TUMAINI UNIVERSITY MAKUMIRA

INFORMATION AND COMMUNICATION TECHNOLOGY POLICY

September 2020

Preface

The TUMA ICT Policy was formulated in 1997 and revised in 2016 and 2020 to guide development, management and proper utilization of ICT facilities. The Policy also fosters integration of application of ICT to the TUMA mission and Strategic Plan aiming at promoting quality teaching and learning, research, consultancy and services to the public nationally and internationally. The previous documents have helped TUMA to improve its infrastructure, systems, content, programmes and human resource. However, due to new developments in science and technology, TUMA has discovered areas of improvements and therefore incorporated these areas in this revised ICT Policy.

The current TUMA ICT Policy aims at achieving excellence in academic and administrative outputs through the development and use of ICT applications and services. This policy is divided into policy objectives; policy statements and procedures; ICT support systems, system Integrity, usage and availability; and the role of ICT Department. The policy emphasizes on providing and securing ICT infrastructure and services that integrate academic and administrative management of information. The policy also underlines guidelines and policies for ICT security, development of contents, and ethical utilization of ICT facilities, regular training for skills development, equipping of the university with e-learning, e-resources, and management of electronic and physical wastes.

This policy is a result of involvement of different stakeholders, especially TUMA ICT personnel forum mandated by the Senate to discuss different matters related to ICT issues for decision making. I also extend my gratitude to TUMA System Administrators, who have been involved in the production of the contents of this policy.

This policy is subject to change at any time depending on the developments in the ICT policy and requirements by stakeholders.

Rev. Prof.Dr. Joseph W. Parsalaw
Vice Chancellor - Tumaini University Makumira
June 2020

Table of Contents

List of Abbreviations and Acronyms

CCTV	Closed-circuit television
DICT	Department of Information and Communication Technology
DVCA	Deputy Vice Chancellor for Administration
DVCAA	Deputy Vice Chancellor for Academic Affairs
E-Learning	Electronic Learning
E-Library	Electronic Library
E-Resource	Electronic Resource
ICT	Information and Communications Technology
ICTC	Information and Communications Technology Committee
TUMA	Tumaini University Makumira
IT	Information Technology
VPN	Virtual Private Network

Definition of Terms

Business System Owner means the nominated custodian that has responsibility for the security of the data and application component of the ICT Asset and is also accountable for those aspects of the Information System. Business System Owners for each of the TUMA Information Systems are identified. Note: Systems Owner for each system must be identified and the list should be attached on the policy.

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

Cloud Computing is a model for enabling access to a shared pool of configurable computing resources such as storage, applications, and services that can be rapidly provided and released with minimal management effort or service provider interaction.

E-library is an electronic or online library where learners can have access to e-books, e-journals and other material.

E-Resources are information resources that users access electronically including, but not limited to electronic journals, electronic books and other Web-based documents.

E-waste describes discarded electrical or electronic devices that have become waste because they cannot be upgraded or repaired for re-use. E-waste includes computers and their accessories, mobile phones, television sets and other electrical equipment.

Information Classification means the categorization of an ICT Asset for the purpose of identifying the security controls required to protect that asset.(This should be developed).

Information and Communications Technology (ICT) Asset means all software; hardware and data used in the management of the related TUMA information resources. (Note: This may include non-ICT resources (e.g. Printed records).

Information Security Management System means a collection of artefacts that support the ICT Security Policy framework, consistent with the Queensland Government's Information Standard IS18 and the ISO/IEC 27001 standard.

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

Information Technology (IT) - Is "a fancy name for data processing", according to Newton, IT means all equipment, processes, procedures and systems used to provide and support information systems (both computerized and manual) within an organization and those reaching out to customers and suppliers. The term information and communications technology (ICT) was coined to reflect the seamless convergence of digital processing and telecommunications.

Internet is the world-wide collection of private and public router-based networks that are interconnected via gateways and exchange points, which all utilize the TCP/IP protocol.

IP address is a set of protocols developed to allow cooperating computers to share resources across a network.

Local Area Network (LAN) is a computer network that spans a relatively small area such as a single building or group of buildings.

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

Third Party TUMA Clients means contractors, consultants, adjunct appointments and other individuals who are not University staff or students but who require access to TUMA Information Systems.

.

1.0 POLICY RATIONALE AND OBJECTIVES

The TUMA ICT Policy was first formulated in 1997 and revised in 2016 to guide the identification, promotion and appropriate utilization of ICT resources and ensure that ICT applications are integrated into the planning and University strategic plan.

Information and Communication Technology (ICT) is fundamental in facilitating TUMA core functions i.e. teaching, research and Service. The importance of ICT in innovation for knowledge generation and technology transfer geared at enhancing national development as a component of Education for life has been embraced in the University strategic plan.

TUMA therefore, reaffirms its commitment to adopt and operationalize e- government standards; ensure availability of Internet bandwidth, improved ICT Infrastructure, ensure that best security measures are in place.

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

1.1 The General Objective

This Policy outlines commitment of the Tumaini University Makumira to effectively manage the Information and Communication Technology (ICT) assets and the obligations of the University community in protecting and guiding these resources into good use.

In compliance with organizational mandates and generally accepted best practices, TUMA provides for the security and privacy of the data stored on, redirected through, or processed by its technology resources.

Henceforth, the purpose of this Policy is to ensure TUMA users have access to best practices for the identification, protection and management of ICT resources available.

Throughout this security policy, the term “user” identifies full and part-time staff members, consultants, temporaries, interns, retirees, vendors and other users affiliated with third parties who access TUMA institution’s ICT resources due to their job responsibilities.

Management expects users to comply with this and other applicable policies, procedures, and laws.

1.2 Specific Objectives

- Provide cost effectively information and communication technology facilities, services and automation;
- Improve customer satisfaction;
- Identify priority areas for ICT development;
- Encouraging innovations in technology development, use of technology and general work flows;
- Help people to adapt to new circumstances and provide tools and models to respond rationally to challenges posed by ICT;
- Promoting information sharing, transparency and accountability and reduced bureaucracy in operations.
- Use technology as platform to meet TUMA strategic goals

1.3 Users Affected by the ICT Policy

This policy intends to protect both the employer and employee from misuse of files, applications, the Internet, email and other electronic interfaces. The extensive use of computers and other ICT equipment is highly encouraged and used in provision of services at TUMA for provision of services. With the rapid evolvement of the Internet and related systems there has been enough scope for misuse.

This Policy sets out guidelines on the use of ICT systems and the consequences for non-compliance.

The Policy applies to all the TUMA employees, contractors, consultants, agents, students and any other person who use or will be given access to email or files, software applications and the internet during the course of their employment or business dealings with the TUMA, whether such use takes place on the TUMA premises or elsewhere.

1.4 Principles of this Policy

This policy shall be guided by the following key principles:

1. Mainstreaming of ICT services in the University;
2. Seamless integration of ICT;
3. Inclusion, flexibility support to all stakeholders in the University and management system;
4. Adherence to best practices & policies;
5. Economies of scale and customer value propositions

2.0 POLICY STATEMENTS AND PROCEDURES

The policy statements are presented in six approaches, i.e., policy issues followed by the operational procedures under each policy statement.

2.1 ICT Security Governance and Management

Effective ICT Governance practices have an impact on how securities of information assets are achieved at the TUMA. This includes how risks are identified, managed; how resources are allocated to implement several security measures as well as TUMA management commitments towards achieving the notable goal of operating in a universally secured environment. Thus, the TUMA ICT Department shall:

- Ensure ICT security practices are implemented on discharging its core functions while maintaining visions and mission highlighted in the strategic objectives.
- Ensure ICT security measures are addressed in all ICT related projects.
- Allocate sufficient funds for effective ICT security and ensure capacity building on updated security issues to ICT staff.
- Ensure changes to the organization, business processes, information processing facilities and systems that affect ICT security shall be controlled.
- Ensure the entire community comply and abide by security measures, which will be put in place.
- Ensure a consistent and effective approach is applied to the management of risk and business continuation plan (BCP) implementation.

The Head of ICT Department shall:

- Allocate sufficient resources for effective ICT security controlling and management
- Ensure regular training to TUMA staff and students on ICT security matters.
- Ensure local and external training of ICT staff on security matters for effectiveness and efficient security technique implementation.
- Ensure the review and updates of Business Continuity Plan (BCP), Data Recovery Plan (DRP) and Risk Assessment (RA) are done on quarterly basis.

2.2 ICT Assets

Asset Management and Controlling involves activities for asset acquisition, storage, usage, maintenance and disposal. The assets include ICT hardware, software, data, system documentation, and storage media, supporting assets such as computer room, air conditioners and UPSs. Inappropriate use of ICT assets may expose the TUMA to risks including but not

limited to loss of these resources, malware attacks, compromising investment, compromise network systems and services and legal implications.

TUMA shall:

- Ensure that ICT assets are protected physically and logically for the entire lifecycle of the asset.
- Ensuring user entitlement of ICT assets is well documented and bonded in their tenures that means all terminated users can submit all ICT related resources given to them during tenure ship.
- Ensure that ICT assets are disposed securely when no longer required.
- Ensure that any lost ICT related resources are reported immediately to DVCA and accounted by finance as well.

The Head of ICT Department shall:

- Ensure that all ICT assets are labelled and classified according to the TUMA asset classification.
- Ensure that all ICT related equipment's are protected from power failures and other disruptions.
- Ensures that all items of equipment containing storage media are verified to ensure that all sensitive data and licensed software has been removed or securely destroyed.
- Ensure all servers shall be in a secure place with a limited access room(s) dedicated for such services (Server Room).
- Ensure that sensitive data or servers have a different geographical location and cloud storage.
- Ensure that periodic change of credentials to all systems in the given time frame or in event where suspicion of mishandling administrator's password or termination of an employee whose role gave access to such password.
- Ensures equipment is properly maintained to ensure its continued reliability, availability and integrity.
- Ensure that equipment, information or software shall not be taken off-site without prior written authorization and documentation for future reference.
- Ensure that every person holding ICT related assets is held responsible with information contained in the asset.
- Ensure data backup is regularly done and on time.
- Ensure no TUMA business information is disclosed unless authorized to do so.
- There shall be an inventory system in place for all TUMA assets including ICT.

2.3 Internet Services

The use of internet service is crucial part of daily operations at TUMA therefore it is essential users understand their role to play in creating efficient and cost-effective ways of communicating and obtaining information in safer environment. However, improper or inappropriate use of the Internet can have an adverse effect on the TUMA operational and can also have serious legal consequences. Therefore, TUMA shall: -

- Ensure cost recovery strategy for Internet and other ICT services and facilities as incorporated in the University Strategic Plan and other policies for sustainability purposes.
- Ensure all projects within TUMA community contribute to Internet and ICT service fees as a means to create sustainable robust services.
- Direct the ICT Department under the Head of ICT Department:
  (i) Ensures that all users provided with access to the Internet and network services have been authorized to use.
  (ii) Ensure Internet security control as stipulated in the TUMA ICT Security Policy.
  (iii)Ensure availability of all anticipated ICT internet services/systems at all workplace in the University;

The following uses of the Internet system are considered unacceptable:

a) Use of the TUMA's Internet system to access, review, upload, download, store, print, post, or distribute pornographic, obscene or sexually explicit material;
b) Use of the TUMA's Internet system for political campaigning;
c) Use of TUMA's Internet system to transmit or receive obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually explicit language;
d) Use of TUMA's Internet system to access, review, upload, download, store, print, post, or distribute materials that use language or images that are inappropriate to the work setting or disruptive to the work environment and will not post information or materials that could cause damage or danger of disruption;
e) The use of TUMA's Internet system to access, review, upload, download, store, print, post, or distribute materials that use language or images that advocate violence or discrimination toward other people or that may constitute harassment or discrimination
f) The use of the TUMA's system knowingly or recklessly post false or defamatory information about a person or organization, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks;
g) The use of TUMA's system to engage in any illegal act or violate any applicable laws of the country;

h) The use of the TUMA's system to gain unauthorized access to information resources or to access another person's materials, information or files without the implied or direct permission of that person;

i) The use of the TUMA's system to post private information about another person or to post personal contact information about themselves or other persons including, but not limited to, addresses, telephone numbers, work addresses, identification numbers, account numbers, access codes or passwords, and will not repost a message that was sent to the user privately without permission of the person who sent the message;

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

k) The use of the TUMA system to violate copyright laws, or usage licensing agreements, or otherwise to use another person's property without the person's prior approval or proper citation, including the downloading or exchanging of pirated software or copying software to or from any TUMA computers;

l) The use of the TUMA system for unauthorized commercial purposes or for financial gain unrelated to the official business of the TUMA. Users shall not also use the TUMA system to offer or provide goods or services or for product advertisement, other than for work purposes.

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

3.0 ICT SUPPORT

As part and plan to ensure TUMA users have sufficient knowledge and skills to utilize ICT resources in their environment. ICT support is therefore categorized into

3.1 Office Support

This category comprises both administrative, teaching and research for employees who have offices located at TUMA premises.

3.2 Offices, Classrooms and Conference rooms

This category includes users above and in addition to students as main users in the physical space and virtual environment as meeting and teaching platforms.

TUMA management shall:

- Promote use of office computing in all offices considering the availability of resources sharing will be required if situation prevails. This applies to lecturers, researchers, administrators, managers, as well as to secretarial and clerical workers.
- Enhance and streamline financial management processes and reporting through the implementation of an integrated financial information management system;
- Continue support in the E-learning initiatives to diversify teaching and learning practices to reach a wider community of potential scholars within and outside the country.
- Enhance and streamline education related administrative and managerial processes and to improve academic reporting through the implementation of an integrated academic records information management system that will reduce cost in paper works and stationeries;
- Provide for the growth of its ICT resources and their financial sustainability through adequate funding and appropriate operational mechanisms.
- Ensure sustainable management of the institution's ICT resources through creation of appropriate policy guidelines and regulations, advisory and operational organs that will cater for the broad interests of all users;

Head of ICT Department shall:

- Ensure that students and staff are trained on a continuing basis to equip them with the requisite skills to fully exploit the ICT potential in their different functions, in order to make the entire University fraternity "ICT – Compliant".
- Diversify support platforms to reach out to users in order to leverage the ratio of technical staff to clients through the use of telephone, online support system, emails, chats, knowledge materials (online and printed) and awareness training.
- Integrate ICT into various operations of the University through proper change management policy.

4.0 SYSTEM INTEGRITY, AVAILABILITY AND ACCESS CONTROL

Overall in charge of systems and computing facilities properties of TUMA are being left to the Head of ICT on machines assigned to users need to be in place and circulated to all Users to understand. Therefore, an information classification document will guide on how to answer what, who, how and where ICT information assets will be provided. Henceforth, users on ensuring system integrity: -

- Shall not be allowed to disconnect PCs or other ICT equipment from each other, from the main supply or from network connection points; doing so may corrupt data stored on the system or the current work of other users.
- Always the user shall contact ICT support staff if there is a need to move any piece of ICT equipment for any reason whatsoever.
- Ensure the report requests access to Head of ICT if any third party user requires access to the University network.

Head of ICT Department shall ensure:

- Infrastructure and supporting platforms are in place to allow availability of services according to the requirement of its establishment.
- Accessibility is limited in the basis of privileges therefore being granted or revoked the access compliance covered in the security document of TUMA ICT Security Policy

5.0 ICT SECURITY SYSTEMS AND BACKUP MANAGEMENT

5.1 ICT Security

There shall be separate TUMA ICT Security Policy. This document covers the following aspects of ICT:

- Networks and Internet security
- System security
- Users access Computer access Server room access Remote access Password policy
- Virus, Malware, spyware, Intrusion Detection protection

5.2 Security CCTV Cameras

There shall be security CCTV cameras where responsibility is placed in the Department of ICT. Therefore, Department of ICT shall: -

- Design, supervise installation and review operation of the CCTV cameras quarterly and on the need basis.
- Ensure access to CCTV D/N-VR is limited to users with clearance as specified in the Security policy.
- Design protocol to request review of CCTV footage by individual within or outside TUMA when required in the Security policy

5.3 Backup and Recovery Management

There shall be a Data recovery plan (DRP) and Business Continuity Plan (BCP)

- Back-up procedures, ensuring that both data and software are regularly and securely backed-up, are essential to protect against loss of that data and software.
- ICT team members shall ensure a daily incremental and a weekly backup to the backup servers, for the purpose of restoring a system in the event of a system failure. In any absence of ICT member(s) then, other ICT member(s) should take responsibility for backup. In the event of a disaster IT personnel shall work hand in hand to restore user files but does not guarantee retrieval. The responsibility for backing up user files remains with the user. However, ICT members should undertake all possible measures to ensure that backing up user files is accurately undertaken and proper operations of the baking up system are done.

6.0 E-MAIL AND INTERNET USAGE

- All official communication via emails within and outside TUMA will require use of TUMA official mail.
- Disclose the inadvertent access to an appropriate manager. This disclosure may serve as a defence against an allegation that the user has intentionally violated this policy.

6.1 Authorized Personal Use of emails and Internet

- Users are entitled to make reasonable personal use of email and Internet facilities outside normal working hours. Such use must be consistent with this policy.
- The TUMA reserves the right to discontinue this entitlement for all or some employees if it is of the views that the use of e-mail and Internet facilities as excessive or inappropriate;
- Users are reminded that any personal use of email cannot be considered private and may be subject to monitoring in accordance with this Policy. Users must make their own arrangements to save electronic or paper copies of their personal emails; the TUMA does not accept any responsibility for the safe storage of personal emails, which may be deleted at any time.

6.2 Unauthorized Use emails and Internet

The Computer's system and networks, and provision of email and Internet facilities, must not be used for the creation, transmission, downloading, browsing, viewing, reproduction or accessing of any image, material or other data of any kind which:

- Is illegal, obscene, pornographic, indecent, vulgar or threatening;
- Contains unacceptable content, including but not limited to, sexually explicit messages, images, cartoons, jokes, or unwelcome propositions, or any other content which is

designed to cause or likely to cause harassment or provocation of any other person or organization based on sex, sexual orientation, age, race, national origin, disability, religious or political belief;

- Is defamatory, slanderous or libellous;
- Deliberately introduces viruses into the email or internet systems of the TUMA or any other party or is designed to deliberately corrupt or destroy the data of other users;
- Conflicts with the TUMA strategic interests;
- Infringes or may infringe the intellectual property or other rights of TUMA or those of a third party;
- Is part of a chain letter, "junk mail" or contains unsolicited commercial or advertising material;
- Violates the privacy of other users;
- Is in breach of the duty of confidentiality which the TUMA owes to the Public and TUMA Staff;
- Disrupts the work of other users;
- Users shall not send emails, which make representations, contractual commitments, or any other form of statement concerning the TUMA unless they have specific authority from the TUMA to do so. Users must not register TUMA email addresses on Internet lists or websites inviting downloads, automated email or remote access (spams).

6.3 Confidentiality

- All TUMA information exchanged by the means of email is subject to confidentiality. No information gained through emails may be disseminated or passed to third parties for whom it was not intended by the originator of the email. If an email is misdirected and you receive an email, which was not intended for you, you must at once notify the originator with information about the circumstances in which you received it. In no circumstances may such an email be forwarded to another, except as part of an investigation into the causes of the misdirection.
- Emails to recipients external to the TUMA shall carry an automatic disclaimer to protect the interests of the originator and of the TUMA.
- Internal emails between two staff members of the TUMA shall not carry such a disclaimer. The proper use of internal emails is governed by this Policy; any improper use of information contained within an internal email shall be considered gross misconduct.

6.4 Privacy and Monitoring

TUMA may undertake the followings ONLY when required by law or competent authority in writing to:

- Monitor and record any e-mails which are transmitted over its computer system;
- Monitor or record the use of the internet by employees, and the nature of material downloaded from the internet;
- Monitor or record any use of computer equipment and user sessions to ascertain whether the TUMA's practices, policies and procedures (including usage of this ICT Policy) have been complied with;
- To investigate or detect the unauthorized use of the TUMA's computer system;
- To secure the effective operation of the TUMA's computer system;
- To determine whether any communication has been made which relates to the business of the TUMA; or
- For the purpose of preventing or detecting crime;
- Any e-mail sent by employees may therefore be intercepted and monitored by the TUMA for any of the above reasons. Accordingly, any messages, which are sent, are not private.

6.5 Access to Server Room

The server room is the room that houses the TUMA ICT infrastructure. Only Authorized Personnel are allowed to enter. The Vice Chancellor, DVCA, and DVCAA of TUMA are allowed to enter accompanied by the ICT personnel.

- The server rooms shall have the Biometric entry access, CCTV Camera for monitoring all security activities.
- All individuals accessing the ICT Server Rooms must sign in and out of the ICT Server Room(s) Access Log. This includes all visitors, who must be accompanied by ICT staff at all times. These log sheets are retained by the Head of ICT.
- Tailgating other staff in order to enter the ICT Server room(s) is not permitted, anyone caught doing that will be given warning while repeated offenders will be disciplined accordingly.
- In Case of emergence, The ICT Personnel in charge shall have access to the server room.

6.6 Server Machines

All software on servers must be authorized and requested by system owners; unauthorized software or data will be removed.

- Anti-virus software will be installed on every windows server and kept up-to- date.

- Passwords on the server machines will be under the custodianship of Department of ICT under supervision of DVCA/DVCAA. Hence not all personnel will have password access.
- All servers will sit behind firewalls, which mean access to these servers to the external environment will be by authorization. Any external support that may be required should then be addressed prior to the Head of ICT and the team (If need arises).

6.7 Environmental Protection

All servers will be protected from surges, spikes, sags or brownouts in the electricity supply by the use of Uninterruptible Power Supplies.

- All servers will be protected from excessively high temperatures and fire by temperature control and fire alarm.
- Security cameras will be installed and controlled so as to increase security within the premises.

6.8 Network Tools and Devices

- All of the network devices/tools should be configured on the base of preventing/filtering malwares, spywares, worms, and Internet viruses specifically to the firewall that is within our network.
- The entire network devices/tools password should not be disposed of to the public except to Vice Chancellor, ICT Head of Department, DVCA/DVCAA, and ICT personnel in charge to assess proper disposal procedure.
- Ensures a continuous updating of network devices/tools thus preventing vulnerable loops within the devices/tools.

7.0 COMPUTER, ICT PROCUREMENT, INVENTORY, WEBSITE AND ICT BUDGET

7.1 Computer Use

a) Computers are an integral part of everyday business life and we cannot escape the continuing growth in their use. This means that the monetary investment by the TUMA in infrastructure and ICT Personnel is huge to the point where the effect of ICT costs cannot be disregarded in the cost budgeting. Misuse of equipment can cause losses to the TUMA and cannot be tolerated.

b) Examples of what are not allowed include:

(i) Unofficially upload of any program strictly not authorized and duly licensed for work purposes by the ICT Department onto any computer. This includes games, screensavers, and unlicensed software's and so on;

(ii) Not to play games at work time. Sometimes it seems to be a feeling amongst people that playing games is an allowable pastime and of lesser concern. This train of thought should be severely discouraged and the offence be put into perspective;

(iii) Not to use the TUMA computer to vandalize, damage or disable the property of another person or organization;

(iv) Not make deliberate attempts to degrade or disrupt equipment, software or system performance by spreading computer viruses or by any other means. Also it is strictly prohibited to tamper with, modify or change the TUMA system software, hardware or wiring or take any action to violate the TUMA security system, and shall not use the TUMA system in such a way as to disrupt the use of the system by other users.

7.2 ICT Procurement

(a) Users shall not use the TUMA budget to purchase ICT goods or services for official use without authorization from the Vice Chancellor, Accounting Officer, Deputy Vice Chancellor for Administration (DVCA), TUMA ICT Head of Department, and other relevant organs applicable at TUMA.

(b) Users planning to request any ICT related hardware/software should fill form and also liaise with ICT Department for verification and need assessment before submitting requisition to Procurement Management Unit for procurement process.

(c) The ICT personnel who verify the purchase of the hardware/software that is no necessary or not related with the user's duties, for example, verifying the purchase of ICT hardware/software of high capacity and therefore leading to high cost not necessarily required by the user in day-to-day activities shall be held accountable.

(d) The University shall not bear cost associated with any requisition of ICT hardware/software which is not channelled through the University procurement system or which is outside of the ICT budget of the respective year unless authorized by the accounting officer in extenuating circumstances.

7.3 Inventory

1) All ICT related hardware/software are required to enter into TUMA ICT inventory within 5 working days once purchased, received in the store. The ICT Department, Accounts, and procurement office keep the ICT inventory.

2) ICT Department shall from time to time update DVCA/DVCAA regarding the status of the University ICT assets as shall be deemed feasible.

7.4 University Website

TUMA has full right for its website; ICT staff in charge should be allowed to update the website from time to time with prior permission from VC/DVCA/DVCAA

8.0 DEPARTMENT OF ICT (DICT)

It is hereby established the Head of Department of ICT shall be accountable to Deputy Vice Chancellor for Academic Affairs (DVCAA).

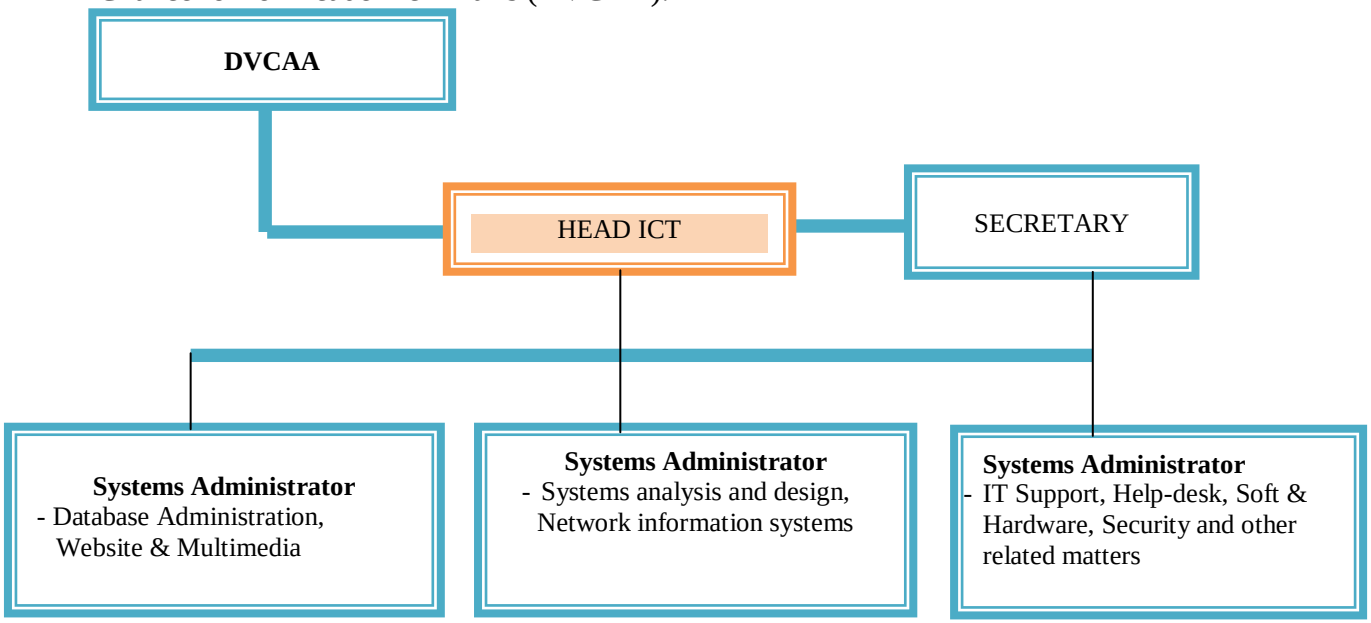

Figure 1: The Organization Structure of the Office of the Head, ICT

8.1 The Role of the Department

1) Administration - The Department through the Head of Department shall be responsible to oversee all activities of the department staff members by assigning tasks and areas of supervision so as to increase accountability, effectiveness and efficiency.
2) The department shall take charge of the safety of the ICT facilities such as computer lab, e-library (including Institutional Repository), and server rooms and ensure users adherence with this policy.
3) Moreover, it is with great interest for the department to create a strong team with a creative mind that shall foster innovative ideals, for this reason department identify, acknowledge and establish a rewarding system.
4) The department will provide one hub for all other entities to officially request the service including Internet distribution.

5) Coordinating - Resources are scarce with alternate use; hence department shall take charge in ensuring that all resources available are utilized in the effective and efficient manner that will be for the best interest of the TUMA development.

   Resources referred here includes to the following:

   - **Computing devices** (Laptops, desktops, tablets, mobile phones)
   - Printing devices (Scanners, fax, Copiers, and Printers)
   - o Projectors and Public Announcements systems
   - Security Cameras
   - LAN resources
     - Student Management System
     - D-Space
     - E-library
     - E-Resources
     - Video Teleconference
     - WAN resources
     - ZOOM, etc.

6) Planning and design - With the growth of the University it is inevitable for the department to forecast activities, demands and design a way forward that will serve as a framework. Moreover, it is the role of the department with linkage to ICTScience to provide the University with a stone/checkpoint and work-plan clearly showing how those plans can be achieved.
7) Development and Training - Department shall oversee training required for capacity building inline with training policy available at from HR as well as uses its members to offer training to the end users such as students and staff according to the planning addressed in the department.

   Henceforth this will include the following aspects:

8) Workshops, Seminars, short courses and Workshop - Department shall prepare a framework that will answer the question on what, when, who, and how the above aspects of the development will be handled without bias and disruption of the daily routines.
9) Advice and consultation - The department shall stand as an internal professional advisory body in the matters relating to the technologies in the TUMA administrative organs.
10) Liaison Head - The Department shall act as interface between ICT team, resources and services available to the potential clients including existing projects, newfound projects at TUMA in general with corroborators.

8.2 Objectives of the Department

- Increase effectiveness in the general ICT services;
- Load balancing job assignment/rotation integrating ICT staff to understand the University logic model and strategic plan.
- Define communication channels-there should be a proper line of communication between staff within the department and all other departments that will be working together.
- Raise awareness - The department will ensure other users within TUMA understands its existence as well as its functionality.
- Link between management- the objective of the department is to lower the gap between the management governing body and the ICT mission. It's of great interest for the ICT department to move in the same direction as University vision.
- Safeguard interest of University as well as members. It is crucial for ICT to provide best service that will serve purpose for staff that will be using in conjunction with students

8.4 Department Management

8.4.1 ICT Committee

It is hereby established a committee of ICT which shall be headed by the chairman - Deputy Vice Chancellor for Academic Affairs and Head of ICT who will be secretary accountable to University Academic Committee (UAC).

Role and jurisdictions are according to the ICT charter; however, members shall be appointed and serve for a duration of threeyears (triennium) prior their re-appointment if it deems fit by the chief accounting officer for a maximum period of six years as for other TUMA officials.

8.4.2 ICT Department Budget

The ICT Department, in collaboration with other University Directorates/Faculties/ Institutes/Departments shall actively participate in determining their Budgets and shall always operate within the Budget approved by the University Management. Any reallocation or expenditure beyond budget shall require written authorization from the accounting officer;

The ICT requisition may be initiated by any other department but ICT experts shall determine what is the right hardware or software needed for the department.

8.4.3 Liability

Any criminal liability accruing in relation with this policy shall be criminally handled. Students or classes, which shall Damage/loseUniversity ICT facilities, shall be required to pay forthwith. The University may take any other measures as per existing Labour Laws.

8.4.4 Right to privacy

1) Users should understand that all equipment, as well as the information it contains, belongs to the TUMA. Users should consequently have no expectation of privacy related to the use of any TUMA system.
2) TUMA has the fullest right to monitor the email and internet system, as well as accessing data such as emails received by employees. In the spirit of mutual respect and trust employees must also be aware that it is not the policy of the TUMA to monitor the email on a constant basis, and that they will be notified if specific departments will be under constant monitoring for certain reasons. Routine maintenance and monitoring of the network might however reveal that violations of the policy by specific users have occurred, which may result in an individual investigation, without any advance warning.

8.4.5 Private use

1) The TUMA agrees that a certain amount of incidental private use is allowed. This use however must not exceed what would be regarded by any reasonable person as fair and just, and is subject to the terms and conditions of the policy.
2) Private use of the system is a privilege and not a right, and what would be considered suitable use on a private account on another system will not necessarily be suitable for the TUMA system. The TUMA may restrict the users' access to the system at management's discretion**.**

9.0 COMPLIANCE WITH THE POLICY

The following actions will be regarded as failures to comply with TUMA ICT Policy and TUMA at its sole discretion shall take action against them:

1) Any failure on the part of an employee of the TUMA to act in accordance with the Policy may result in disciplinary action being taken against him or her depending upon the severity of the breach of the Policy.
2) Any failure to comply with the Policy on the part of a User who is not an employee may result in the immediate termination of the contractual or other relationship between that person or organization and the University. The non-compliance attributed by TUMA employees shall be handled in accordance with the National and University legal framework.
3) Any unauthorized use of Files, Applications, email or the Internet by a User which the TUMA, at its sole discretion, considers may amount to a criminal offence shall, without notice to the User concerned, be immediately reported to the respective authority.

10.0 REVIEW OF ICT POLICY

This policy shall be reviewed on a regular basis to accommodate demands arising from advancement in science and technology. Under normal circumstances the policy will be reviewed every three years. However, nothing shall limit the University inherent power to review this policy at any time as shall be deemed to be necessary and equitable.