information, to promote a culture of compliance and responsibility by setting clear standards for acceptable use. Account Management and Incident Response is committed to ensuring that all member university communities understand their roles and responsibilities for protecting IT resources.

Additionally, the policy emphasizes the importance of strong security measures, such as password management. network access control and securing the physical infrastructure. Its aim is to ensure business continuity through effective disaster recovery planning. and reduce risks associated with unauthorized access and data breaches. By integrating user awareness initiatives and promoting continued professional development in ICT skills, the policy supports the University's mission of leveraging technology as a key factor in teaching, learning and research. In the end, this IT Policy shall serve as a guiding document that aligns technology practices with the university's strategic goals, improve service and foster an environment conducive to innovation and collaboration.

2.0 Rationale of the Policy

The rationale of the ICT Policy shall be to guide all stakeholders while making use of the ICT facilities and services, while at UMU.

3.0 ICT Legal Framework

The University ICT policy shall be implemented in compliance with relevant National and International Laws and conventions. These may include among others:

i. Electronic Media Act, 2012
ii. Electronic Signature Act, 2011
iii. Electronic Transaction Act, 2011
iv. National Development Plan III
v. National ICT Policy, 2014
vi. National Information Technology Authority Act, 2009
vii. The Anti-Pornographic Act, 2014
viii. The Communications Act 2013

ix. The Computer Misuse Act, 2021 as Amended
x. The Constitution of the Republic of Uganda (1995) as Amended
xi. The Employment Act 2006 and regulations
xii. The National Council for Science and Technology Act, 2009
xiii. The National e-Governance policy 2011
xiv. The PPDA Act 2003
xv. The Universities and Other Tertiary Institutions Act, 2001 as amended
xvi. Uganda Communication Regulatory Authority Act, 2012
xvii. Uganda Human Rights Act, Cap.24

4.0 Scope of the policy

This policy applies to University Management, the ICT Department, Faculties, Schools and Institutes, all academic staff, students and consultant. The policy shall be used as a tool to guide, manage and ensure that ICT facilities, infrastructure and services provide support to the core business of teaching and learning while maintaining upgrades of systems to match trending technologies.

Policy Statements

Information and Communication Technology facilities are tools that facilitate the storage, manipulation, analysis and transfer of the university data.
UMU Management shall be committed to facilitate the provision of safe, effective and efficient usage of ICT facilities to its stakeholders (Academic and Administrative Staff, students, and Visitors).

ICT department of UMU shall train staff and students to develop innovative ICT technologies that provide more secure, efficient and effective solutions to teaching and learning, research and community engagement.

1. **eLearning** comprises all forms of electronically supported learning and teaching. eLearning applications and processes include Web-based learning, computer-based learning, virtual education opportunities and digital collaboration. Content is delivered via the Internet, intranet/extranet, audio or video tape, satellite TV, and other electronic media. It can be self-paced or instructor-led and includes media in the form of text, image, animation, streaming video and audio.

1. **Fully online courses** meet online for 100% of the class meetings required per student credit hour, including class meetings for which exams, tests and quizzes are administered.

2. **Blended courses** contain a mixture of face-to-face classes and sessions conducted online, with no more than 60% of class meetings held in assigned on-campus classroom locations, 40% of class sessions are held online.

5.0 Guiding Principles

UMU shall ensure that:

Principle 1: Match to the Curriculum

pedagogy is matched and aligned to the appropriate curriculum as approved by Uganda National Council for Higher Education through, clear objectives, relevance of content covered, appropriateness of student activities and nature of the assessment

Principle 2: Inclusion

the mode of delivery supports inclusive practice in terms of different types and range of achievement; physical disabilities that can be particularly supported by eLearning; different social and ethnic groups; and gender. eLearning solutions shall be designed to place the student in charge of their own education. The range of communications approaches adopted should provide support to practices of a wide variety of social, ethnic and gender preferences.

Principle 3: Learner Engagement

the mode of instruction on the e-platforms engages and motivates learners. This engagement should be evident in the ethos of being both educational and motivating. The user interface of the eLearning platform shall be friendly and accessible, avoiding confusion or discouragement of students and teachers. Students' progress reports and task lists should be provided to students to keep them up-to-date.

Principle 4: Innovative Approaches

eLearning shall be fit for purpose. It shall be evident why learning technologies are being used, rather than a non-technological approach which achieves the same end as effectively. UMU provides technology and tools that make it easy to create a connected and personalised environment that challenges students to practice problem-solving, to work together and to use creativity to construct, share, and present their ideas, thinking and learning.

Principle 5: Effective Learning

eLearning provision can meet the needs of a full range of flexible and independent learning experiences. This includes on and off campus learners in local, regional, national and international settings and cover both blended and full eLearning courses ranging from full awards to informal and individual learning

Principle 6: Coherence, Consistency & Transparency

teaching is internally coherent and consistent in the way the objectives, content, student activity and assessment match to each other. Teaching is open and accessible in its design.

Principle 7: Interoperability of eLearning Environments

all systems, both manual and electronic, used in the eLearning context interoperate in the most effective way to provide learners with an effective and increasingly individualized learning environment encompassing all aspects of their experience as a student of the University, as part of a holistic Managed Environment for Learners

Policy Statements

i. eLearning Infrastructure

   a. ICT Infrastructure

      i. eLearning requires a robust, scalable and available network infrastructure. It is necessary therefore for management to invest in high quality network infrastructure and internet bandwidth for seamless learning.
      ii. End-users including staff and students need mobile devices (including laptops and tablets) to access eLearning materials on the Virtual Learning Environment (VLE) - Moodle.

   b. Management and Administration of eLearning Infrastructure

      i. It is the responsibility of the ICT department to design, implement and maintain the eLearning network infrastructure. Access to the eLearning VLE, Moodle shall be governed by the Network Access Policy guidelines and the network will be protected by the required Firewall configurations according to the Network Firewall Standards.

ii. Data in the VLE will be stored for a period not exceeding 2 years.
iii. The ICT Department has responsibility of meeting the guidelines below for the VLE systems which they maintain, namely Moodle:
    a. students should be confident that any programme or element offered for study has had the reliability of its delivery system tested, and that contingency plans would come into operation in the event of the failure of the designed modes of delivery;
    b. students should be confident that the delivery system of the programme or element of study delivered through eLearning methods is fit for its purpose, and has an appropriate availability and life expectancy;
    c. students should be confident that the delivery of any study materials direct to students remotely through, for example, eLearning methods or correspondence, is secure and reliable, and that there is a means of confirming its safe receipt
    d. students should be confident that their assessed work is properly attributed to them, particularly in cases where the assessment is conducted through remote methods that might be vulnerable to interception or other interference;
    e. students should be confident that any mechanisms, such as web-based methods or correspondence, for the transfer of their work directly to assessors, are secure and reliable, and that there is a means of proving or confirming the safe receipt of their work.

iv. Faculties and schools that use delivery systems which are not supported by ICT would be expected to assume responsibility for ensuring that:

    1. All the above guidelines apply
    2. Data stored on the platform conforms to the Data Classification and Information Security Policy

c. Support Personnel

i. Designated personnel must be recruited and or appointed by Management to provide technical support to users of the eLearning VLE. These include:
    1. eLearning Administrator: This individual is part of the ICT Team and is responsible for the Administration of the VLE,

Moodle.

2. ICT Helpdesk: The IT Helpdesk Officers provide support for hardware and software issues related to access and use of Moodle. These can be contacted on phone, email or telegram
3. Video and Content Editor: This is a professional individual that provides support to the Academic staff to develop online videos for teaching and learning purposes.

ii. eLearning Policy Implementation.

a. The ICT department will oversee the implementation of eLearning and will report to the ICT Steering Committee. The Steering Committee will oversee the development of an evaluation plan to assess the impact of the policy.

b. eLearning material: All teaching and learning material produced at the Uganda Martyrs University belongs to the University. This policy mandates the placement of online course materials produced at UMU on the official VLE, Moodle.

c. Intellectual Property Right: A Faculty, School or Institute has the same control and ownership of the substantive and intellectual content of their online course materials as stipulated in the Intellectual Property policy

d. All students who register to study at UMU will be required to have a laptop, tab or tablet for use during study as a must. UMU will allow students to join its scheme which allows them to acquire a connected laptop at very minimal prices.

iii. Faculties, Schools and Institutes should:

a. ensure that students have access to information that sets out the respective responsibilities of the school / Faculty and University for the delivery of the programme, module, course unit or element of study;

b. ensure that students have access to module descriptors, to show the intended learning outcomes and teaching, learning and assessment methods of the module(s) / course unit (s)

c. ensure that students have access to a clear schedule for the delivery of their study materials and for assessment of their work.

d. ensure that students can be confident that study materials, whether

delivered through traditional methods or through web-based or other distribution channels, meet the expectations of the University with due respect to the quality of teaching and learning-support material for a programme or element of study leading to one of its awards;

e. ensure that students can be confident that staff who provide support to learners on these programmes have appropriate skills, and receive appropriate training and development;

f. ensure that students can be confident that the online programme, content and delivery is subject to Quality Assurance and the University Periodic Review process.

g. ensure that students have access to a schedule for any learner support available to them through timetabled activities, for example tutorial sessions or web-based conferences;

h. ensure that students have access to clear and up-to-date information about the learning support available to them locally and remotely for their programme or elements of study;

i. ensure that prospective students receive a clear and realistic explanation of the expectations placed upon them for study of the programme or elements of study, and for the nature and extent of autonomous, collaborative and supported aspects of learning.

j. ensure students have access to documents that set out their own responsibilities as learners, and the commitments of the University, faculty, school and institute for the support of a programme or element of study.

k. ensure students have where appropriate, regular opportunities for inter-learner discussions about the programme, both to facilitate collaborative learning and to provide a basis for facilitating their participation in the quality assurance of the programme;

l. ensure students have appropriate opportunities to give formal feedback on their experience of the programme and the Faculty, School or Institute should provide feedback to students on their concerns.

m. ensure students have access to information on the ways in which their achievements will be judged, and the relative weighting of units, modules

or elements of the programme in respect of overall assessment.

n. ensure students have access to timely formative assessment on their academic performance to provide a basis for individual constructive feedback and guidance, and to illustrate the awarding institution's expectations for summative assessment.

o. ensure that students can be confident that those with responsibility for assessment are capable of confirming that a student's assessed work is the original work of that student only, particularly in cases where the assessment is conducted through remote methods.

iv. Students and Prospective students should:

a. note that only registered UMU students with an Official UMU email address will have access to the VLE, Moodle and any online course.

b. note that only the ICT Department through your Faculty, School or Institute will create your Moodle access account.

c. note that all students accessing Moodle online courses must adhere to the rules, principles and guidelines of the Acceptable Use Policy and Information Security Policy. Students must also note that breach of any of these policies will lead to disciplinary action.

5.1 ICT Acceptable User Policy

Policy Objectives

UMU ICT shall:

i. Have resources for its core business purposes and shall be used to achieve its core mandate, vision and mission.
ii. Protect users' rights while accessing UMU ICT resources.
iii. Ensure Integrity, confidentiality and quality of UMU data, resources and ICT services.

Policy Statements

i. Authorization: In order to use the ICT Facilities of the University a person shall first be properly registered to use such services. Use of universities ICT facilities shall be deemed to be in acceptance of the terms and conditions of this policy. It is expected that all users will adhere to the University's password policy and

guidelines, Information Security policies in addition to all relevant university, regulatory and legal requirements.

ii. The University recognises that individuals may conduct personal use of email and the Internet. However, this shall be kept to a minimum and be compliant with the various university and legislative requirements. The University reserves the right to revoke such permission if, in the judgement of the University, these facilities are abused.

iii. University staff that have access to personal data (as defined under the Data Protection and Privacy Act 2019 and the Data Classification Policy) are responsible for ensuring that such data is not made available to unauthorised individuals and that the security of all systems used to access and manage this data is not compromised.

iv. The University has the right to access a personal account after the staff member leaves for operational reasons and for the continuing delivery of services.

v. Where abuse is suspected (especially criminal activity and/or gross misconduct), the University may conduct a more detailed investigation involving further monitoring and examination of stored data (including employee-deleted data) held on servers/disks/drives or other historical/archived data.

vi. Where disclosure of information is requested by the police (or another law enforcement authority) the request where possible will be handled by the University's ICT Department or other relevant person. Other than in emergency situations, all requests for access to personal data shall be subject to approval by the Office of the Vice Chancellor.

Unacceptable & Acceptable Usage: ICT Labs:

i. Food or drinks shall not be consumed in the vicinity of ICT equipment to avoid damage to the equipment and encourage vermin.

ii. Excessive noise (talking, loud music) that may interfere with other users is prohibited.

iii. Mobile phones must be switched off or put in silent mode before entering an ICT area as they can interfere with other users.

iv. Unreasonable behaviour (for example using facilities for games, chats etc. when others cannot access a system to carry out study related work) is not acceptable.

Unacceptable & Acceptable Usage: ICT Facilities:

i. Creating, displaying or transmitting material that is fraudulent or otherwise unlawful or inappropriate.
ii. Threatening, intimidating or harassing employees/students.
iii. Using obscene, profane or abusive language.
iv. Intellectual property rights infringement, including copyright, trademark, patent, design and moral rights.
v. Defamation (genuine scholarly criticism is permitted).
vi. Unsolicited advertising is often referred to as "spamming".
vii. Sending emails that purport to come from an individual other than the person
actually, sending the message using, e.g., a forged address.
viii. Attempts to break into or damage computer systems or data held thereon.
ix. Actions or inactions which intentionally, or unintentionally, aid the distribution of
computer viruses or other malicious software.
x. Attempts to access or actions intended to facilitate access to computers for which
the individual is not authorised.
xi. Using the University network for unauthenticated access.
xii. Unauthorised resale of university services or information.
xiii. Using the ICT Facilities to conduct personal commercial business or trading.
xiv. Connecting devices that have not been explicitly approved/sanctioned by ICT to University equipment for the purposes of using University ICT services.
xv. Any other conduct, which may discredit or harm the University, its staff or the ICT Facilities or is intentionally unethical / illegal even if not specifically listed in this policy is deemed unacceptable. This will be decided by the relevant University authorities.

Unacceptable & Acceptable Usage Additional Restrictions:

1. Downloading, distribution, or storage of music, video, film, or other material, for which you do not hold a valid licence or other valid permission from the copyright holder.
2. Distribution or storage by any means of pirated software.
3. Connecting an unauthorised device to the University network, i.e. one that has not been configured to comply with this policy and any other relevant

regulations and guidelines relating to security, purchasing policy, and acceptable use.

4. Circumvention of network access control.
5. Monitoring or interception of network traffic, without permission.
6. Probing for the security weaknesses of systems by methods such as port-scanning, without permission.
7. Associating any device to network Access Points, including wireless, to which one is not authorised.
8. Non-academic activities, which generate heavy network traffic, especially those which interfere with others' legitimate use of ICT services or which incur financial costs.
9. Excessive use of resources such as file storage, leading to a denial of service to others, especially when compounded by not responding to requests for action.
10. Frivolous use of University owned ICT facilities, especially where such activities interfere with others' legitimate use of ICT services.
11. Use of University business mailing lists for non-academic as well as unofficial purposes.
12. Use of CDs, DVDs, and other storage devices for the purpose of copying unlicensed copyright software, music, etc.
13. Copying of other people's website material without the express permission of the copyright holder.
14. Use of peer-to-peer and related applications within the University. These include, but are not limited to, Ares, BitTorrent, Direct Connect, Morpheus, KaZaA etc.
15. Publishing or distributing material or statements which encourage or glorify terrorism.
16. Disseminating terrorist publications.
17. Collecting information likely to be useful in the commission or preparation of terrorism.
18. Downloading or distributing indecent images of children.
19. Downloading or distributing pornographic images.
20. The University reserves the right to implement filtering to block access to unlawful material, except where access is necessary as part of a legitimate research project where access to unlawful material has been specifically authorized under the University’s research ethics procedures.

5.2 ICT Standards

Policy Objectives

It is the intention of UMU to ensure that:

i. ICT systems are of the current, highest and most cost effective technical and operational standards.
ii. all systems are interoperable and integrated.

Policy Statements

The ICT Department shall be responsible for:

i. The development of ICT technology standards and advising users and management of the various units of the university on the application of standards from time to time.

ii. Development of the specifications for all user ICT systems.

iii. All ICT Procurements, system development and acquisitions and compliance with the ICT Standards and specifications shall be approved by the ICT Department of the University.

iv. Ensuring follow up of the ICT Standard Operating Procedures (SOPs) and policies as described in this manual.

v. Continuously reviewing business needs, direction, and developing or updating the necessary ICT standards and specifications to match prevailing needs.

vi. Reviewing and incorporating the ICT Industry and statutory standards into UMU's ICT SOPs in order to ensure that its standards conform to the legal, Industry, market standards and trends.

vii. Publishing/advising users of current standards as and when they are realized.

viii. Inspecting, testing and certifying all ICT systems (new or existing), to ensure that they conform to the set IT standards.

5.3 User Account Management

Policy Objective

The purpose of the UMU User Account Management Policy shall be to establish the rules for the creation, monitoring, control and removal of user accounts

Policy Statements

i. All individuals who shall use the UMU applications and/or have access to any UMU information systems shall have individual user accounts.

ii. All accounts shall be uniquely identifiable using the assigned username. The official names of the staff shall be captured and associated with the account during the registration process.

iii. Users with administrative rights shall log on the system using their own user names. The main administrative account shall only be used with approval from the Head of ICT of the University.

iv. For security purposes, the default Administrative Account name(s) and default password of any newly implemented Information System at UMU must be changed within 3 working days of "go-live". A list of administrative account names and passwords for the respective systems running at UMU shall be kept securely with the Head of the ICT Department of the University. This list shall be kept up to date as per changes to the accounts.

v. User accounts shall be in the format "*FirstNameInitialLastname*", eg. A user called Antonio Kapere shall have a user account as "*akapere*"

    a. In case there are users with similar names, the initials of the middle name will be used.

vi. All accounts created shall have an associated request and approval from Head ICT of the University.

vii. The Director, Human Resources (HR) shall be responsible for sending and authorising requests for creation and deletion of staff user accounts. The Director HR shall also inform the IT unit leadership about staff who are suspended or whose accounts require to be disabled temporarily.

viii. The Heads of Department, in consultation with Director HR, shall be responsible for sending and authorising requests for provision and modification of the appropriate user access rights/levels to the specific systems. The Heads of Department shall also make requests for user accounts for non-UMU members of staff who require temporary systems access, indicating at a minimum the business need, duration of access and the systems to be accessed.

ix. All accounts must have a password that complies with the UMU Password Policy.

x. System Administrators or other designated staff:

   a. Are responsible for creating, modifying and removing the user accounts as per written and authorised requests indicated above, documenting and maintaining the documentation for this process

   b. Must periodically, preferably every 3 months, and in conjunction with Heads of Department review existing accounts for validity. User accounts that are idle or dormant for more than 45 calendar days without prior notice shall be disabled and marked for deletion.

   c. Are subject to independent audit review,

   d. Must provide a list of accounts for the systems they administer when requested by authorized UMU management,

   e. Must cooperate with authorized UMU management investigating security incidents.

5.4 Telephone Usage

Policy Objective

The purpose of this policy shall be to provide:

i. guidance on the use of mobile and fixed telephones, to promote the responsible use of telephones and mobile communications devices, and to provide guidance for the use of such devices in compliance with UMU regulations.

ii. Support of fixed telephones, it may under special circumstances permit the purchase of mobile service to further UMU's mission. UMU desires that the use of these devices be cost-effective and properly managed. This policy details responsibilities of staff of UMU with regard to use of telephones and mobile communications devices.

Policy Statements

i. All UMU owned or operated telephone systems shall be used only to conduct official business.

ii. Desk telephones are provided to enable staff members to perform their duties and to conduct the business of UMU. Where there is a direct business need, a mobile phone will be provided by UMU, who will pay for network access and work-related calls.

iii. Airtime shall be provided to users as per management approved schedules from time to time. Staff who require additional airtime or services shall make the request through their respective Head of Department.

iv. Employees receiving mobile telephone handsets or devices shall be required to sign acknowledging that they have received the equipment and understand the usage policies.

v. Staff must ensure that they secure their telephone devices with a PIN or password to ensure that unauthorised users do not access or use their devices.

vi. UMU recognises that, from time to time, staff may need to make personal calls using the UMU telephone systems. Users are expected to use professional judgement and keep personal calls to the minimum. Personal calls should not interfere with one's duties or with the duties of other staff and should not impact on productivity. Where it is established that personal usage is undermining business objectives, UMU management may restrict usage and require the staff to pay the accumulated bills.

vii. Internal telephone extensions (landlines) should not be diverted to mobile phones, as this escalates the cost to UMU. Where there is a business need, the staff shall make a request through their Head of department and the application shall be considered for approval by UMU management.

viii. In accepting an UMU mobile or desk telephone staff should acknowledge UMU's right to list their names in its telephone or other associated directories and to have the extension number and calling party displayed.

ix. University registered telephones must never be used to threaten, harass or indulge in gaming/gambling. Any user found guilty will be individually liable for prosecution.

5.5 Demilitarised Zones (DMZ)

Policy Objective

i. The purpose of this policy is to define standards to be met by all equipment owned and/or operated by UMU located outside UMU's Internet firewalls. These standards are designed to minimize the potential exposure to UMU from the loss of sensitive or company confidential data, intellectual property, damage to public image etc., which may follow from unauthorized use of UMU's resources.

ii. Devices that are Internet facing and outside the UMU firewall are considered part of the "demilitarised zone" (DMZ) and are subject to this policy. These devices (network and host) are particularly vulnerable to attack from the Internet since they reside outside UMU firewalls

Policy Statements

UMU Demilitarised (DMZ) shall:

i. Be separated and segmented from the University's internal networks
ii. Be clearly labelled and identifiable from the rest of the network systems. In addition, the Head ICT of UMU shall maintain a list of who has access to the equipment
iii. A firewall device must be the only access point between the DMZ network and the rest of UMU's networks and/or the Internet. Any form of cross-connection which bypasses the firewall device is strictly prohibited.
iv. Original firewall configurations and any changes thereto must be reviewed and approved by Head ICT of UMU (including both general configurations and rule sets).
v. Traffic from UMU's DMZ to the UMU internal network, including VPN access, falls under the Network Access Policy
vi. All routers and switches not used for testing and/or training must conform to the DMZ Router and Switch standardization documents.
vii. Operating systems of all hosts internal to the DMZ running Internet Services must be configured to the secure host installation and configuration standards
viii. Current applicable security patches/hot-fixes for any applications must be applied within the DMZ network. UMU must have processes in place to stay current on appropriate patches/hotfixes
ix. Services and applications not serving business requirements must be disabled.
x. UMU's Confidential information is prohibited on DMZ equipment where non-UMU personnel have physical access (e.g., equipment in training laboratories),

5.6 ICT Project Management

Policy Objective

The purpose of this policy shall be to ensure that ICT projects at UMU are consistently initiated, planned, implemented and closed in a manner that they deliver solutions that are within schedule, budget and desired quality.

Policy Statements

ICT Projects shall:

i. Have clear specifications, goals, scope, requirements and activity/implementation schedule before execution.
ii. Have a formal ICT Project Business case prepared for all medium to major projects.
iii. Be designed and executed in such a manner that they produce solutions/products that offer value-for-money and are fit-for-purpose.
iv. Have a Project initiator who shall seek and gain project execution/implementation approval from the respective User / Beneficiary department head, and Head ICT UMU.
v. Present projects to the ICT Department of the University for guidance and oversight.
vi. Be fully costed and have approved budgets, prior to execution. Projects that don't have approved budgets, must first get budget approvals, through either budget relocations or supplementary budgets
vii. Be assigned a Project Manager and project execution team, who will manage the project from beginning to end/closure.
viii. Have a Project Manager who shall ensure that the project is managed in such a manner that keeps the project on schedule, within budget and specified quality.
ix. Be formally documented, from initiation through execution up to closure
x. Have changes within the project formally documented and approved through a formal change management process of the University.
xi. At closure, be formally handed over to the respective beneficiary department and ICT Department, with all the solution/product documentation, as well as project management documentation.
xii. Do Post implementation review, and management of Warranty, Snugs, guarantees must be carried out after project closure.

5.7 Incident Management

Policy Objective

The objective of Incident Management shall be to:

i. Respond to security breaches or system failures quickly and effectively, reducing any potential business impact and to reduce the risk of similar incidents occurring.
ii. Ensure that UMU is able to identify perpetrators of malicious acts and that UMU preserves sufficient evidence to prosecute them if required.
iii. Reduce the time spent in recovering from incidents and will help in minimising the effects of an incident after it has happened and will help in preventing recurrence,
iv. Ensure proper tracking of incidents and creating a knowledge base of past events to be used in performance analysis and future planning.

Policy Statements

i. All information security incidents shall be reported and recorded in the ICT helpdesk, reviewed and resolved using an incident management process.
ii. Information security incident management communications shall be limited and shared with individuals on a need-to-know basis.
iii. Where necessary ICT shall make changes to systems, applications or networks and the incident response procedure must feed into any existing change management process.
iv. Incidents shall be reviewed to identify common threats and trends.
v. There must be mechanisms in place to enable the number, frequency, types and impact of information security incidents and issues to be quantified and reviewed.
vi. A clear point of contact shall be established for all employees, contractors and third-party users allowing them to raise information security incidents. The ICT Helpdesk shall be the main point of contact
vii. All users (including third party users) of UMU ICT Services shall be made aware of their responsibility to report suspected or actual information security non-compliance, and incidents, and the correct process for reporting information security incidents.
viii. The security incident owner shall track the information security incident to resolution and closure.

ix. Once incidents are identified measures shall be put in place to ensure that the incident does not spread to other systems or areas within the network.
x. Due care shall be taken to ensure that the incident containment process does not result in loss of evidence which will be key in resolving the cause of the incident.
xi. Computer incidents shall be separate from the UMU disaster management incidents.
xii. All identified disaster management incidents shall be escalated to the disaster management team.
xiii. Once recovery is successful the recovery procedure shall be recorded in the Helpdesk as lessons learnt in the incident log
xiv. Only members of the Helpdesk and competent ICT Technical staff shall be allowed to manage the recovery process
xv. All information about the incident shall be recorded and stored for future reference
xvi. An escalation procedure shall be used in the helpdesk depending on incident priorities.

5.8 Software Use Policy

Policy Objective

To ensure users of UMU systems are aware of the appropriate use of software, the inherent risk of using pirated software and caution shall be given against practices that can result in infringement of software license and copyright.

Policy Statements

i. Software shall be provided to UMU staff and students for purposes of supporting processes that relate to the University's business goals.
ii. All Software shall be centrally acquired and distributed in line with the Procurement policies, in order to ensure copyright and license compliance, information security, interoperability, support and maintenance and cost management.
iii. All software acquired for or on behalf of UMU or developed by UMU staff or contract personnel on behalf of UMU is and shall be deemed property of the University. All such software shall be used in compliance with applicable licenses, contracts, and agreements

iv. Only ICT Department approved software shall be installed on UMU equipment. The ICT Department shall work with the different faculties, schools, directorates and departments to establish their specific requirements for software.

v. All software used for or on behalf of UMU shall be correctly and appropriately licensed and used only in conformity with the terms of the license, whether the usage is on systems belonging to UMU or not.

vi. All software shall have sufficient documentation for license management, Administration and usage

vii. All copies of any illegal software installed by users on UMU computers shall be uninstalled immediately. This includes legally purchased software that has not been approved by the Head ICT UMU to run on University ICT equipment. The approval shall be in writing or in electronic format by the Head ICT UMU.

viii. No pirated software, i.e. computer software which one possesses illegally, is permitted to be used either on UMU's computer or on Personal computers for UMU's business.

ix. UMU software, licenses or product keys shall not be used or installed on equipment that does not belong to the University, unless properly authorised.

x. It is the responsibility of the ICT Department to ensure that UMU has the necessary software licenses for all software installed or authorized to be installed on UMU's computers.

xi. The ICT Department shall ensure that the latest software versions, patches and upgrades are available to staff and students of UMU.

xii. Only personnel of the ICT Department of the University or authorised personnel shall install software on UMU equipment. The ICT Department is exclusively responsible for installing and supporting all software on the University's computers. Users shall not install or modify software installed on the University's ICT equipment

xiii. No UMU staff member, contractor or agent working for or on behalf of UMU shall copy and/or install software onto any UMU computer without prior written approval /confirmation from Head ICT UMU.

xiv. Users shall request for additional software or software features/functionality from the ICT Department, for evaluation and eventual acquisition. Such requests shall be evaluated based on business needs, interoperability, information security, licensing requirements and cost-benefit

xv. All proposed software into the UMU ICT environment should have a supported business case and such a business case should be approved by the user Department Head and the Head ICT UMU.

xvi. All software applications shall be configured to enable and provide for automated and non-editable logs and audit trails.

xvii. A software application and license register shall be maintained by the ICT Department.

xviii. Software vendors shall demonstrate that they are duly authorized by the original software developers to resell the respective software. They shall also be in position to install, customize, support and maintain the software applications.

xix. This policy is applicable not only to any original installation but also to any upgrades to later versions of the software, which shall also be properly licensed.

xx. No one may use UMU ICT resources to modify, distribute, or copy proprietary data, directories, programs, files, disks or other software without proper authorization.

xxi. Where development of applications or infrastructure is being conducted by third-parties, specific measures must be taken to ensure that the security of both the development process and the delivered code are protected, as well as the fulfilment of security requirements derived from this Policy.

xxii. Software development process, whether internal or external shall follow a formal software development process e.g. SDLC, and shall be subject to a formal project management approach as well as the change management process.

xxiii. Open-Source Software (OSS) is software whose source code is openly published, is often developed by voluntary efforts and is usually available at no charge under a license defined by the Open-Source Initiative which prevents it from being redistributed under a more restrictive license. OSS is also subject to the requirements and restrictions stipulated in this software policy. This policy shall govern its acquisition and use within UMU.

xxiv. Contracts for the purchase of pre-developed packaged software or for the development of software by third parties must provide clarity and protection of UMU rights over licensing, ownership of code, access to source code and intellectual property.

xxv. When implementing 'Commercial, off the shelf' solutions, similar considerations should be part of the evaluation. The functional requirements of a system should as a minimum:

a) Document the process flows of the business processes to be automated
b) The expected key performance / system features
c) Should specify the competencies and roles that are required to complete the process.

d) Specify the key performance indicators required for the process to be completed
e) Specify the key inputs and expect outputs for each process

5.9 Change Management

Policy Objective

To implement formal change management control procedures that protect UMU information assets and to ensure that the change management procedure shall be used for efficient, planned, authorised and prompt handling of all changes, in order to minimise the impact of any related incidents upon service.

Policy statement

Changes to all information processing facilities, systems, software, or procedure shall be strictly controlled according to formal change management procedures.

i. *Change Initiation*: All system changes shall be initiated by filling in the change management request, which will be signed by the respective applicant, and addressed to the Head ICT UMU or his/her designate. The applicant shall as a minimum state;
   a) the required change,
   b) the reasons or basis for the change,
   c) change category (Minor or Major)
   d) the resources required,
   e) the risks / impact of the change, eg systems affected, downtime, etc,
   f) the testing plan,
   g) the date the change is required and duration of change,
   h) the lead person accountable for the change,
   i) the change implementation team and,
   j) the roll back plan.

ii. *Change Authorisation*: Authorisation for any changes, whether urgent or not, can only be given by the Head ICT UMU.

iii. *Testing of changes*: All testing will be done from a test environment and not the production environment.

iv. *Change approval*: The concerned user Unit shall check the system to see whether the results produced are as expected and a user acceptance testing (UAT) form shall be signed off before implementation in the production environment.

v. *Change Scheduling*: To minimize disruption to the normal working operations of UMU, changes will be scheduled during weekends, public holidays or after business working hours.

vi. *Change Communication*: All planned system changes should be communicated in advance to the concerned parties to minimize business disruption and inconveniences.

vii. *Change Recovery, Safety measures (Back-out / roll back plans)*: Before effecting any change in the production environment, a full backup of both the data and system state, on a clearly labelled backup data storage medium will be taken and kept.

viii. *Change Support*: In the event that the system change requested requires a vendor or 3rd party support/service provider, the request will be forwarded as thus, by the Head ICT UMU or any authorised persons, but the due process will be followed before its implementation in the production environment.

ix. *Change Documentation and tracking*: All system changes, whether approved or not will be documented and filed.

5.10 ICT Security Policy

Policy Objective

This policy shall aim at putting in place a framework for the handling and usage of USB ports and removable media in order to protect UMU information resources.

Policy statement

i. Users are responsible and accountable for the introduction of any malware and resultant disruption of UMU ICT systems and business operation, attributed to their usage of USB devices or other removable media,

ii. The use of removable media to carry UMU information out of the UMU environment is prohibited. Users must gain specific authorisation from their Heads of Department and Head ICT UMU.

iii. Management may limit or block USB ports or use of removable media on all or particular systems at any time.

iv. UMU removable media may not be connected to or used in computers that are not owned or leased by UMU without explicit permission of the UMU ICT Department staff.

v. Sensitive information shall be stored on removable media only when required in the performance users' assigned duties or when providing information required by other departments. Such usage must be duly authorised and documented.

vi. When Sensitive information is stored on removable media; it shall be encrypted and password protected to prevent unauthorised access,

vii. Users of UMU ICT systems shall not connect or attempt to connect any USB device or removable media from unknown and/or unauthorised sources or persons. Users must report any unattended devices or unknown devices found in the UMU environment to the ICT Department,

viii. All removable media shall be scanned for viruses and malware before being used at every usage event. In the event of any malware being detected and the antivirus system is unable to clean it, the user must discontinue usage and disconnect the device or media immediately, and immediately inform the ICT Department.

5.11 Business Continuity Plan & Disaster Recovery Policy

Policy Objective

i. To ensure continuous performance of UMU's Information Systems especially during emergencies through;
   a) Protecting equipment, data, and other assets, and reducing or mitigating disruptions to operations.
   b) Reducing damage and losses.
   c) Achieving timely and orderly recovery from emergencies and resumption of full service to all stakeholders

ii. This policy defines the backup for computer systems that store the University's data or information. Servers expected to be backed up include file servers, mail servers, web servers, application servers and database servers. All network configurations shall be backed up.

iii. To prevent the loss of university data in the event of an equipment failure or destruction

Policy Statements

i. UMU shall implement a Risk Management framework/register and carry out ICT risk analysis at least once every year. This process shall identify risks to ICT

systems and provide risk management measures, especially for the most critical systems.

ii. The contingency plan for UMU shall cover all business-critical applications within UMU and ensure that there is no-single point of failure for critical business operations and attendant systems.

iii. The contingency plan actions and provisions shall be tested from time to time to confirm its relevance and applicability to the present ICT operating environment. At a minimum, tests shall be carried out every 6 months. All tests shall be documented.

iv. Staff within the ICT Department shall be trained on the execution of the contingency plan actions and provisions and refresher training held at least once every 6 months.

v. UMU's Information Resources backup and recovery process for each system shall be documented and periodically reviewed for integrity. The review shall be done once every 3 months.

vi. When backups are taken, a log shall be kept. In the absence of an automated or electronic log, a physical/hardcopy log book shall be kept.

vii. The frequency and extent of backups shall be in accordance with the importance of the information and the acceptable risk as determined by the data owner. At minimum;
   a) A 2 hourly incremental data backup shall be taken for all mission critical UMU Application Databases, mail files, and the file server,
   b) A Monthly backup shall be taken for system state, system configuration files and the entire file repository.
   c) Backups shall not be kept together with the production systems. At a minimum, all backups should be kept off site.

viii. The vendor(s) providing offsite backup storage for UMU must be cleared to handle the highest sensitivity level of information stored. An SLA and NDA must be signed before commencement of service. The offsite backup or disaster recovery facility must be visited and checked at least once every 6 months to ensure the facility is functioning as intended.

ix. UMU shall endeavour to maintain the following in the contingency planning process;

a) An updated Risk Register, reviewed at least once every year.
b) Data Backup plan/schedule with off-site storage,
c) Backup, redundant or clustered servers and key infrastructure components, e.g., switches, routers, firewalls, data/internet connectivity and other mission critical systems – for purposes of fail-over or quick recovery,
d) Automatic fire suppression systems in the Server rooms. The Fire suppressants shall be designed to suite electronic equipment,
e) Server rooms shall have CCTVs and Biometric access controls that maintain an access logs,
f) Backup or secondary power and cooling systems,
g) System monitoring solutions with alerts and triggers for alarms and/or sending alerts to ICT and other key personnel about actual or imminent dangers to the systems,
h) Support and Maintenance contracts with vendors or 3rd party service providers, for mission critical systems,
i) A register of contacts for key personnel including Management, ICT, Administration, Security and vendors or 3rd party support/service providers,
j) System Documentation and labelling of Servers and key infrastructure components,
k) Systems planned preventive maintenance/service schedule,
l) Periodic tests and audits at least once every 3 months,
m) Register of the tests and how successful they were during the last recovery tests.
n) Training and awareness program to be done once every 6 months.

5.12 Internet Usage

Policy Objective

The policy shall:

i. define the appropriate uses of the Internet by UMU Staff, Students and affiliates.

ii. Ensure compliance with applicable statutes, regulations, and mandates regarding the use of the internet.

iii. Establish prudent and acceptable practices regarding the use of the Internet.

iv. Educate individuals who shall use the Internet, the intranet, or both with respect to their responsibilities associated with such use

Policy Statements

i. All UMU staff and students shall be eligible for internet access and usage. All non-staff/non-students shall require separate application and approval via the Head of Department of the supervising department or unit and Head of ICT UMU.
ii. Access to Internet shall be provided to users to support UMU business activities and only on an "as-needed" basis.
iii. Staff use of UMU internet shall not interfere with the normal performance of their duties or usage by other UMU users.
iv. Before connection to the internet a security firewall and proxy server shall be implemented to ensure only authorized traffic is allowed to be transmitted.
v. Any computer connected directly to the internet without going through the standard UMU firewall, shall be disconnected from the UMU network. Users shall disconnect from the UMU network before making direct internet connections. This shall apply to users who may have internet modems, routers or other access mechanisms other than the UMU internet service.
vi. Before Internet Domain Names are registered with Internet Service Providers (ISPs) they shall be approved by UMU management. This shall ensure that UMU presents a consistent corporate image to the external Internet community.
vii. Internet usage and all sites accessed shall comply with all Laws, the UMU Acceptable Use Policy and other UMU policies. At a minimum the following shall not be permitted when using internet services/facilities provided by UMU:
    a. Internet access to gain unauthorized access to other internal or external systems. A University VPN shall be used to access;
    b. Using any system that masks or hides the identity of the user,
    c. Creation, upload, download, viewing, storage, copying, or transmission of sexually suggestive, explicit or pornographic materials, materials deemed to undermine children or other persons privacy or rights;
    d. Creation, upload, download, viewing, storage, copying, or transmission of materials related to racial, gender, religious or partisan political activity, gambling, weapons, terrorist activities, and any other unlawful activities or activities otherwise prohibited by UMU or applicable laws;
    e. Downloading, copying, and/or playing of computer games;
    f. Downloading, playing /streaming audio and video files on the internet, other than those authorized by management,

g. Use for private commercial purposes or in support of "for-profit" activities or in support of other outside employment or business activity (e.g., consulting for pay, sales or administration of business transactions, sale of goods or services) unrelated to UMU
h. Engaging in any outside fundraising activity, endorsing any product or service, participating in any lobbying activity, unless approved by management;
i. Patent or Copyright infringement

viii. UMU staff and students intending to make information about UMU available on the Internet, e.g. on the website, shall have all material formally approved by UMU Management via the Public Relations Office for use on the Internet before the content is uploaded.
ix. All files uploaded to, and downloaded from the Internet shall be scanned for viruses using the approved anti malware / anti-virus detection software
x. All sensitive UMU material transmitted over external network shall be encrypted
xi. All user activity on UMU Information Resources assets is subject to logging and review. UMU may install tools and applications to monitor and enforce provisions of this policy.
xii. Internet access shall be discontinued upon termination of Staff, completion of contract, end of service of non-Staff, or disciplinary action arising from violation of this policy.
xiii. UMU reserves the right to limit or disable internet access to some or all users if there's abuse by any users.
xiv. Users shall report to their Supervisors or ICT Department any suspected, unusual or proved activity involving security breach or misuse or any such activity that has or may be in violation of the ICT policy.

5.13 Service Level Management

Policy Statements

i. The ICT Department shall be responsible for the contract management and supervision of Service Level Support and/or Maintenance agreements or contracts for ICT systems that the University shall enter into.
ii. Service Level Agreements shall form a basis for performance appraisal of the respective providers, and also form a basis for their payment or compensation.

iii. The ICT Department shall also formulate and monitor internal service levels for systems availability and Help desk support provision.

5.14 Support and Maintenance

Policy Objective

i. The purpose of this policy shall be to provide a framework for an effective and productive relationship with the users and ICT Department and to ensure that users enjoy the use of ICT services in the way and manner in which they were initially intended.
ii. The Policy shall ensure that UMU ICT Systems are well maintained.

Policy Statements

i. The ICT Department shall be available to all users of UMU ICT facilities to provide them with all needed user support. This shall include installation and setup of equipment and systems, upgrades, troubleshooting of system failures.
ii. The ICT Department, in conjunction with the Procurement Unit of the University, shall be the liaison between the University and the external suppliers, vendors or contractors of ICT support and maintenance services.
iii. All ICT equipment and services of a recurring nature, such as data/internet connectivity, software/applications, telephony, etc shall be covered by a maintenance, support or Service Level Agreement. All equipment shall be serviced at least once every 6 months.
iv. Users who require external support shall inform the ICT Department of such a need so that the ICT department coordinates such an effort with the service provider.
v. Users shall not sign service job cards or completion reports or the equivalent for maintenance works from external providers, unless there is dual signature by Staff of ICT Department or prior authorisation has been granted by Head ICT UMU.
vi. The ICT department shall maintain a log of all service and maintenance requests.

5.15 ICT User Awareness and Commitment Policy

Policy Statements

i. All UMU Staff Upon hire and annually thereafter, review ICT Acceptable Use Policy, Information Security and any supplemental institution acceptable use policies, if applicable.
ii. All UMU Staff every fiscal year shall complete information security awareness training that shall provide information security best practices and the individual's role in protecting the university's systems and data. All newly hired employees shall complete information security awareness training within 30 days of their initial hire date.
iii. All UMU Students shall receive notification of Information Security and ICT Acceptable Use Policies.
iv. All UMU Students shall be provided access to information security awareness training that includes information security best practices and their role in protecting the university's systems and data.
v. The ICT department shall make available to all UMU campuses system wide information security awareness training which promotes information security as an integral part of day-to-day activities.
vi. Faculties and Departments shall be responsible for ensuring that employees have access to, and have completed, information security training each fiscal year. Institutions may take appropriate action, including but not limited to the removal of access to UMU System information assets for those who have not completed training requirements.
vii. The ICT Department shall foster additional broad-based information security awareness activities as they deem necessary through methods such as:
    a. Websites
    b. Email
    c. Social media
    d. In-person or online training sessions
    e. Conferences or events
    f. New staff or student orientations
    g. Social engineering campaigns

5.16 Information Security Policy

Policy Objectives

i. Provide a framework for establishing suitable levels of information security for all UMU information systems (including but not limited to all Cloud environments commissioned or run by UMU, computers, storage, mobile

devices, networking equipment, software and data) and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems.

ii. Make certain that users are aware of and comply with all current and relevant Ugandan legislation.

iii. Provide the principles by which a safe and secure information systems working environment can be established for staff, students and any other authorised users.

iv. Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle.

v. Protect UMU from liability or damage arising out of misuse of its ICT facilities.

vi. Maintain research data and other confidential information provided by suppliers at a level of security commensurate with its classification, including upholding any legal and contractual requirements around information security.

vii. Respond to changes in the context of the organisation as appropriate, initiating a cycle of continuous improvement.

Policy Statements

i. The University manages and produces information that is private, confidential or sensitive in nature, together with information that is regarded as being readily available for general sharing. The University recognises that it is imperative that all information is protected from compromise of confidentiality, integrity and availability.

ii. Information assets are identified, classified and protected in accordance with the Data Classification Policy. Any security controls which are implemented must be proportionate to the defined classification. Key information assets are governed by an appointed Data Steward in accordance with the key responsibilities defined in Data Classification Policy.

iii. University Units and community members shall ensure that their electronic devices, including personally owned devices used for University business, and other resources which store, transmit, or process University information, or can impact the security of the data, meet the information security processes and standards of this policy, and all pertinent laws, regulations, or contractual obligations. Examples of standards include controls related to data storage, access, change management.

iv. Where a third-party provider is utilised for any services which involves contact with university information, an information security risk assessment is carried

out to ensure they comply with the appropriate University's Information Security Policy and Standards.

v. Back-up and disaster recovery plans, processes and technology, are in place in accordance with the Data Storage and Backup Standard to mitigate risk of loss or destruction of information and/or services and to ensure that processes are in place to maintain availability of data and services.

vi. Authorized individuals (See Data Classification Policy) shall be provided access to data they need to carry out work responsibilities.

   a. Data custodians (See Data Classification Policy) shall limit access to university data classified as private data to those individuals whose work responsibilities require it.
   b. Employees and departments shall follow the appropriate approval processes to request access to non-public information and request removal of access when no longer needed.
   c. Individuals authorized by their job responsibilities to share University data with internal audiences shall follow the procedures related to sharing University data, including instructions on aggregating data where appropriate.

vii. Information shall be protected against unauthorized access and processing in accordance with its classification level.

viii. Breaches of this policy must be reported

ix. Information security provision and the policies that guide it shall be regularly reviewed, including through the use of annual internal audits and penetration testing.

x. Legal and Regulatory Obligations. Uganda Martyrs University has a responsibility to abide by and adhere to all current Ugandan and East African legislation as well as a variety of regulatory and contractual requirements.

xi. Suppliers: All UMU's suppliers shall abide by UMU's Information Security Policy, or otherwise be able to demonstrate corporate security policies providing equivalent assurance. This includes:

   - when accessing or processing UMU assets, whether on site or remotely
   - when subcontracting to other suppliers.

xii. Cloud Providers: Under the DPPA, a breach of personal data can lead to a fine of up to two hundred and forty-five currency points or ten years imprisonment. Where UMU uses Cloud services, UMU retains responsibility as the data controller for any data it puts into the service, and can consequently be fined for any data breach, even if this is the fault of the Cloud service provider. UMU will

also bear the responsibility for contacting the National Information Technology Authority's Office concerning the breach, as well as any affected individual. It will also be exposed to any lawsuits for damages as a result of the breach. It is extremely important, as a consequence, that UMU is able to judge the appropriateness of a Cloud service provider's information security provision.

xiii. Any security breach of UMU's information systems could lead to the possible loss of confidentiality, integrity and availability of personal or other confidential data stored on these information systems. The loss or breach of confidentiality of personal data is an infringement of the Data Protection and Privacy Act 2019, contravenes UMU's Data Protection Policy, and may result in criminal or civil action against UMU.

5.17 Password Policy

Policy Objectives

i. Establish a secure environment for all UMU users and their data as they carry out core business processes.

ii. Improve the successful delivery of university communications to all faculty, staff and students, and

iii. Reduce the risk of university data classified as Legally Restricted or Confidential going through email systems that are not managed by the University.

Policy Statements

iv. All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed on a quarterly basis.

v. All production system-level passwords must be part of the Information Security administered global password management database.

vi. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed once every six months.

vii. User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.

viii. Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

ix. All user-level and system-level passwords must conform to the guidelines described below.

x. General Password Construction Guidelines

a. Strong passwords contain at least three of the five following character classes:

a.i. Lower case characters

a.ii. Upper case characters

a.iii. Numbers

a.iv. Punctuation

a.v. "Special" characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc)

b. Contain at least eight alphanumeric characters.

c. Weak passwords have the following characteristics:

c.i. The password contains less than fifteen characters

c.ii. The password is a word found in a dictionary (English or foreign)

c.iii. The password is a common usage word e.g. family names, 1234.

5.18 Network Configuration

Policy Objective

UMU Network shall appropriately be configured by the authorized personnel to ensure quality of service and business continuity

Policy Statements

ICT Department shall:

i. Be responsible for the UMU network infrastructure configuration; it will continue to manage further developments and enhancements to this infrastructure.

ii. Operate and maintain a reliable network with appropriate redundancies to meet quality of service goals.

iii. maintain a list of systems connected to the UMU network.

iv. Be responsible for Installing or authorizing a contractor to install all cabling and network hardware. All new or upgraded cabling shall conform to set standards for cabling to extend consistency with UMU's mission.

v. Be responsible for approving the specifications used to configure all network equipment connected to the UMU network.

vi. Authorize changes to the configuration of active network management devices guided by the Change Management and Configurations Standards.
vii. Be responsible for ensuring UMU Firewalls are installed and configured based on the Network Firewall Standard.
viii. Ensure that Users do not extend or re-transmit network services in any way. Network aggregation devices (i.e. router, switch, hub, wireless access point) shall not be connected to the UMU network without ICT approval.
ix. Ensure that Users are not permitted to alter network hardware in any way.

5.19 Systems Acquisition Policy

Policy Objective

1. This policy shall provide a framework that guides the university on how to appropriately acquire systems that will support the university's core business functions.
2. The policy categorizes and defines the types of systems that the University can acquire

Policy Statements

The Policy shall categorize the different types of systems that the University seeks to acquire to maximize effectiveness in the use of resources designated for information systems. Specifically, the policy distinguishes between enterprise systems, enterprise support systems, departmental unit support systems, and infrastructure systems. Adherence to this policy is required to receive acquisition authority and to get necessary signatures on contracts.

i. **Enterprise systems:** enterprise systems are those which manage the data for core business functions of the University, which require integration or which have significant integration potential with other systems and which must be managed and maintained effectively for the University to thrive. Examples of these systems are Student Management Systems, E-learning systems, alumni systems, the University email collaboration system, customer relationship management systems, Enterprise systems may be hosted by UMU or they may be hosted externally (cloud-based).

ii. Acquisition and replacement of these systems shall require approval from the ICT Steering Committee. In addition, the Office of ICT shall be involved at all levels of selection of these systems, from problem definition through request for

proposal, vendor review, vendor selection, contract negotiation, change management, implementation, and any subsequent stages. UMU hosted enterprise systems shall be hosted by the ICT Department in the University Data Center and shall be incorporated into disaster recovery and data backup systems. The ICT Department shall manage the exchange of data between UMU-hosted enterprise systems and any cloud-based enterprise system, in collaboration with functional user offices. Change management for these systems will be controlled by the collaborative ICT Steering Committee. These systems are subject to the University's information security policies and as implemented by the ICT Advisory Committee.

iii. **Unit support systems:** unit support systems are those that principally support one department, unit, or one function and which require minimal integration, usually only one-way, with enterprise systems or enterprise support systems. Examples include SPSS statistical software. Acquisition and replacement of these systems require collaboration among offices that use the systems. The ICT Department should be involved at the stage no later than product review and contract approval.

iv. **Infrastructure systems**: infrastructure systems are those platforms largely managed by the ICT Department in collaboration with appropriate technical staff in other units. These systems support ICT operations and ensure stability and security, but are not directly involved in delivering services to faculty, staff, students, alumni, donors, or other stakeholders. Examples include MySQL or Oracle database systems, data backup systems, IP network and firewall systems, voice-over-internet systems, security monitoring systems, job scheduling systems, address verification systems, and anti-virus protection systems.

v. Acquisition and replacement of these systems require collaboration among the technical staff that use the systems across campus. The Office of Information Technology will manage the stages of problem definition, proposal solicitation, product review, product selection, contract negotiation, implementation, and any subsequent stages. Change management for these systems will be controlled by the collaborative ICT Steering Committee. These systems are subject to the University's information security policies, as set and implemented by the ICT Steering Committee.

5.20 BYOD (Bring Your Own Device) Policy

Policy Statements

As an UMU user, if you use your own device for university work, it shall be deemed important to ensure that the information on the device is appropriately protected. All information that is classified 'restricted' or 'confidential' shall be treated with utmost care even when used on personal devices. Below are the guidelines for using your own device:

i. Set and use a passcode (e.g. pin number or password) to access your device. Always use a strong passcode/password as guided by the Password policy. Do not share the passcode with anyone.
ii. Set your device to lock automatically when the device is inactive for more than a few minutes.
iii. Take appropriate physical security measures. Do not leave your device unattended.
iv. Keep your software up to date.
v. Make arrangements to back up your data.
vi. Keep master copies of work data on a University managed storage service.
vii. If other members of your household use your device, ensure they cannot access University information, for example, with an additional account passcode. (Our preference is for you not to share the device with others.)
viii. Organise and regularly review the information on your device. Delete copies from your device when no longer needed.
ix. When you stop using your device (for example because you have replaced it) and when you leave the University's employment, securely delete all (non-published) University information from your device.
x. Encrypt the device (to prevent access even if someone extracts the storage chips or disks and houses them in another device).
xi. Report any data breaches.
xii. Configure your device to maximise its security. For example, each new technology brings new enhanced security features. Take time to study and discover how to use these and decide which of them are relevant to you. Seek help from your ICT support team if necessary.
xiii. Whenever possible, use remote access facilities to access information on university systems. Log out and disconnect at the end of each session.
xiv. Configure your device (mobile phone, smartphone and tablet) to enable you to remote-wipe it should it become lost. If your device is second hand, restore to factory settings before using it for the first time. Only download applications ('apps') or other software from reputable sources.

xv. Laptops, computers and more sophisticated tablet devices Use anti-virus software and keep it up to date

xvi. Using wireless networks outside the University Control your device's connections by disabling automatic connection to open unsecured Wi-Fi networks and make risk-conscious decisions before connecting. Disable services such as Bluetooth and wireless if you are not using them.

xvii. The loss, theft or misuse of a BYOD is personally distressing. If you use sensitive data, it can also have serious consequences for others, for example staff and students about whom information is held. In addition, there may be significant legal, financial and reputational consequences for the University, including fines as stipulated in the Data Protection and Privacy Act 2019. You may also carry personal responsibility, which, in serious cases could result in disciplinary action with the University.

5.21 ICT Physical Infrastructure Security Policy

Policy Objective

To prevent unauthorised access or damage to IT services. To prevent the loss of, damage to, or compromise to information assets, and interruption to the business activities of the University.

Policy Statements

i. All computer equipment that provides access to university information should be kept secure by physical means or by using good practice (this is especially important for users of mobile devices).

ii. File servers and equipment that store or process key information or high availability data shall be located in physically secured areas.

iii. Entry to secured areas shall be restricted to authorised users

iv. Access rights shall be revoked immediately for staff who leave the employment of the University

v. Other visitors shall be granted access for specific and authorised purposes only, and shall be supervised

vi. A log shall be maintained of all access to restricted areas, via the signing out of access keys.

vii. Cables between buildings should be underground wherever possible. Ducts and entry points into buildings should be secure and inspected annually for signs of damage or interference. A log of these inspections shall be retained by Network Administrator

viii. Wherever possible, cabling within buildings should be installed in ceiling voids and secure ducts.

ix. Wherever possible, wireless access points should be installed at a high level to make them less exposed and more secure from theft or tampering.

x. All communications equipment shall be kept secure, either in locked rooms or in racks and cabinets with locks. Keys to communications rooms, racks and cabinets shall be held securely by technical specialists and the University Security Service so that they are not available to individuals who are unauthorised to access network devices.

xi. Data centres shall be protected by appropriate air conditioning.

xii. Temperatures in data centres shall be monitored by ICT Staff, and undue variances reported immediately to the University's Estates Department.

xiii. Equipment shall be protected from power failures or electrical anomalies.

xiv. Data centres shall be protected by suitable local stand-by power supplies (generator or uninterruptible power supply).

xv. Wiring cabinets, and the rooms in which they are located, should be inspected annually to assess security risks and hazards arising from environmental conditions. A log of these inspections shall be retained by the Head of Networks and Infrastructure.

xvi. Equipment shall be maintained in accordance with manufacturers' recommendations, to ensure its availability and integrity. All faults (or suspected faults) shall be logged in the current Incident Management System and all changes shall be logged in the current Change Management System. All regular maintenance checks such as PAT testing shall also be recorded.

xvii. An inventory shall be maintained of file servers and communications equipment and recorded in the current Asset Management System, which shall be regularly checked to ensure that the University's information assets are accounted for.

xviii. All items of equipment containing storage media shall have any software or sensitive data irretrievably removed before disposal.

5.22 Network Access Policy

Policy Objective

The objective of this policy is to ensure that the university network is used to achieve the university's strategic goals while maintaining Quality of Service for all users.

Policy Statements

i. The ICT Department is responsible to administer this policy, and to make referrals to appropriate administrative offices for disciplinary action. Any exception to the policy must be approved in writing by the Information Technology Services unit.

ii. The University reserves the right to regulate any activity that occurs on the campus network or on any other computer-based system owned by the University. This includes, but is not limited to, the following implications:
    a. Anyone who uses the campus computing environment must have appropriate status (e.g. staff, faculty and current students) and must be properly authorized when required.
    b. Anyone not adhering to University policy should expect any or all of the following disciplinary actions:
        i. Restriction or suspension of access privileges.
        ii. Referral to the appropriate disciplinary body of the University.
        iii. Referral to the appropriate local, state or federal authority for legal prosecution.

iii. Material (software, hardware or data) that is found to be in violation of this policy can be banned, confiscated, or otherwise eliminated from the University computing environment.

iv. The University will be as proactive as possible to ensure compliance with this policy, including surveillance commensurate with appropriate maintenance of the right to privacy.

v. Users must not engage in activity outside the limits of access that have been authorized for them. This includes but is not limited to:
    a. Performing an act that negatively impacts the operation of computers, peripherals or networks, or that impedes the ability of someone else to do his/her work. Examples include but are not limited to:

b. Tampering with any transmission medium or hardware device, or connecting any unauthorized device (such as a router, switch, hub, wireless access point, etc.) or computer to the University network.
c. Propagating a software virus or worm.
d. Damaging or destroying data owned by the University or someone else.
e. Modifying any disk or software directory provided by the University for any type of special use.
f. Performing an act that places an unnecessary load on a shared computer or the University network.
g. Illegal file sharing.

vi. Attempting to circumvent protection schemes for access to data or systems, or otherwise uncover security loopholes.

vii. Gaining or granting unauthorized access to computers, devices, software or data. This includes, but is not limited to:
a. Admitting someone into a locked facility, or unlocking any facility that is normally locked, without permission.
b. Revealing a password to any account, including one's own personal account, without permission.
c. Permitting the use of any account, including one's own personal account, in a way that allows unauthorized access to resources.

viii. Using the University's facilities to broadcast unauthorized personal messages to large segments of the user community. Examples include but are not limited to:
a. Advertising campaigns for personal financial gain or political purposes.
b. Pranks and chain messages.
c. Announcements not approved for dissemination by this method.

ix. Users must abide by all applicable laws or government regulations, and operate within the limits articulated by the University for ethical and moral behaviour. Examples include but are not limited to:
a. Using any material in violation of any software licensing agreement or copyright law.
b. Using software or data that infringes on the rights of others. Examples include the production or propagation of material that is abusive, profane or sexually, racially or religiously offensive; or material that may injure or harass someone else, or lead to a lawsuit or criminal charges.

x. Using University equipment or network infrastructure to access off-campus resources (including materials on the internet) in a manner that is in violation of the ethical or moral standards of the University.

xi. Monitoring someone else's data communications, or otherwise reading, copying, changing or deleting files or software without proper permission of the owner.

xii. Using University facilities for personal gain, or for the benefit of an organization other than the college, without permission.

xiii. Users must abide by all other applicable University policies. Examples include but are not limited to:

   a. The software piracy policy.
   b. Usage restrictions, physical access regulations, and behavioural expectations established for each location containing equipment designated for public use.
   c. Usage restrictions for network connections in residence hall rooms. Example: Setting up any server-based host system for commercial use. Setting up any FTP servers for copyrighted music material, games and application software. (ex. MP3's). Setting up any game servers without proper authorization and for outside domain access. Registering a "personal" domain using the University's addressing scheme. Tampering with the Residence Hall Network. Extending access to others by tampering with the Residence Hall Network (utilizing wireless access points, routers, switches, hubs, etc.). Using the Residence Hall Network to commit data access security violations.

xiv. The ICT officers will collect the following information from the network:

   a. Logs detailing P2P traffic and usage on the University network will be collected.
   b. Logs will contain IP addresses involved in data transfer, direction of transfer (if retrievable), metadata of file (if retrievable), time, protocol used, and amount of data transferred.
   c. Logs will not contain any personal identifying information.
   d. Logs will be kept for one year.

xv. Information collected will be used for the following activities:

   a. Logs will be subject to periodic review for enforcement of this policy.
   b. Information collected may be used in aggregate format for reporting purposes.
   c. Individual usage will not be actively or routinely monitored.
   d. Logs may be used to investigate complaints or suspicious traffic patterns.
   e. Individual campus, faculty, departments, functional or administrative areas, and entities of the University may request information about P2P usage pertinent to that area. This request may only be made by the dean,

department head, manager, or other leadership of the area requesting information.

f. The University will not release any information collected by the appliance to any entity external to the University unless compelled or obligated by law or court order, subpoena, warrant, or writing.

5.23 ICT System Access Control

Policy Objective

The objective of the Access Control Policy is to communicate the need for access control, establish specific requirements for protecting against unauthorised access and create an ICT infrastructure that will foster data sharing without sacrificing security ICT Infrastructure resources.

Policy Statements

UMU shall provide:

i. ICT Services, Facilities and Infrastructure in support of teaching, learning, research and operational activities.

ii. either public services or private services, to Authorised Users only. Public services include, but not limited to the University's publicly available website and the information contained on it and services offered by the University Library.

iii. All other ICT services for use to Authorised Users only. Authorised Users shall only be eligible to hold an active account while their relationship with the University is current. At the cessation of their relationship with the University, they shall no longer be considered Authorised Users and their Access shall be revoked.

iv. Facilities and infrastructure, to persons having any of the following relationships with the University and automatically afforded Authorised User status:
   a. a currently employed officer or employee of the University
   b. a currently-enrolled student of the University.

v. In addition, any person falling under the following categories shall apply for non-University Member status and receive authorisation from the Head ICT, to use the University's ICT Services, Facilities and Infrastructure and become recognised as an Authorised User:
   a. a contractor undertaking work for the University under the provisions of a legal contract

b. a member of a collaborative venture in which the University is a partner
c. a visiting lecturer, student or other associate/consultant who is undertaking similar activities in a recognised University, at the discretion of the Head ICT.

vi. Account creation shall occur when a person becomes an Authorised User. This process indicates a person has a current relationship with UMU. Account creation will only occur when a person has been registered:
   a. as a current student, through enrolment
   b. as a current staff member, through Human Resources processes or
   c. has completed the Request for Access to University Services process and registered as a non-University member.

vii. Account deactivation shall occur upon termination of an Authorised User's relationship with UMU. This may occur via, but is not limited to, the following events:
   a. Student: on graduation from a course of study
   b. failure to re-enrol during a course of study
   c. expulsion from the University.
   d. Staff: on termination of employment
   e. Resignation
   f. on retirement.
   g. Associate: on conclusion of contract or consultant services
   h. conclusion of collaborative research project
   i. termination of associate staff/study arrangements.

viii. Assignment of account privileges shall based on the principle of least privilege. An Authorised User will be provided with access sufficient for their role at UMU, and will not be afforded greater levels of access.

ix. If an Authorised User's role within the University changes, their access rights shall change to reflect the requirements of their new role.

x. Periodic auditing of accounts shall be performed by the University to identify and revoke non-active, unused or non-authorised accounts; or to perform the reallocation or revocation of privileges.

xi. Administration of ICT Services, Facilities and Infrastructure shall only be carried out by:
   a. ICT Officers authorised by a Senior Officer of the University, or by a senior ICT Officer in a Campus or Unit
   b. A person who holds responsibility, via their current position description, for the maintenance and management of data, or an ICT Service.

xii. Administrators shall be the current members of the University or approved third party support persons. Administration rights, access and group membership held by an individual shall be immediately revoked upon cessation or suspension of employment with the University, change in role, or termination of contractual support arrangements with the University.

xiii. Administrator Account details shall be made secure as per the requirements of the ICT Systems Administrative Password Procedure.

xiv. Administrators of ICT Services, Facilities and Infrastructure shall not hold rights greater than those required of their role.

xv. Separation of duties and responsibilities shall be used to ensure no one person has the ability to circumvent normal auditing processes.

xvi. Minimum implementation to separate the roles of Systems Administrator and Application Manager for all systems holding confidential or financial information, or any system identified as a corporate system.

xvii. The use of shared, guest, anonymous and other such generic user accounts shall be avoided where possible. If guest or anonymous accounts must be used to UMU ICT Services and Facilities shall be supported by a process that identifies the user of the account, such as a record of account allocation.

xviii. Generic accounts shall have the minimum rights and privileges required to perform their role, and shall not be used to access any corporate systems or stores of confidential information.

xix. Generic access to information stored in databases shall be allowed only for non-interactive tasks. A non-interactive task is one that is scheduled to run automatically or one that is triggered by a series of events. A User shall not directly initiate the task, nor directly receive information. This includes automatic downloads and other linkages for data transfer.

xx. Information related to the use of UMU ICT Services and Facilities shall be collected and consulted to ensure compliance with University Policies, Procedures and Guidelines; and relevant National Legislation. This information shall be accessed for purposes of investigating allegations of misuse.

xxi. Information shall be provided to law enforcement agencies where necessary to investigate or report suspected unlawful activity, as per UMU Policy.

xxii. Breach of this Policy shall result in disciplinary action.

xxiii. Staff, students and associates learning of any violation of this Policy shall be obligated to bring this matter to the attention of an appropriate staff member within the University without delay.

5.24 eLearning Policy

Policy Objectives

The eLearning Policy shall:

i. facilitate and support eLearning through the use of information and communication technologies by guiding and coordinating all the stakeholders within and outside Uganda Martyrs University
ii. provide protocols and guidelines for all eLearning courses and degree/certificate programs offered by Uganda Martyrs University. The policy encourages and enables schools and faculties to develop quality hybrid and fully online courses.

Policy Statements

1. **eLearning** comprises all forms of electronically supported learning and teaching. eLearning applications and processes include Web-based learning, computer-based learning, virtual education opportunities and digital collaboration. Content is delivered via the Internet, intranet/extranet, audio or video tape, satellite TV, and other electronic media. It can be self-paced or instructor-led and includes media in the form of text, image, animation, streaming video and audio.

1. **Fully online courses** meet online for 100% of the class meetings required per student credit hour, including class meetings for which exams, tests and quizzes are administered.

2. **Blended courses** contain a mixture of face-to-face classes and sessions conducted online, with no more than 60% of class meetings held in assigned on-campus classroom locations, 40% of class sessions are held online.

Guiding Principles

Principle 1: Match to the Curriculum

UMU ensures that pedagogy is matched and aligned to the appropriate curriculum as approved by Uganda National Council for Higher Education through, clear objectives, relevance of content covered, appropriateness of student activities and nature of the assessment

Principle 2: Inclusion

UMU ensures that the mode of delivery supports inclusive practice in terms of different types and range of achievement; physical disabilities that can be particularly supported

by eLearning; different social and ethnic groups; and gender. eLearning solutions shall be designed to place the student in charge of their own education. The range of communications approaches adopted should provide support to practices of a wide variety of social, ethnic and gender preferences.

Principle 3: Learner Engagement

UMU ensures the mode of instruction on the e-platforms engages and motivates learners. This engagement should be evident in the ethos of being both educational and motivating. The user interface of the eLearning platform shall be friendly and accessible, avoiding confusion or discouragement of students and teachers. Students' progress reports and task lists should be provided to students to keep them up-to-date.

Principle 4: Innovative Approaches

eLearning should be fit for purpose. It should be evident why learning technologies are being used, rather than a non-technological approach which achieves the same end as effectively. UMU provides technology and tools that make it easy to create a connected and personalised environment that challenges students to practice problem-solving, to work together and to use creativity to construct, share, and present their ideas, thinking and learning

Principle 5: Effective Learning

UMU ensures that its eLearning provision can meet the needs of a full range of flexible and independent learning experiences. This includes on and off campus learners in local, regional, national and international settings and cover both blended and full eLearning courses ranging from full awards to informal and individual learning

Principle 6: Coherence, Consistency & Transparency

UMU ensures that teaching is internally coherent and consistent in the way the objectives, content, student activity and assessment match to each other. Teaching is open and accessible in its design.

Principle 7: Interoperability of eLearning Environments

UMU ensures that all systems, both manual and electronic, used in the eLearning context interoperate in the most effective way to provide learners with an effective and

increasingly individualized learning environment encompassing all aspects of their experience as a student of the University, as part of a holistic Managed Environment for Learners

Policy Statements

i. eLearning Infrastructure

a. ICT Infrastructure

i. eLearning requires a robust, scalable and available network infrastructure. It is necessary therefore for management to invest in high quality network infrastructure and internet bandwidth for seamless learning.

ii. End-users including staff and students need mobile devices (including laptops and tablets) to access eLearning materials on the Virtual Learning Environment (VLE) - Moodle.

b. Management and Administration of eLearning Infrastructure

i. It is the responsibility of the ICT department to design, implement and maintain the eLearning network infrastructure. Access to the eLearning VLE, Moodle shall be governed by the Network Access Policy guidelines and the network will be protected by the required Firewall configurations according to the Network Firewall Standards.

ii. Data in the VLE will be stored for a period not exceeding 2 years.

iii. The ICT Department has responsibility of meeting the guidelines below for the VLE systems which they maintain, namely Moodle:

a. students should be confident that any programme or element offered for study has had the reliability of its delivery system tested, and that contingency plans would come into operation in the event of the failure of the designed modes of delivery;

b. students should be confident that the delivery system of the programme or element of study delivered through eLearning methods is fit for its purpose, and has an appropriate availability and life expectancy;

c. students should be confident that the delivery of any study materials direct to students remotely through, for example, eLearning methods or correspondence, is secure and reliable, and that there is a means of confirming its safe receipt

d. students should be confident that their assessed work is properly attributed to them, particularly in cases where the assessment is conducted through remote methods that might be vulnerable to interception or other interference;
e. students should be confident that any mechanisms, such as web-based methods or correspondence, for the transfer of their work directly to assessors, are secure and reliable, and that there is a means of proving or confirming the safe receipt of their work.

iv. Faculties and schools that use delivery systems which are not supported by ICT would be expected to assume responsibility for ensuring that:

1. All the above guidelines apply
2. Data stored on the platform conforms to the Data Classification and Information Security Policy

c. Support Personnel

i. Designated personnel must be recruited and or appointed by Management to provide technical support to users of the eLearning VLE. These include:
   1. eLearning Administrator: This individual is part of the ICT Team and is responsible for the Administration of the VLE, Moodle.
   2. ICT Helpdesk: The IT Helpdesk Officers provide support for hardware and software issues related to access and use of Moodle. These can be contacted on phone, email or telegram
   3. Video and Content Editor: This is a professional individual that provides support to the Academic staff to develop online videos for teaching and learning purposes.

ii. eLearning Policy Implementation.

a. The ICT department will oversee the implementation of eLearning and will report to the ICT Steering Committee. The Steering Committee will oversee the development of an evaluation plan to assess the impact of the policy.

b. eLearning material: All teaching and learning material produced at the Uganda Martyrs University belongs to the University. This policy

mandates the placement of online course materials produced at UMU on the official VLE, Moodle.

c. Intellectual Property Right: A Faculty, School or Institute has the same control and ownership of the substantive and intellectual content of their online course materials as stipulated in the Intellectual Property policy

d. All students who register to study at UMU will be required to have a laptop, tab or tablet for use during study as a must. UMU will allow students to join its scheme which allows them to acquire a connected laptop at very minimal prices.

iii. Faculties, Schools and Institutes should:

a. ensure that students have access to information that sets out the respective responsibilities of the school / Faculty and University for the delivery of the programme, module, course unit or element of study;

b. ensure that students have access to module descriptors, to show the intended learning outcomes and teaching, learning and assessment methods of the module(s) / course unit (s)

c. ensure that students have access to a clear schedule for the delivery of their study materials and for assessment of their work.

d. ensure that students can be confident that study materials, whether delivered through traditional methods or through web-based or other distribution channels, meet the expectations of the University with due respect to the quality of teaching and learning-support material for a programme or element of study leading to one of its awards;

e. ensure that students can be confident that staff who provide support to learners on these programmes have appropriate skills, and receive appropriate training and development;

f. ensure that students can be confident that the online programme, content and delivery is subject to Quality Assurance and the University Periodic Review process.

g. ensure that students have access to a schedule for any learner support available to them through timetabled activities, for example tutorial sessions or web-based conferences;

h. ensure that students have access to clear and up-to-date information about the learning support available to them locally and remotely for their programme or elements of study;

i. ensure that prospective students receive a clear and realistic explanation of the expectations placed upon them for study of the programme or elements of study, and for the nature and extent of autonomous, collaborative and supported aspects of learning.

j. ensure students have access to documents that set out their own responsibilities as learners, and the commitments of the University, faculty, school and institute for the support of a programme or element of study.

k. ensure students have where appropriate, regular opportunities for inter-learner discussions about the programme, both to facilitate collaborative learning and to provide a basis for facilitating their participation in the quality assurance of the programme;

l. ensure students have appropriate opportunities to give formal feedback on their experience of the programme and the Faculty, School or Institute should provide feedback to students on their concerns.

m. ensure students have access to information on the ways in which their achievements will be judged, and the relative weighting of units, modules or elements of the programme in respect of overall assessment.

n. ensure students have access to timely formative assessment on their academic performance to provide a basis for individual constructive feedback and guidance, and to illustrate the awarding institution's expectations for summative assessment.

o. ensure that students can be confident that those with responsibility for assessment are capable of confirming that a student's assessed work is the original work of that student only, particularly in cases where the assessment is conducted through remote methods.

iv. Students and Prospective students should:

a. note that only registered UMU students with an Official UMU email address will have access to the VLE, Moodle and any online course.

b. note that only the ICT Department through your Faculty, School or

Institute will create your Moodle access account.

c. note that all students accessing Moodle online courses must adhere to the rules, principles and guidelines of the Acceptable Use Policy and Information Security Policy. Students must also note that breach of any of these policies will lead to disciplinary action.

5.25 Email Use Policy

Policy Objective

1. Improve the successful delivery of University communications to all faculty, staff and students.
2. Reduce the risk of University data classified as Legally Restricted or Confidential going through email systems that are not managed by the University.

Policy Statements

i. UMU Staff
   a. Email services are primarily intended to allow faculty and staff to conduct University business. Personal use of email is allowed, provided that personal use (a) does not materially interfere with performance of work responsibilities, (b) does not interfere with the performance of the University networks and (c) is otherwise in compliance with this and other University policies especially the Acceptable Use Policy.
   b. Staff Email users must not use email to communicate data classified as University legally restricted or confidential information without appropriate security layers such as email encryption (Please refer to the Information Security and Data Classification Policies).
   c. Email services are provided only while a user is employed by the University and once a user's electronic services are terminated, as specified in the ICT System Access Control, employees may no longer access the contents of their mailboxes, nor should they export their mailbox to a personal account before departure.

ii. Students
   a. The University currently provides email services to all students. Student use of email is subject to this Policy, the University's Information Security and Data Classification Policies and the University's Acceptable Use Policy.
   b. 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.

c. Email addresses for students that have graduated will be retained for a period not exceeding 2 years, unless authorized by the Academic Registrar.

iii. Alumni and others

a. Individuals with special relationships with UMU, such as alumni or official visitors, who are neither employed nor enrolled at UMU, are granted limited email privileges, including an email address, commensurate with the nature of their special relationship. UMU is free to discontinue these privileges at any time.

iv. Official Email Address

a. Students and University workforce members will be assigned an Official Email Address, which will include a mailbox assigned to the Google Apps for Education Service

b. The Official University Email Address is the address from which, and to which, University business-related Email is to be sent and received.

c. The Official Email Address will be used for all University Email correspondence lists, for populating lists for classes, and for the official online directory.

d. Official communications from University Offices, such as the VC's Office, Human Resources, Registrar, Finance, Security and others, will be directed to the Official Email Address.

e. Accordingly, users shall be presumed to have received all official University Email messages sent to their Official University Email Address.

f. If an individual has both a student and employee affiliation, the University may provision a separate email box for each affiliation.

v. Email Forwarding: Manually forwarding University Email that contains information classified as University Legally Restricted is only permissible for valid business purposes and appropriate security precautions such as email encryption must be taken.

vi. Confidentiality and Security: Although the University does not monitor Email content routinely, users must not assume that Email content will remain private and confidential. A user's expectation of privacy in emails is defined and limited by the University's Information Security Policy.

vii. The password associated with an Email account may be used to authenticate identity in other university online services. To safeguard your identity and your

privacy, do not share your account or give your password to anyone. See the Password Policy.

viii. Retention and Disposal: Users should avoid retaining large numbers of email (whether in the Inbox, Sent Items, Deleted Items or personal folders) for long periods of time.

6.0 Accounting Officer

The Deputy Vice Chancellor shall be the Accounting Officer.

7.0 Responsible University Officer

The Head ICT will be the Officer responsible for ensuring that the ICT policy is well implemented and adhered to by all parties.

8.0 Review Date

This policy was approved by the **101st University Council meeting** that sat on **8th February 2025**.

The ICT Policy shall be reviewed every 1 year.

Most Rev. Raphael p'Mony Wokorach, MCCJ
Chaiperson, UMU Council

Rev. Dr. Josef Buchana Kisoga
Secretary, UMU Council