



TECHNICAL UNIVERSITY OF MOMBASA

A Centre of Excellence

ICT POLICY



TUM IS ISO 9001: 2015 CERTIFIED

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS	v
DEFINITIONS	vi
PREFACE	ix
FOREWORD	x
ACKNOWLEDGEMENT	xi
EXECUTIVE SUMMARY	xii
1.0 INTRODUCTION	1
1.1 Vision	1
1.2 Mission.....	1
1.3 Core Values	1
1.4 Motto	2
1.5 Statement of Purpose	2
1.6 Guiding Principles	3
1.7 Policy Objectives.....	3
1.8 Legislative and Administrative Requirements	4
1.9 Regulatory framework:	4
1.10 Responsibilities	4
1.11 Scope/Applicability	5
2.0 ICT ACCEPTABLE USE	6
2.1 Purpose	6
2.2 Scope	6
2.3 ICT Acceptable Use Policy Statement	6
2.3.1 Professional and Ethical Use of ICT Facilities and Services	6
2.3.2 Withdrawal of Access.....	7
2.3.3 Commercial Activities	8
2.3.4 Donations and Gifts	8
2.3.5 Collaboration with Other Departments.....	8
2.3.6 Contract Management.....	8
2.3.7 ICTS Procurement Requirements	9
2.3.8 Collaborative Agreements with Authorized Suppliers.....	9

3.0 TELECOMMUNICATION INFRASTRUCTURE MANAGEMENT	
10	
3.1 Purpose	10
3.2 Scope	10
3.3 Telecommunication Policy Statement	10
4.0 NETWORK INFRASTRUCTURE MANAGEMENT	11
4.1 Purpose	11
4.2 Scope	11
4.3 Network Management Policy Statement	11
4.4 ICT Network Provision in New and Refurbished Buildings.....	12
4.5 Virtual Private Networks (VPN).....	13
4.6 Installation of Equipment.....	13
4.7 Connecting to the ICT Network.....	13
4.8 External Data Communications	13
4.9 Web Filtering.....	13
4.10 New or Changed Use of ICT Equipment.....	13
4.11 Monitoring of Network Performance.....	14
4.12 Wireless Network Users Responsibilities	14
4.13 Bring Your Own Device (BYOD)	14
5.0 INTERNET USAGE.....	16
5.1 Purpose	16
5.2 Scope	16
5.3 Internet Usage Policy Statement	16
5.4 Acceptable use of the Internet	16
5.5 Appropriate Use of Electronic Mail.....	17
5.6 Unacceptable use of Internet	18
6.0 SOFTWARE DEVELOPMENT, ACQUISITION, INTEGRATION & SUPPORT	19
6.1 Purpose	19
6.2 Scope	19
6.3 Software Development, Acquisition & Support Policy Statement	19

6.4 Outsourced Applications/Software Development	19
6.5 In-house Applications/Software Development	20
6.6 System integration.....	20
6.7 Software licenses	20
7.0 ICT EQUIPMENT REPAIR AND MAINTENANCE.....	21
7.1 Purpose	21
7.2 Scope	21
7.3 ICT Equipment Repair and Maintenance Policy Statement	21
7.4 Maintenance	22
7.5 Operational Logistics	22
7.6 Printing Facilities.....	22
7.7 Computer Servers.....	22
7.8 Computer Server Rooms	23
8.0 BUSINESS CONTINUITY AND DISASTER RECOVERY	24
8.1 Purpose	24
8.2 Scope:	24
8.3 Business Continuity and Disaster Recovery Policy Statement.....	24
9.0 INFORMATION ICT (CYBER) SECURITY POLICY.....	25
9.1 Purpose	25
9.2 Identified Risks	25
9.3 Scope	25
9.4 Policy Statement	26
9.5 Access to ICT Systems	27
9.6 Password Policy Rules.....	27
9.7 Inactivity Period	28
9.8 Protection against Malicious Software	28
9.9 Change Management.....	28
9.10 Authority for Monitoring ICT Systems.....	29
9.11 Physical Security.....	29
9.12 User Security Training and Sensitization	30
9.13 Asset Management.....	30

9.14 Information Security Incident Management30

9.15 Periodic Management Review30

10.0 REVIEW OF THE ICT POLICY.....32

ABBREVIATIONS AND ACRONYMS

BYOD	Bring Your Own Device
DBA	Database Administrator
DICTS	Directorate of Information and Communication Technology Services
ICT	Information and communication Technology
ITIL	IT Infrastructure Library
MFD	Multi-Function Device
MIS	Management Information Systems
LAN	Local Area Network
SOP	Standard Operating Procedures
SSL	Secure Sockets Layer
TUM	Technical University of Mombasa
VC	Vice Chancellor
VPN	Virtual Private Network

DEFINITIONS

"**Access**" means gaining entry into or intent to gain entry by a person to a program or data stored in a computer system and the person either:

- i) Alters modifies or erases a program or data or any aspect related to the program or data in the computer system;
- ii) Copies, transfers or moves a program or data to;
 - a. Any computer system, device or storage medium other than that in which it is stored; or
 - b. To a different location in the same computer system, device or storage medium in which it is stored;
- iii) Causes it to be output from the computer in which it is held, whether by having it displayed or in any other manner; or
- iv) Uses it by causing the computer to execute a program or is itself a function of the program;

"**Account holder**" shall mean any person granted a user account with the Technical University of Mombasa.

"**Authorized supplier**" shall mean any hardware or software company that has an updated partnership agreement with the manufacturers.

"**Bring Your Own Device (BYOD)**" refers to the policy of permitting employees to bring personally owned devices like laptops, tablets and smartphones, to their workplace, and to use those devices to access privileged institutional network, information and application.

"**Compliance**" means undertaking activities or establishing practices or policies in accordance with the requirements or expectations of an external regulatory authority.

“**Cybercrime**” or computer-oriented crime, is the crime that involves a computer and networks such as the Internet (networks including chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS).

“**Denial of Service**” means procedures or actions that can prevent a system from servicing normal and legitimate requests as expected.

“**ICT Resources**” refers to all of the University’s Information and Communication Technology Resources and facilities including, but not limited to: mail, telephones, mobile phones, voice mail, SMS, facsimile machines, email, intranet, e-Services, computers, printers, scanners, access labs or other facilities that the University owns, leases or uses under license or by agreement.

“**ICT security**” can be defined as 'the state of being free from or mitigating unacceptable risk'

“**ITIL - IT Infrastructure Library**” is a series of books explaining procedures and best practices for the IT industry to follow

“**Malware**” or malicious software, is a blanket term for any kind of computer software with malicious intent

“**Manager**” means the Academic and Administrative Head of the Department established by the University statutes.

“**Multipurpose Printer**” is typically a printer, incorporating scanning, copying, and printing. Some can also be used for emailing and faxing.

“**Network Sniffing**” means attaching a device or a program to a network to monitor and record data travelling between computers on the network.

“**Ping attack**” is a form of a denial of service attack, where a system on a network receives an echo-request, by another system at a fast repeating rate thus tying up the computer so no one else can contact it.

“**Port scanning**” means attempting to learn about the weaknesses of a computer or a network device by repeatedly probing it with a series of requests for information.

“**Redundancy**” describes a computer or network system components that are installed to back up primary resources in case they fail

“**Spam**” means unauthorized and/or unsolicited electronic mass mailings

“**Spoofing**” means the deliberate inducement of a user or a computer device to take an incorrect action by Impersonating, mimicking, or masquerading as a legitimate source.

“**Standard**” is a reference point against which different aspects of the program and/or institution are compared or evaluated against for quality assurance purposes.

“**Standard Operating Procedures (SOP)**” is a set of step-by-step instructions compiled by an organization to help staff carry out complex routine operations.

“**Student**” means a person registered by the University in a study programme.

“**University**” This term shall be used to refer to Technical University of Mombasa.

“**User**” refers to any person accessing/developing/implementing and/or using ICT-based information and ICT resources owned, managed, supported or operated by, or on behalf of, the University.

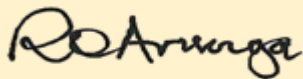
“**User Account**” shall mean an authorized user account, provided to a user, to be used solely by that user, for the purpose of accessing services as granted to that user account.

“**Vice-Chancellor**” means the Academic and Administrative Head of the University.

PREFACE

This ICT policy takes cognisance of recent developments and strides that have occurred in the Information and Communication Technology sector, particularly in terms of information gathering and sharing. In the education sector, technological advances have empowered institutions of higher learning to improve on their delivery of knowledge, by providing means of personalized instruction, customised teaching and enabling educators to use a variety of learning methods.

The policy provides TUM users with guidelines and regulations on proper usage of existing ICT services and facilities for enhanced service delivery in teaching, partnership, research, innovation, administration and other scholarly activities. The policy encompasses the current laws governing ICT development and usage in Kenya. All developers and users of ICT services and facilities are advised to read and be familiar with this policy.



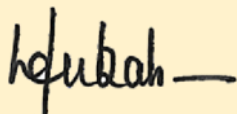
Dr Robert Arunga
Chairman of Council

FOREWORD

Information and Communication Technology (ICT) is a crucial enabler in the achievement of the University's vision and mission. It is in recognition of this, that, Technical University of Mombasa has reviewed the ICT policy to encompass the emerging trends in the industry.

Technical University of Mombasa through the policy commits to adhere to the appropriate use of Information and Communication Technology Services in support of teaching, partnerships, research, innovation, learning, and administrative functions for enhanced service delivery. The Management also commits to ensuring that adequate resources are provided to implement a reliable and appropriate ICT infrastructure for the guaranteed provision of quality services.

On behalf of the University Senate and Management, I would like to take this opportunity to thank the University Council, Management and the Directorate of ICT services for their efforts in reviewing comprehensively the ICT policy that will guide the development and management of ICT and its utilization in the University.



Prof. Laila U. Abubakar

Vice-Chancellor

ACKNOWLEDGEMENT

I would like to take this opportunity to thank all members involved in the review of the ICT policy. I wish to particularly acknowledge the contribution of the Adhoc committee that reviewed this policy.

- | | | |
|-------|---------------------|----------------------------|
| i) | Prof. Joseph Rasowo | DVC AFP (Chairman) |
| ii) | Mr Mohamed Swaleh | Manager ICT (Secretary) |
| iii) | Dr Mvurya Mgala | Director, ICI |
| iv) | Mr Joel Awino | Dean of students |
| v) | Ms. Serah Welcome | Deputy Registrar A. A |
| vi) | Ms. Serah Okumu | Deputy Chief Legal Officer |
| vii) | Dr Kennedy Ondimu | ICI Department |
| viii) | Mr Horatius Kimwere | ICT Office |



Prof. Joseph Rasowo
Deputy Vice-Chancellor (AFP)

EXECUTIVE SUMMARY

A new TUM strategic plan 2018 – 2022 has been developed following the expiry of the previous plan 2014 – 2018. Based on the contextual analysis of the operating environment, TUM recognizes that successful implementation of the strategic plan will depend heavily on the ICT function.

It is against this background that the University has reviewed the ICT Policy that takes into account the changes in the ICT sector which is a dynamic industry.

This policy provides for the policies on acceptable use, telecommunications and infrastructure, network management, internet usage, ICT equipment, repair and maintenance, business continuity, cybersecurity and implementation.

1.0 INTRODUCTION

Technical University of Mombasa (TUM) is an institution of higher learning established by the Universities Act, 2012 and University Charter, 2013. Core among her mandate is to undertake technological, professional and scientific education and training to disseminate knowledge while ensuring access, equity, quality and relevant education.

The Directorate of Information and Communication Technology Services has been keen on creating a conducive ICT environment that facilitates the free flow of information to enhance knowledge sharing in education, scientific findings dissemination, cultural exchange among others. This has been actualized through the adoption of the ICT Policy as a guiding framework in the development, implementation, and effective usage of the ICT services and facilities. All ICT users of the University community will be expected to be familiar with and comply with the provisions of the policy.

This policy is guided by the following:

1.1 Vision

A Technical University of Global Excellence in Advancing Knowledge, Science and Technology

1.2 Mission

To advance knowledge and its practical application through teaching, research and innovation to serve both industry and the community

1.3 Core Values

The Council, Senate, Management, staff and students of TUM will endeavour to institutionalize and inculcate values fostering a strong corporate culture while promoting quality service delivery, cohesion in our diverse community and

achieving the targeted goals. These will be realized by espousing the following values:

- i) *Excellence.* We strive for excellence in quality teaching, learning and research, and customer focus by continuously assessing ourselves, applying our own and international benchmarks.
- ii) *Integrity and Professionalism.* We expect high standards of integrity, ethics and respect from one another across the institution and honour collegiality and a climate of critical professionalism among staff and students.
- iii) *Equity.* We are committed to equity, diversity and fairness, and seek to nurture and build on our diverse cultural heritage
- iv) *Teamwork.* We place a high premium on teamwork and shared responsibility working with each other and with external groups in ways that are mutually beneficial.
- v) *Creativity, innovativeness and environmental sustainability.* We embrace innovative problem solving and promote creative value-based solutions. We cultivate a socially secure, responsive and sustainable green environment.

1.4 Motto

Jiddu Tajidu (Endeavour and Achieve)

1.5 Statement of Purpose

This University-wide ICT policy is formulated to guide the implementation and usage of University ICT resources and facilities by providing appropriate standards to be adopted at the University. The policy is also meant to safeguard the University against legal implications and to ensure availability, integrity and confidentiality of ICT data and information.

1.6 Guiding Principles

- i) The University ICT Resources exist and are maintained to support the core purposes of the University in teaching, learning, research, innovation and administration.
- ii) The University reserves the right to monitor the use of its ICT Resources and to deal appropriately with Users who use its ICT resources and facilities in ways contrary to the conditions of use set out in this policy.
- iii) Materials produced using the University ICT Resources are to be generated subject to the relevant University policies without compromising on privacy and confidentiality of University data and information.
- iv) The University accepts no responsibility for loss or damage, consequential loss or damage, or loss of data arising from the use of its ICT Resources or the maintenance of its ICT Resources

1.7 Policy Objectives

The objective of this ICT policy is:

- i) To provide guidance in developing a pervasive, reliable and secure communications infrastructure conforming to recognized international standards;
- ii) To provide a framework for the development and management of ICT network services;
- iii) To develop and implement Management Information Systems in the University;
- iv) To establish information requirements and implement security across the University's ICT infrastructure;
- v) To provide leadership in ensuring compliance of applicable statutes, regulations and mandates while handling organizational information within the University;

- vi) To uphold the integrity and image of the University by ensuring that the content of the University's website is accurate, consistent and up-to-date.

1.8 Legislative and Administrative Requirements

The following but not limited to, legal instruments and institutional policies shall be applicable to this policy:

- i) The Constitution of Kenya;
- ii) The Kenya Information and Communications Act (Amended 2013);
- iii) The Computer Misuse and Cybercrimes Act 2018;
- iv) The Universities Act 2012;
- v) The Access to Information Act of 2016;
- vi) The Copyright Act 2014;
- vii) The Trademarks Act 2012;
- viii) The Public Finance Management Act 2012;
- ix) The Public Procurement and Asset Disposal Act 2015;
- x) The Public Archives and Documentation Service Act 2012;
- xi) The Records Disposal Act 2015;
- xii) Technical University of Mombasa Statutes.

1.9 Regulatory framework:

This policy is intended to meet regulatory requirements such as the Information Security Standard, ICTA-3.001:2016.

1.10 Responsibilities

The Manager ICT shall have overall responsibility in the implementation of this policy.

1.11 Scope/Applicability

The policy shall apply to all University staff and students, any other organizations accessing services over University ICT resources, persons contracted to develop, repair or maintain University's ICT resources and suppliers of outsourced ICT services.

The policy provides guidelines for:

- i) Acceptable use of ICT facilities
- ii) Telecommunication Infrastructure Management
- iii) Network Infrastructure Management
- iv) Use of Internet and Email
- v) Development and use of Management Information Systems
- vi) ICT Equipment Repair and Maintenance
- vii) University Data Backup Procedures
- viii) Information / Cyber Security
- ix) Non-compliance of the Policy

2.0 ICT ACCEPTABLE USE

2.1. Purpose

The policy seeks to define appropriate controls to access or use of the University ICT resources and requires that the users utilize these facilities and services in an appropriate and responsible manner. The University reserves the right to record and monitor activity, limit, restrict, cease, or extend access to all ICT facilities and services.

The purpose of the ICT Acceptable Use Policy is to:

- i) Provide a framework for the development and management of ICT network services in line with the objectives of the university;
- ii) Guide in the handling of organizational information within the University by ensuring compliance with applicable statutes, regulations and mandates;
- iii) Provide standards, guide users and decision-makers in the development and use of ICT resources;
- iv) Promote widespread use of ICT applications for efficient teaching, partnerships, research, innovation and learning;
- v) Ensure that ICT resources are secured and protected against abuse, damage, loss or theft while in use;
- vi) Provide the consequences of misuse of ICT resources within the University.

2.2. Scope

The policy is applicable to all ICT resources.

2.3. ICT Acceptable Use Policy Statement

2.3.1. Professional and Ethical Use of ICT Facilities and Services

All users of ICT facilities and resources are expected to:

- i) Act in a professional and ethical manner while using the facilities;

- ii) Refrain from using ICT resources for the commission of cybercrimes;
- iii) To apply the same personal and professional courtesies and considerations in electronic messages as they would in other forms of communication;
- iv) Refrain from transmitting frivolous, inciting, abusive or defamatory messages;
- v) Refrain from transmitting electronic messages that are illegal or contravene other University policies;
- vi) Not to make available any content that they do not have rights to; and
- vii) Not to cause interference with other users of electronic messaging services. Such interference includes transmission of an e-mail, chain letters, widespread distribution of unsolicited e-mail, junk mail, pyramid mail and the repeated sending of the same message.

2.3.2. Withdrawal of Access

The University shall withdraw access to ICT facilities and services under the following conditions: -

- i) Upon termination of a staff member's employment with the University and the exit of a student from the Institution;
- ii) When instructed by the Vice-Chancellor;
- iii) Upon violation of the provisions of this policy;
- iv) When charged with a criminal offence.

Upon withdrawal of access to ICT facilities, the following shall apply;

- i) Students or staff whose access has been suspended shall have the right to appeal in writing to the ICTS Committee;
- ii) Upon termination of employment with the University, any University issued ICT device must be returned to the University;
- iii) Upon termination of employment with the University, any University data must be returned to the University.

2.3.3. Commercial Activities

Unless permitted by other University policies or approved by the University management, the ICT resources shall not be used for commercial purposes or personal gain.

2.3.4 Donations and Gifts

Donations of any ICT equipment will have to be sanctioned by the ICTS committee and shall remain the property of the university.

The Anti-corruption policy on gifts and donations shall apply.

2.3.5 Collaboration with Other Departments

The Department shall ensure collaboration with other departments to ensure the reliable and prompt provision of ICT services.

2.3.6. Contract Management

DICTS shall:

- i) Be the user department on all ICT contracts;
- ii) Be required to set specifications for the procurement of all ICT related software and hardware;
- iii) Ensure that all contracts comply with the requirements of standard ICT contracts;
- iv) Be included in all commissioning and installation of ICT equipment and software within the University;
- v) Ensure that all equipment and software purchased in relation to ICT shall have a warranty period.

All system maintenance contracts shall run for a maximum period of two (2) years for smooth handover of the system to the university staff. During this period, the consultant will be required to train not less than two (2) ICTS staff on the maintenance of the same.

2.3.7. ICTS Procurement Requirements

ICT equipment, hardware and software, should only be purchased from authorized suppliers with a warranty period that has to be specified during the procurement process.

2.3.8. Collaborative Agreements with Authorized Suppliers

The University will develop linkages and collaborate with partner suppliers of authentic hardware and software. The linkages and collaboration will encompass training and workshops on sensitization of current ICT trends, students' attachment and potential recruitment of our students.

3.0 TELECOMMUNICATION INFRASTRUCTURE MANAGEMENT

3.1. Purpose

The policy defines appropriate use of telecommunications services at the University.

3.2. Scope

The policy applies to all telecommunications services: billed services to University accounts and the traditional telephones, software-based phones and remote phones, cellular phones, cellular tablet devices, pagers, calling cards, conferencing services and voicemail.

3.3. Telecommunication Policy Statement

Under this policy, the following shall constitute acceptable use of telecommunication facilities and services provided for or within the University:

- i) University telecommunication facilities are intended for calls related to University business activities;
- ii) Access and use of University telecommunication facilities is a privilege that is granted in connection with an individual's duty to the University;
- iii) The University reserves the right to extend policies to mobile devices and to remotely reset devices;
- iv) University staff are expected to use all devices in a safe and prescribed manner and in adherence to all laws, rules and regulations applicable.

4.0 NETWORK INFRASTRUCTURE MANAGEMENT

The policy establishes the provisions for the installation, maintenance and operation of the University Network. The University network provides inter-connections between all University computing resources. Therefore, it is important that the network infrastructure is properly controlled, maintained and managed.

4.1. Purpose

The policy defines requirements for the management and operation of University ICT networks.

4.2. Scope

The Policy applies to all University network infrastructure and/or staff responsible for the provision and management of ICT networks owned by or operated on behalf of the University.

4.3. Network Management Policy Statement

The University requires that:

- i) The University's network shall be managed and maintained by suitably authorized and qualified staff;
- ii) The network must be designed and configured in order to deliver high performance and reliably meet the University's needs;
- iii) Configured firewalls and other security systems as may be approved from time to time by the ICTS committee must be used to protect the domains containing sensitive information, vulnerable equipment and the University's Management Information Systems.
- iv) Remote access to the network and other network resources will be subject to robust authentication. Data must be encrypted during transit across the network.
- v) DICTS has ownership of all Network Components comprising the Computer

Network and must maintain proper documentation and inventory of all Network Components connected directly or indirectly to the Computer Network.

- vi) Use of the network for training will require liaising between the Directorate and the training department.
- vii) DICTS should ensure availability of network at all times without compromising on integrity and security and preserve the privacy of users to the greatest extent possible.
- viii) DICTS is responsible for managing all aspects of network security, traffic profiling, traffic prioritization, authentication and control of access to the Computer Network
- ix) DICTS is responsible for the disaster recovery of the network.
- x) DICTS will operate a helpdesk facility for the logging of all faults and problems with the Computer Network. All faults requiring the attention of the Network Operators must be documented.
- xi) All communication rooms and cabinets shall remain locked at all times and access to such facilities or interference with ICT network equipment shall be restricted to designated ICT staff.

4.4 ICT Network Provision in New and Refurbished Buildings

- i) Network provision for new and refurbished buildings shall be made in accordance with the specifications published from time-to-time by the DICTS.
- ii) Where the Network requirements are of specialized nature, the officer concerned shall seek further guidance from the Network Administrator.
- iii) All new buildings to be erected in the University shall incorporate an appropriate structured cabling system to allow connection to the University network.
- iv) DICTS will maintain a network infrastructure that supports network hierarchy.

4.5 Virtual Private Networks (VPN)

Authorized users of the University ICT services shall be granted rights to use VPN connections if they intend to gain access to the University ICT intranet services through public networks.

4.6 Installation of Equipment

The specification(s) and installation of any equipment in the server rooms and cabinets shall require the prior written consent of the Manager, DICTS.

4.7 Connecting to the ICT Network

All connections to the University's ICT networks must conform to the protocols defined by DICTS and with the requirements that apply to Internet Protocol (IP) addresses.

4.8 External Data Communications

- i) All external data communications shall be channelled through University-approved links.
- ii) No external network connections shall be made without the prior written consent of the Manager, ICTS.

4.9 Web Filtering

DICTS shall be responsible for the implementation of appropriate filtering facilities for appropriate internet traffic.

4.10 New or Changed Use of ICT Equipment

The Manager, DICTS shall approve any plan that involves a new use, a change of use or addition to the University's ICT networks that might impact on the performance or security of the network.

4.11 Monitoring of Network Performance

DICTS shall monitor and document University ICT network performance and usage and shall maintain regular monthly reports.

4.12 Wireless Network Users Responsibilities

- i) Any person attaching a wireless device to the University network shall be responsible for the security of the computing device and for any intentional or unintentional activities arising through the network pathway allocated to the device.
- ii) The University accepts no responsibility for any loss or damage to the user computing device as a result of connection to the wireless network.
- iii) Users shall ensure that they run updated antivirus, host firewall and anti-malware software and that their devices are installed with the latest operating system patches and hotfixes.
- iv) Wireless network users shall ensure that their computer systems are properly configured and operated so that they do not cause inconveniences to other University network users.
- v) A wireless network is provided to support teaching, research or related academic and administrative activities at the University. Use of the University wireless network services for other purposes is prohibited.

4.13 Bring Your Own Device (BYOD)

- i) Employees who prefer to use their personally-owned ICT equipment for work purposes must secure university data to the same extent as university ICT equipment, and must not introduce unacceptable risks, such as malware.
- ii) The University has the right to control its information. This includes the right to backup, retrieve, modify and/or delete corporate data without reference to the owner or user of the device.
- iii) The University has the right to seize and forensically examine any device within the University premises believed to contain, or to have contained

- corporate data where necessary for investigatory or control purposes.
- iv) Suitable antivirus software must be properly installed and running on all devices.
 - v) Device users must ensure that valuable corporate data created or modified on the devices are backed up regularly on the corporate network.
 - vi) Devices used for BYOD will receive limited support on a “best endeavours” basis for academic and administrative purposes.
 - vii) Use of BYOD within the university network is at the owners ‘risk.
 - viii) BYOD should not be used to infringe on other people’s privacy rights.

5.0 INTERNET USAGE

5.1 Purpose

The policy defines the rules to ensure that usage of the internet complies with University policy and to protect the University against damaging legal consequences.

5.2. Scope

The Policy applies to all users granted access to any University ICT Resource with the capacity to connect and access the internet, the intranet, or both.

5.3 Internet Usage Policy Statement

- i) The University may at its own discretion use network monitoring tools to police her networks and identify restricted behaviour or illegal activities; and
- ii) Internet users at the University are expected to use internet resources in compliance with the University policies.

5.4 Acceptable use of the Internet

Internet users are encouraged to use the Internet to further the goals and objectives of the University.

The types of activities that are encouraged include:

- i) Use of internet services to support the educational, partnership, research, innovation and administrative goals of the University;
- ii) Participating in professional development activities; and
- iii) Communicating with university stakeholders;

5.5 Appropriate Use of Electronic Mail

- i) Electronic mail provided by the University is intended for teaching, learning, research, outreach and administrative purposes.
- ii) Electronic mail may be used for personal communications within appropriate limits.
- iii) Mass unsolicited mailings and dissemination of chain letters are prohibited.
- iv) Users shall explicitly recognize their responsibility for the content, dissemination and management of the messages they send. This responsibility means ensuring that messages:
 - i. Are courteous and polite;
 - ii. Are consistent with University policies;
 - iii. Do not contain obscene, offensive or slanderous material;
 - iv. Are not used for purposes that conflict with the University's interests;
 - v. Do not unnecessarily or frivolously overload the email system (e.g. spam and junk mail);
 - vi. Do not carry harmful content, such as Viruses
 - vii. Are not for commercial purposes
- v) Users agree to indemnify the University for any loss or damage arising from the use of University's email.
- vi) Postings by users from the University email address to newsgroups shall contain a disclaimer stating that

"The opinions expressed are strictly the user's and not necessarily those of the University....."
- vii) The user shall exercise caution when opening e-mail attachments received from unknown senders, which may contain viruses.

5.6 Unacceptable use of Internet

- i) The Internet may not be used for illegal or unlawful purposes;
- ii) The Internet may not be used in any way that violates University policies, rules, or administrative orders including, but not limited to, terms of service for staff or students code of conduct.
- iii) The policy prohibits access for non-employees to TUM resources or network facilities (unless pre-approved by University management),
- iv) Unacceptable use of the internet includes the following:
 - i. Downloading, Displaying or sending of graphics which may be reasonably interpreted as offensive.
 - ii. Breaching the terms and conditions of a software licensing agreement.
 - iii. Violations of the rights of any person or company protected by intellectual property (IP) law and University regulations.
 - iv. Introduction of malicious programs into the network or server, for instance, viruses, worms, Trojan horses or e-mail bombs.
 - v. Causing a security breach or disruptions of network communication.
 - vi. Port scanning or security scanning, unless prior notification is made to DICTS.
 - vii. Circumventing user authentication or security of any host, network or account.

6.0 SOFTWARE DEVELOPMENT, ACQUISITION, INTEGRATION & SUPPORT

6.1 Purpose

The Policy defines the general guidelines for applications/software development and support within the University.

6.2 Scope

The policy covers software development and support guidelines for University-owned application/software developed within and outside the University.

6.3 Software Development, Acquisition & Support Policy Statement

DICTS is responsible for developing and maintaining university administrative and academic systems.

The policy governs system development, acquisition and support in the University. DICTS must ensure the following:

- i) Availability of funding for any software project before embarking on any ICT project;
- ii) Signoffs and approval are provided by system owners prior to moving any system or application to a production environment;
- iii) Use of web-based and open source applications in the university is encouraged;

6.4 Outsourced Applications/Software Development.

- i) DICTS is allowed, subject to University management approval, to procure software or customize the software for internal usage. Such software must comply with the University policies and statutory requirements.
- ii) Outsourced software must conform to the required standard for software development.

- iii) University shall not provide any support to any systems built outside DICTS or inherit any systems developed outside of DICTS or purchased without any pre-approval by the University.
- iv) Website content is the responsibility of departments, schools/Institutes and Corporate Communications office. However, the DICTS shall provide technical support to the University website.

6.5 In-house Applications/Software Development

- i) All systems developed internally must conform to the required standards for software development.
- ii) Functional and user requirement must be approved by University management, and must be as complete as possible to avoid later changes or additions, which have cost implications.

6.6. System integration

- i) University systems must interoperate. DICTS shall ensure that the University procures an integrated system.
- ii) Once the system is procured, DICTS shall fully manage the installation, commissioning and operationalization of the system.

6.7 Software licenses

- i) The University and all software users are personally responsible for complying with the Copyright Act 2014 and with the terms and conditions of the particular contracts or software licenses relating to purchased, leased or acquired hardware and software. In particular, copying software without authorization from the copyright holder is a breach of the Act.
- ii) DICTS is responsible for compliance and licensing for University managed software and packages.

7.0 ICT EQUIPMENT REPAIR AND MAINTENANCE

7.1 Purpose

The Policy outlines the standards for maintenance and support of university-owned equipment.

7.2 Scope

The policy includes all computer equipment owned, managed, supported or operated by, or on behalf of the University. This may include, but not limited to Laptops, desktop system, tablets (such as iPads etc), Smartphones, Routers/Wireless Access Points, Printers, etc.

7.3 ICT Equipment Repair and Maintenance Policy Statement

- i) DICTS shall provide full support for software and hardware to administration, School, staff and students using University-owned equipment. This includes the installation of necessary software, updates and patches as well as troubleshooting and repair of any issues related to the operation of the devices.
- ii) Equipment service must follow the user support policy.
- iii) Unserviceable equipment will be disposed of in accordance with the Public Procurement and Asset Disposal Act 2015.
- iv) The university will not take any responsibility in case of any problems that may arise as a result of DICTS support of any additional non-university owned equipment that they would like to use.
- v) DICTS are responsible for maintaining and supporting software on the workstation. All software installed on university-owned machines should be directly related to university business, licensed and authorized.

7.4 Maintenance

The Manager ICT shall draw a schedule for maintenance at the beginning of every financial year. Preventive maintenance and corrective maintenance shall be carried out according to the recommendations of the manufacturer of the hardware, in terms of frequency and method of maintenance.

7.5 Operational Logistics

- i) Operationally, users shall resolve basic problems as the first level of maintenance and support.
- ii) At the second level, an ICT Officer-in-charge of every school/campus shall offer support to the users on issues they cannot resolve.
- iii) At the third level, specialist Maintenance Engineers at the Central DICTS office shall handle issues escalated from various schools.
- iv) The fourth and final level should enable the DICTS central office to work in liaison with vendors, suppliers and hardware manufacturers to repair and/or replace faulty equipment.
- v) The DICTS central office shall be charged with the responsibility of enforcing any maintenance contracts, agreements and warranties.

7.6 Printing Facilities

- i) The DICTS shall, where possible set-up managed multi-purpose printers (3-in-1 printer, scanner and copier) with access control, with the majority being in open access areas available for staff. Multi-purpose printers in staff offices and locked rooms will be minimized.
- ii) The multipurpose printers may be serviced via an outsourced contract which ensures that the printer fleet is managed effectively.

7.7 Computer Servers

- i) All servers shall be registered with the DICTS.

- ii) Any server deployed on the University ICT network shall have an operational group that shall be responsible for its system administration.

7.8 Computer Server Rooms

- i) The computer server rooms shall contain an adequate air conditioning system.
- ii) No drainage pipes shall run within or above computer server rooms to reduce the risk of flooding. Where possible, the floor within the computer server room shall be a raised false floor to allow computer cables to run beneath the floor and reduce the risk of damage to computer equipment in the case of flooding.
- iii) Power feeds to the servers shall be connected through Uninterrupted Power Supply (UPS) and surge, protector, to allow smooth shutdown and protection of computer systems, in case of power failure. The standby power source shall be provided to the computer site to help protect the computer systems in the case of mains power failure.
- iv) Access to the computer server rooms shall be restricted to authorized University staff only.

8.0 BUSINESS CONTINUITY AND DISASTER RECOVERY

8.1 Purpose

The policy provides a means to restore the integrity of the computer systems in the event of a hardware/software failure or physical disaster and provide a measure of protection against human error or the inadvertent deletion of important files.

8.2 Scope:

The policy covers all University personnel, processes and technology.

8.3 Business Continuity and Disaster Recovery Policy Statement

- i) The policy requires that all University data maintained by University be backed up periodically and that the backup media be stored at a secure off-site location, and that recovery tests are performed on a regular basis.
- ii) Technology Redundancy – Mission-critical functions must always have ready to go alternatives e.g. a mirror server.
- iii) Human Resource Redundancy – Each core responsibility needs to have one or more alternative personnel so as to allow continuity of operations. The Manager, ICTS shall ensure that every project has alternatives for staff that provide essential support service to guarantee that services are provided even in the absence of these staff members for the continuity of systems.
- iv) Process/procedures redundancy – alternative procedures to be documented in Standard Operating Procedures (SOP) in case of disaster recoveries.

9.0 INFORMATION ICT (CYBER) SECURITY POLICY

9.1 Purpose

This policy can also be referred to as 'Information Security', 'ICT security' or 'Cybersecurity policy'.

This policy seeks to ensure appropriate security for all ICT resources, facilities and systems in the University domain of ownership and control and to promote security awareness among the members of the University.

9.2 Identified Risks

The identified risks to the University concern the following categories:

- i) Confidentiality of information - the privacy of personal or corporate information;
- ii) The integrity of data (the accuracy and completeness of data) - Protection is required against deliberate or accidental corruption of data;
- iii) Assets - identifying and accounting of assets;
- iv) Efficient and appropriate use - ensuring that University ICT resources and systems are used for the purposes for which they were intended, in a manner that does not interfere with the rights of others; and
- v) System availability-concerned with the full functioning of a system and its components.

9.3 Scope

The policy covers all assets associated with information systems including information assets, software assets, physical assets and services and applies to all ICT users, campuses, departments and sections.

The policy will adhere to all provisions of "The Computer Misuse and Cybercrimes Act 2018" and its regulations.

9.4 Policy Statement

- i) There shall be no unauthorized access to either physical or electronic information within the custody of TUM.
- ii) All users of ICT assets are responsible for the protection, integrity and availability of the assets assigned to them.
- iii) All tangible ICT assets are to be located in appropriately secure physical locations.
- iv) All members of the University are obligated to respect the rights of individuals and to protect confidential and/or private information.
- v) Users of information systems are required to report any observed or suspected security weaknesses in, or threats to, systems and services.
- vi) All university users of BYOD are responsible for the security of their personally-owned computers or other network devices and are subject to this Security policy.
- vii) All third party vendors providing University services and support, whether on campus or from a remote location, are subject to this Security policy and will be required to acknowledge this in the contractual agreements.
- viii) Any entity that is a registered user and connected to the university network is responsible for the security of its computers and network devices and is subject to this Security Policy
- ix) While the University communications systems are electronically safeguarded and maintained in accordance with current best practice, no guarantee can be given regarding the protection, confidentiality, privacy or security of any information.
- x) The University reserves the right to withdraw, restrict or limit any User's access to its ICT Resources in the event that a breach of this policy and policies associated with this policy is suspected.
- xi) The University may further investigate any such suspected breach under other University processes and may result in disciplinary action

(as contained in the relevant University statutes and/or employer-staff agreements) being taken against the offender.

9.5 Access to ICT Systems

All individuals who require access to the ICT system and information resources will be properly identified, by means of a unique user account. Appropriate access controls will be introduced into every ICT system, with three objectives in mind:

- i) Preventing unauthorised users from accessing and misusing the system;
- ii) Constraining the authorised Users to their legitimate purposes; and
- iii) To provide the ability to create audit logs detailing User's activity.

9.6 Password Policy Rules

- i) All system-level passwords shall be changed at least once every month.
- ii) All user-level passwords such as email, web, and desktop computer shall be changed at least once every six (6) months.
- iii) Passwords shall not be inserted into email messages or other forms of electronic communication.
- iv) Passwords for the University accounts shall not be used for other non-University access such as personal account, Yahoo Mail, and Bank ATM.
- v) Users shall not share the University passwords with anyone.
- vi) Users shall not use the "Remember Password" feature of applications like Google apps.
- vii) Users shall not write passwords down and store them anywhere in their offices.
- viii) Where an account or password is suspected to be compromised the affected passwords shall be changed immediately. DICTS shall be alerted immediately to investigate if it affects critical University information systems or processes.

9.7 Inactivity Period

- i) If there has been a period of inactivity on a desktop computer or terminal, the system must automatically blank the screen and suspend the session. Re-establishment of the session must take place only after the User has provided the proper authentication.
- ii) All corporate applications will incorporate automatic time-out of log-ins after an appropriate period of inactivity.

9.8 Protection against Malicious Software

In order to mitigate the risk of virus infections to ICT facilities and services and, in order to ensure the integrity of University ICT facilities and services, the University through the DICTS will:

- i) Ensure that a licensed and trusted anti-virus software is deployed and updated on all ICT facilities and services provided by the University in all its campuses.
- ii) Computer Laboratory Administrators and owners of computers, in consultation with the DICTS, shall be responsible for executing required procedures that ensure virus protection on their computers. Computers shall first be verified as virus-free before being allowed to connect to the University network.
- iii) Not permit any use or deployment of unlicensed anti-virus software, or any software not approved by the DICTS.

9.9 Change Management

- i) Change control procedures through ITIL, will provide a formal approach to the management of change, enabling individual changes to be applied in a controlled and consistent manner.
- ii) A change control process must be used to ensure that all changes in software, hardware, communications links and procedures are effected only after

receiving proper authorization from Management.

9.10 Authority for Monitoring ICT Systems

Users have a legitimate expectation to privacy in the carrying out of approved University activities. However, the University also has a right to inspect any data on a computer system connected to the University's resources (regardless of data or system custodianship), to prevent, detect or minimize unacceptable behaviour on that computer system, and to provide, to any authorized member of the University community, or law enforcement bodies, any information it possesses regarding the use of the University's resources. Where such action is taken, users who have data inspected, and are found to be conforming to this policy, have a legitimate expectation that confidentiality will be preserved.

9.11 Physical Security

- i) **Physical security of ICT facilities** is necessary to prevent unauthorized use and to ensure that systems are adequately protected against natural hazards, theft and damage. Access to every office, computer room, and work area containing sensitive information, or the means to access such information, will be physically restricted. Rooms and facilities, which house non-public ICT resources will be protected with physical security measures that prevent unauthorised persons from gaining access.
- ii) **Security marking.** All University computer hardware shall be prominently marked, either by branding or etching, with the name of the University unit and name of office or computer laboratory where the equipment is normally located.
- iii) **Sitting of computers:** Wherever possible, computer equipment shall be kept at least 1.5 metres away from external windows in high-risk situations.
- iv) **Opening windows:** All opening windows on external elevations in high-risk situations shall be fitted with permanent grills.

9.12 User Security Training and Sensitization

All aspects of ICT security will be incorporated into formal staff induction procedures for all new staff members and be conveyed to existing staff members on a regular basis. Similar training for students will occur when they first enrol at the University.

9.13 Asset Management

DICTS will maintain an asset inventory of all hardware and software, acquired by the university, and will define asset ownership and classification in order to achieve and maintain appropriate protection of organizational assets.

9.14 Information Security Incident Management

- i) DICTS will implement mechanisms for reporting and recording security incidents, monitoring them and learning from them, with the aim of implementing improvements to minimize the impact of incidents.
- ii) The security logs and audit trails will be backed up in all scheduled system backups.
- iii) All Users will be made aware of the procedures for reporting an incident and be required to report any observed or suspected incidents as quickly as possible to the correct authority. A formal reporting procedure will be established together with an incident response procedure.

9.15 Periodic Management Review

- i) Regular auditing procedures will be carried out on all computer systems to check for conformance to this policy and to satisfy the requirements of the University's internal and external auditors. The depth and regularity of each level of an audit should be outlined in the system procedures manual SOP.
- ii) DICTS will periodically review the adequacy of information system controls as well as compliance with such controls.
- iii) DICTS are also responsible for the maintenance of the security measures

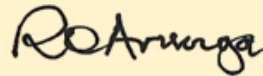
documented in each system's security plan and will conduct regular checks to ensure that the measures are being followed.

10.0 REVIEW OF THE ICT POLICY

The ICT policy shall be reviewed to conform to the university's requirements as necessitated as follows:

- i) To accommodate the fast-changing ICT environment, the policy shall normally be reviewed after THREE years or as/when the need arises;
- ii) When there is a significant change in the university's systems and procedures;
- iii) When there is a major institutional strategy change;
- iv) When there is a change in the prevailing IT standards and guidelines and technologies.

THIS ICT POLICY IS EFFECTIVE FROM THIS 15TH DAY OF APRIL 2019.



COUNCIL CHAIRPERSON



CONTACT:

Technical University of Mombasa (TUM)
Tom Mboya Street Tudor,
P. O. Box 90420 - 80100,
Mombasa - Kenya.

Tel: (254) 41-2492222/3,
Fax: (254) 41- 2495632,
Mobile: (+254) 0733 -955377 | 020 8095365 | 020 8095368 | 020 8095371
E-mail : vc@tum.ac.ke
Website: www.tum.ac.ke



TUM IS ISO 9001: 2015 CERTIFIED

A Centre of Excellence