



WI-1-1-043

# TECHNICAL UNIVERSITY OF MOMBASA

*A Centre of Excellence*

## SECURITY & SAFETY POLICY



TUM IS ISO 9001: 2015 CERTIFIED



# TECHNICAL UNIVERSITY OF MOMBASA

---

# SECURITY & SAFETY POLICY

---

*Issue No. 1*

*Revision No. 0*

*April 2021*

---

**TABLE OF CONTENTS**

PREFACE..... 5

FOREWORD ..... 6

ACKNOWLEDGEMENT ..... 7

DEFINITIONS ..... 8

ABBREVIATIONS AND ACRONYMS..... 9

EXECUTIVE SUMMARY ..... 10

1.0 INTRODUCTION ..... 11

1.1 Citation..... 11

1.2 Vision ..... 11

1.3 Mission..... 11

1.4 Core Values ..... 11

1.5 Motto ..... 12

1.6 Policy Statement ..... 12

1.7 Guiding Principles ..... 12

1.8 Policy Objectives..... 12

1.9 Legislative and Administrative Instruments ..... 13

1.10 Scope/ Applicability ..... 13

1.11 Responsibilities ..... 13

1.11.1 University Management Team..... 13

1.11.2 Vice Chancellor ..... 13

1.11.3 Chief Security Officer ..... 13

1.11.4 Security Department Management Team ..... 14

1.11.5 Security Shift Officers ..... 14

1.11.6 HODs & CODs ..... 14

1.11.7 University Staff..... 15

1.11.8 University Students ..... 15

1.11.9 Visitors..... 16

2.0 SECURITY POLICY ..... 17

2.1 University Security and Safety Advisory Committee..... 17

2.2 Security Reports..... 17

2.3 Security and Safety Standard Operating Procedures..... 18

2.4 University/Private/Public Events..... 18

2.5 Access Management..... 18

2.6 Identity Card ..... 18

2.7 Crime Prevention..... 19

2.8 Security Awareness ..... 19

2.9 Incident Reporting..... 20

2.10 Crime Investigation..... 20

2.11 Perimeter Protection Management ..... 21

2.12 Building Protection Management ..... 21

2.13 Surveillance Management..... 22

2.14 Use of Closed-Circuit Television (CCTV) ..... 22

2.14.1 Reason for Use ..... 22

2.14.2 Locations ..... 23

2.14.3 CCTV Operating Procedures ..... 23

2.14.4 Use of CCTV by the Police ..... 23

2.14.5 Disciplinary Procedures ..... 23

2.14.6 Recorded Images ..... 23

2.14.7 CCTV Policy ..... 24

2.15 Intrusion Detection Management .....24

2.16 Dangerous Weapons .....24

2.17 Trespass.....24

2.18 Property Damage, Misuse, or Theft .....25

2.19 Preventing Workplace & Campus Violence .....25

2.20 Prohibited Behaviour .....26

2.21 Reporting Requirements.....26

2.22 TUM Owned Student Hostels .....26

2.23 Students’ Accommodation Owned by Private Landlords .....27

2.24 Missing Students .....28

2.25 Information Management .....28

2.26 Confidentiality of University Information and Documents.....28

2.27 Privacy.....29

2.28 High Risk Personnel Management .....29

2.29 Risk Management.....29

2.29.1 Risk Analysis.....29

2.29.2 Risk Audit.....29

2.30 Assets and Material Management.....30

2.31 Sexual Assault/Harassment .....30

2.32 Lost and Found .....30

2.33 Parking .....31

2.34 External and Out-Sourced Security Assistance.....31

2.34.1 External Assistance .....31

2.34.2 Out-Sourced Security .....31

2.35 Alcoholic Beverages and Illegal Drugs .....32

2.36 Key Control Guidelines .....32

3.0 SAFETY POLICY.....34

3.1 Fire ..... 34

3.2 Fire Extinguishers.....34

3.3 Fire Detectors and Alarm.....35

3.4 Fire Escape.....35

3.5 Terrorism .....35

3.6 Lightning .....36

3.7 Earthquakes.....36

3.8 Floods.....36

3.9 Road Safety.....36

3.10 Disposal of Hazardous Waste .....36

3.11 Outbreak of Diseases .....36

3.12 Public Disorder (Strikes and Riots).....37

3.13 Chemical, Biological and Radiological Attacks .....37

4.0 IMPLEMENTATION MECHANISMS .....38

4.1 Operationalization of the Policy .....38

4.2 Implementation Framework.....38

5.0 REVIEW OF THE SECURITY AND SAFETY POLICY.....38

## PREFACE

Security and Safety is of paramount importance in all Institutions. Weak security and safety systems have occasioned destruction of property, displacement, injury, loss of lives and trauma. Therefore, providing security and safety for the University will not only help create a conducive environment for Students to learn but also help Staff maximize their potential in executing their functions as well as safeguarding the assets of the University.

The Policy provides the necessary measures and procedures required to make the University secure and safe. Its overriding objective is to enable the University operate a campus security and safety system which is credible and comprehensive.

Lastly, the Policy takes cognisance of the 'Kenya Universities Standards and Guidelines on Security and Safety' and the 'Action Plan on the Management of Security and Safety in Universities in Kenya'. The two documents play a pivotal role in guiding the efforts of modernizing security management and raising the level of security at the University.

The University Council is confident that this Policy will adequately address issues related to security and safety within the Institution. On behalf of the Council, I wish to thank all those who participated in developing this Policy.



**Dr Robert Arunga**  
**Council Chairman**

## FOREWORD

Providing security and safety is complex and multifaceted. It requires a high level of understanding of not only the elements of security and safety but also the procedures which must be followed by Staff and Students to counteract prevailing security threats in the society. This understanding needs to be well articulated and embraced to ensure that security and safety becomes a culture in the University.

The Security Department is charged with the responsibility of ensuring effective implementation of the Security and Safety Policy. Responsibility for personal security and safety rests with all persons who study, work or reside in, or who visit the University campuses. All Students, Staff, visitors, contractors and suppliers have a duty to support the Security and Safety Team to ensure the success of this Policy.

Personal security and safety is everyone's responsibility and cannot be left solely as a matter for the Security Team. Staff, Students and other members of the University Community are strongly encouraged to accurately and promptly report crimes, emergencies, potential threats, or risks to the Security Department for investigation, action, analysis and statistical recording. The University reserves the right to take appropriate action against any person who acts negligently, dishonestly, or commits a crime against the University.



**Prof. Laila U. Abubakar**  
**Vice-Chancellor**



## ACKNOWLEDGEMENT

I would like to take this opportunity to thank all members involved in the development of the Security and Safety Policy. I wish to particularly acknowledge the contribution of the following committee members:

- |                                |                             |
|--------------------------------|-----------------------------|
| 1. Major (Rtrd) Mohamed Morowa | Chief Security Officer      |
| 2. Mr Christopher M. Mgunya    | Senior Security Officer I   |
| 3. Mr. Mathew A. Jakait        | Senior Security Officer III |
| 4. Mr. Stephen M. Kitii        | Senior Security Officer III |
| 5. Ms. Ronce Karue             | Security Officer I          |
| 6. Mr. Robert O. Wafula        | Security Officer II         |
| 7. Mr. Isaack B. Kalama        | Office Administrator        |
| 8. Ms. Serah Okumu             | Deputy Chief Legal Officer  |



**Prof. Joseph Rasowo,**  
**Deputy Vice Chancellor (AFP)**

## DEFINITIONS

“**Staff**” means an employee of Technical University of Mombasa.

“**Stakeholder**” means a person with an interest in Technical University of Mombasa.

“**Standard**” means 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**” means a set of step-by-step instructions compiled by an organization to help Staff carry out complex routine operations.

“**Student**” means a person admitted and registered to pursue an academic programme at TUM.

“**University**” means Technical University of Mombasa.

“**University Community**” means all individuals who have a relationship with or to the University (or had at the time of the incident), including but not limited to Staff, Students, Council members, visitors, suppliers, contractors and cjbjkjkjconsultants.

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

**ABBREVIATIONS AND ACRONYMS**

<b>AA</b>	Academic Affairs
<b>ALARP</b>	As Low As Reasonably Practicable
<b>AP</b>	Administration and Finance
<b>BIDS</b>	Building Intrusion Detection System
<b>CBR</b>	Chemical, Biological and Radiological
<b>CCTV</b>	Close Circuit Television
<b>COD</b>	Chairman of Department
<b>CSO</b>	Chief Security Officer
<b>DVC AFP</b>	Deputy Vice Chancellor Administration Finance Planning
<b>DVC ARE</b>	Deputy Vice Chancellor Academic, Research and Extension
<b>EER</b>	Emergency Evacuation Routes
<b>ICT</b>	Information and Communication Technology
<b>ID</b>	Identity
<b>PIDS</b>	Perimeter Intrusion Detection System
<b>PRI</b>	Partnership Research and Innovation
<b>SFP</b>	Security Focal Point
<b>SOP</b>	Standard Operating Procedures
<b>TUM</b>	Technical University of Mombasa
<b>USSAC</b>	University Security and Safety Advisory Committee
<b>VC</b>	Vice Chancellor

## EXECUTIVE SUMMARY

The Policy addresses the measures that the University shall put in place to draw attention and address the current security needs of the Institution. It also highlights the standard policies in relation to different security access points and what the general Policy shall be with regard to how the University will implement security SOPs. The Policy also supports the formulation of the Security and Safety Committee which will ensure that issues with regard to security are handled promptly and prioritised by the University. Security is an inseparable part of every activity in the University and as an aspect of University life must be handled as responsibly and methodically as are issues concerning quality, productivity, and cost efficiency.

In view of the aforestated, the Security and Safety Policy shall be aligned with the University's Security and Safety Strategic Plan. It shall enhance aspirations of the Vision, Mission, Core Values and commitments of the University.

## 1.0 INTRODUCTION

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

Open access to University campuses is an indispensable ingredient of academic life but is not without risks. The University acknowledges the value of a safe and secure work and learning environment for the well-being and productivity of its Staff and Students. In a bid to provide safe, clean and healthy work environment as enshrined in Articles 41, 42, 69 and 70 of the Constitution of Kenya, 2010, the University will endeavour to put in place the apposite security measures that will reduce security threats to as low as reasonably practicable (ALARP).

The Security and Safety Policy, therefore, seeks to formalise a cohesive and integrated approach to security and safety throughout the University.

### 1.1 Citation

This Policy shall be cited as the **Technical University of Mombasa Security and Safety Policy**.

### 1.2 Vision

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

### 1.3 Mission

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

### 1.4 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:

- a) *Excellence;*

- b) *Integrity and Professionalism;*
- c) *Equity;*
- d) *Teamwork; and*
- e) *Creativity, Innovativeness and Environmental Sustainability*

### **1.5 Motto**

*Jiddu Tajidu* (Endeavour and Achieve)

### **1.6 Policy Statement**

The University will strive to safeguard as far as is reasonably practicable, the security and safety of Students, Staff and other Stakeholders whilst at all University campuses and any other University controlled facilities through implementation of this Policy.

### **1.7 Guiding Principles**

The Policy is guided by the following principles:

- a) Mitigating University risks by reducing threats to as low as reasonably practicable and enhancing rapid recovery efforts to reduce potential consequences from adversaries;
- b) Sensitization of Stakeholders on Security and Safety and strengthening our partnerships with security agencies and other external Stakeholders;
- c) Provision of leadership, guidance and capacity to ensure security concerns are adequately addressed; and
- d) Upholding privacy, transparency, integrity and dignity when engaging members of the University community.

### **1.8 Policy Objectives**

The Policy is guided by the following objectives:

- a) To safeguard the University assets;
- b) To ensure safe working and learning environment;
- c) To provide timely security advice to management;
- d) To ensure and guarantee a security sensitized University Community;
- e) To maintain law and order at the University; and
- f) To liaise with local and national security agencies on matters of mutual interests.

## 1.9 Legislative and Administrative Instruments

The following, but not limited to, legal instruments and Institutional Policies shall be applicable to this Policy:

- a) The Constitution of Kenya, 2010;
- b) The Universities Act, 2012;
- c) Occupational Safety and Health Act, 2007;
- d) The Prevention of Terrorism Act, 2012;
- e) The Kenyan Penal Code, 2012;
- f) The Evidence Act, 2012;
- g) The Public Officer Ethics Act, 2003;
- h) Private Security Regulation, 2016;
- i) TUM Code of Conduct and Ethics, 2017;
- j) Technical University of Mombasa Statutes, 2019;

## 1.10 Scope/ Applicability

The Policy shall apply to all University Community members. The scope of the Policy comprises issues touching on security and safety at TUM.

## 1.11 Responsibilities

The following highlights specific areas of responsibility assigned to various offices in the University:

### 1.11.1 University Management Team

- a) Providing support and resources to aid in the implementation of the Security and Safety Policy; and
- b) Training of security personnel to attain acceptable standards of operation.

### 1.11.2 Vice Chancellor

- a) Ensuring and facilitating the development and planning of security strategy, Policies and Procedures ; and
- b) Overseeing the operation of the Security Department..

### 1.11.3 Chief Security Officer

- a) Developing, documenting and implementing the security strategy, policies and procedures and monitoring their effectiveness and efficiency.;

- b) Ensuring crime cases, breaches in security and Student and Staff disciplinary matters are investigated;
- c) Providing expert and impartial up-to-date advice on security and safety matters; and
- d) Liaising with civil police, emergency services and relevant County Government authorities on matters of mutual interests.

#### **1.11.4 Security Department Management Team**

- a) The team will be responsible for the day-to-day management and implementation of the Security Policy and Procedures;
- b) Monitoring of these Policies and Procedures to ensure their continued effectiveness; delivery of an efficient and effective service to the University;
- c) Management and training of Staff;
- d) Investigation of crime; and
- e) Advice on implementation of security solutions, security hardware, CCTV, intruder alarm installations etc.

#### **1.11.5 Security Shift Officers**

- a) Conducting security duties as defined in SOPs, including the operation of the Central Control Room, CCTV monitoring, responding to all incidents, e.g. fire and intruder alarm activations, disturbances, electrical/mechanical failures, damage to University fabric and lock-outs, on and off the University campus. This could include major incidents affecting the University's business continuity and disaster management.
- b) Patrolling University buildings and campus on foot and in designated patrol vehicles to ensure that the Staff, buildings, contents, Students and other users remain safe and secure, react to and deal with incidents and emergencies that arise.

#### **1.11.6 HODs & CODs**

They have a crucial role in promoting security within their area of jurisdiction. The actual responsibilities will vary according to the location and the nature of the activity taking place.

HODs & CODs should:



- a) Ensure their Staff have access to and are familiar with the Security and Safety Policy;
- b) Ensure that all members of Staff and Students in their Departments understand and exercise their security responsibilities, including the displaying of University Identity cards, and have due regard to University property;
- c) Control access to their Departmental areas by approving the issuance of keys and by authorising Staff to have 'out of hour's access' only when necessary;
- d) Ensure that their Departmental Staff return to the Department any University items issued to them which include but not limited to University identity cards, keys and laptops on their last day of work;
- e) Notify the Security Department of any security risk (including the purchase of expensive equipment etc.) who will advise on any additional security or protection measures; and
- f) Ensure Emergency Evacuation Routes (EER) are located at vantage points in their office areas. The EER to include but not limited to exit/escape routes from each building, assembly areas, location of first aid boxes and fire fighting equipment.

#### **1.11.7 University Staff**

- a) All University Staff (Research Staff, contracted workers, Post-graduate Students, visiting lectures and anyone employed as tutor, supervisor or lecturer on an ad hoc basis) must ensure they are acquainted with the Security and Safety Policy, paying specific consideration to those issues that are applicable to their activities.
- b) They must also cooperate with requests from the Security Team, specifically in emergency or evacuation circumstances and in relation to security procedures. Staff must, at all times, when within the University premises carry their University cards.

#### **1.11.8 University Students**

- a) Safeguarding University facilities;
- b) Following security procedures intended to protect University's property;

- c) Cooperating with the Security Team during emergencies and evacuations;
- d) Adhering to regulations set out in the Students' Handbook;
- e) Having their University cards at all times while on Campus; and
- f) Students residing in the University hostels should follow hostels' procedures and security instructions issued to them.

#### 1.11.9 Visitors

- a) All visitors, including conference delegates, external event attendees and kiosk operators, have a general responsibility to preserve the University facilities whilst on campus and to give due consideration to security issues;
- b) In particular they must follow security procedures designed to protect University property and where issued, wear their visitors' badge at all times; and
- c) Visitors must follow instructions from the Security Team or from their host Department, particularly in emergency situations.

## 2.0 SECURITY POLICY

### 2.1 University Security and Safety Advisory Committee

The University shall establish a cross functional University Safety and Security Advisory Committee (USSAC) whose mission is to advise on plans, strategies, coordination of all safety, security and emergency issues for the University.

The Vice chancellor shall be the Chairperson of the USSAC and in his/her absence the person holding brief shall assume the duties of the Chairperson. The Vice Chancellor shall appoint a committee comprising the following:

- |                              |           |
|------------------------------|-----------|
| 1. DVC ARE                   | Member    |
| 2. DVC AFP                   | Member    |
| 3. All University Registrars | Member    |
| 4. Corporation Secretary     | Member    |
| 5. Dean of Students          | Member    |
| 6. Finance Officer           | Member    |
| 7. HR Manager                | Member    |
| 8. TUMSA Chairman            | Member    |
| 9. Chief Security Officer    | Secretary |

The Vice Chancellor may, where appropriate, co-opt any person to attend the deliberations of the USSAC. Notice of the USSAC meeting accompanied by an agenda shall be sent to members through email fourteen (14) days prior to the meeting. Two-thirds (2/3) of the total number of the members present during the USSAC meeting shall be deemed to form a quorum exclusive of co-opted members.

In the event that a special USSAC meeting is necessary, the Secretary in consultation with the Chairperson, shall convene such special meeting by a notice in writing, stating the agenda to be deliberated.

### 2.2 Security Reports

TUM shall keep crime statistics compiled from University security reports. These reports detail the types and number of crimes that occur on and around the University as reported by the University Community to the Security Department, who will thereafter prepare a report for management, consumption and decision making.

### 2.3 Security and Safety Standard Operating Procedures

The University shall make standard security and safety procedures in operational undertakings of the security function. The security aspect of operational procedures shall be determined between line management responsible for that operation and the Security Team or local SFP.

### 2.4 University/Private/Public Events

All public and private meetings and or events which are to be conducted within the University shall be approved by the Registrar AP in consultation with the Security Department. The Security Department, therefore, shall determine the appropriate measures to be adopted within the University at all times.

Political oriented rallies or gatherings shall not be held within the University premises at any time.

### 2.5 Access Management

- a) Open access to University campuses is a requisite element of academic life but is not without risks. It is, therefore, in that spirit that TUM main gates and premises shall be protected on a 24-hour basis by the deployment of security personnel and enhanced by an automated access control system. Entry to TUM facilities shall hence be controlled.
- b) University Staff, Students and visitors shall enter TUM through designated and controlled access points after undergoing security checks as required.
- c) Accompanying of visitors by their hosts shall be at the discretion of the University Security Staff.
- d) Vehicles and bicycles shall be issued with security identification tags after the normal security checks have been conducted and the same to be surrendered on exit.

### 2.6 Identity Card

- a) In the interest of safety and security, TUM shall operate an identity card scheme that requires all Staff, Students, contractors, suppliers and visitors to wear and have clearly visible identity cards/passes at all times whilst on its premises. The ID card must be displayed using the coloured TUM lanyard and holder issued. Clips may be used in circumstances where a lanyard poses

a potential health and safety risk e.g. workshops. Loss and damage of the card will attract a replacement fee.

- b) Identification cards are not transferable.
- c) The Security Department shall be responsible for issuance of Staff and Student identity cards.
- d) Staff and Students who attempt to obtain University identity cards under false pretence or who fail to show University identity cards when requested by an appropriate member of the University may be denied access to University facilities and are subject to disciplinary action in accordance with the Student and Staff disciplinary guidelines.

## 2.7 Crime Prevention

- a) The University community shall report all crimes at the institution to the duty room office or any other available Security Officer.
- b) The University will approach crime prevention through intelligence gathering, incident reporting, crime investigation, security awareness and training.

## 2.8 Security Awareness

- a) Personal valuables should be kept safely and never left unattended.
- b) Windows in offices must be closed and secured on departure where locks are fitted. Curtains or blinds in these rooms should be closed at dusk and lights (except security lighting) should be turned off when leaving.
- c) Laptops and other portable Information Technology and Audio Visual equipment should be kept safe when not in use.
- d) All incidents of crime on University premises, real and suspected, must be reported to the Security Team.
- e) Security Officers will conduct patrols on Campus, to aid in the identification of security risks, monitor public safety and act as a deterrent against crime.
- f) Staff members and Students who bring visitors to the University shall be personally responsible for the visitors' conduct, wellbeing and safety.

## 2.9 Incident Reporting

It is the responsibility of all University community to report all activity, suspected or real, of a security/safety nature. Incident reporting is crucial to the identification of patterns of criminal activity and risk analysis. It permits investigation and recommendations to be made to prevent a recurrence. Comprehensive reporting of incidents provides an accurate picture of the level of crime throughout the University and thus ensures that adequate resources are provided to combat that crime.

- a) All incidents of a security/safety nature on Campus should be reported in the first instance to Security Control 0733955377/0722955377 ext. 6999 (24 hours) or Police Emergency numbers 999, 911 or Mombasa County Police Control room 0789-999395.
- b) All incidents of a security/safety nature at the Hostels should be reported in the first instance to Residence Janitor or Security Officer on duty 0733955377/0722955377 ext. 6999 (24 hours) or Police Emergency numbers 999, 911 or Mombasa County Police Control room 0789-999395.
- c) The victims in all reported cases of all crimes, but in particular assault, indecency, fraud, theft (including car or cycle theft) and burglary are advised to inform both the Security Team and Police. In case of doubt, advice on Police involvement may be sought from the Chief Security Officer.
- d) Any Police involvement on University premises is to be notified to the Chief Security Officer to enable effective management of any subsequent actions within the University jurisdiction.
- e) Where appropriate, in addition to any Police involvement in alleged criminal offences by Staff, Human Resources will be informed by the Chief Security Officer for possible consideration under the University's disciplinary procedure.

## 2.10 Crime Investigation

All crimes that occur on University premises will be investigated appropriately to prevent re-occurrence and aid crime prevention. The CSO or other members of the Security Team as delegated will carry out internal investigations of security related

incidents, producing written reports for circulation where necessary and providing follow up crime prevention advice.

### **2.11 Perimeter Protection Management**

The University shall have a site perimeter fence to clearly demarcate its property. The extent of perimeter protective measures shall be in accordance with the nature of the University facility. The security risk analysis shall be determined by the Security Department. Where a secure perimeter is required, fencing shall be a minimum of 2.4 metres high with anti-climb hostile topping extending the fence to 3 metres overall. Fences shall be topped with coiled razor wire. Walls shall be topped with a rotating spike defence.

Fencing should be buried at the base wherever practicable. Where not possible, gaps between the bottom of the fence and ground shall not exceed 5 cm. Storm drains, culverts, pipelines, utility tunnels, etc. in excess of 600 cm<sup>2</sup> which pass through or under the perimeter fence shall be fitted with security bars or a grille to be resistant to intrusion. A properly equipped gatehouse shall be established on the perimeter to control access.

### **2.12 Building Protection Management**

The University will put in place the following baseline security measures for its premises in order to reduce potential threats:

- a) Ensuring strong external doors which are resistant to removal or penetration;
- b) The use of strong locks with multiple locking points on external doors;
- c) Appropriate protection for windows up to 5m from ground level;
- d) Proper Illumination;
- e) Internal locking for out of working hours separate from working hours;
- f) Building intrusion detection systems deployed on doors and windows (shell protection), to protect interior building spaces (volumetric protection), and specific objects (target protection);
- g) CCTV surveillance; and
- h) An emergency plan.

### 2.13 Surveillance Management

The University shall put in place the following surveillance means and methods for the purpose of gathering real time information that will support security operations function:

- a) CCTV;
- b) Foot patrols(with dogs);
- c) Vehicle patrols; and
- d) Watch towers.

### 2.14 Use of Closed-Circuit Television (CCTV)

#### 2.14.1 Reason for Use

The use of Closed-Circuit Television (CCTV) has been widely recognised as an effective tool in the fight against crime, both in its prevention and detection. Moreover, the Government of Kenya recognises the utility of surveillance cameras in national security and law enforcement. In this regard, these security controls have become an indispensable part of detection, prevention, investigation and prosecution of crime. The surge in crime has compelled various institutions and individuals, both in the private and public sector, to use CCTV cameras to deter, mitigate, and disrupt potential security threats.

The **National CCTV Policy** provides standard guidelines for the installation, operation and management of CCTV systems. The University shall use CCTV systems around the campus covering many of the public access points, sensitive offices, hostels, lecture halls and adjacent areas. CCTV shall be installed, with the objective of assisting in the provision of a safe and secure environment. This objective shall be met through the monitoring of the CCTV system so as to:

- a) Assist in the prevention and detection of crime;
- b) Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public disorder; and as an aid to public safety;
- c) Assist in the University's Emergency Procedures;
- d) Assist with traffic management;
- e) Promote safer communities; and
- f) Provide a training facility.



All these shall be carried out in a manner, which is consistent with the **National CCTV Policy**.

#### **2.14.2 Locations**

The system shall consist of PTZ and static cameras installed around the University. The main Control Room shall be located at the Main Campus, while one other Control Room shall be located at Kwale, Mabokoni Campus.

#### **2.14.3 CCTV Operating Procedures**

The procedures shall ensure the concerns of Confidentiality, Integrity and Ethics are not compromised. The intention is to guarantee that the information obtained from the CCTV will give public confidence, that the rights of individuals are being fully protected. Access to the CCTV monitoring and recording systems in the Control Room is strictly controlled and is limited to duty security Staff, CCTV operator or authorised management. All these will be done in synchronization with the **National CCTV Policy**.

#### **2.14.4 Use of CCTV by the Police**

In general, the Police should not require access to (nor be allowed access to) University CCTV systems except under the following circumstances:

- a) Emergencies or investigation of serious incidents;
- b) Identification of offenders; and
- c) Liaison and training purposes, by prior arrangement with the Chief Security Officer as authorised by the Vice Chancellor.

#### **2.14.5 Disciplinary Procedures**

On occasions, it is necessary to use CCTV as part of disciplinary investigation and source of evidence. Footage to support such an investigation can be accessed to support investigations with the authorisation of the Chief Security Officer who shall consider the request and ensure it complies with the objectives of the system as detailed under "Reason for Use" above.

#### **2.14.6 Recorded Images**

Images shall be kept securely and in line with the requirements of the National CCTV Policy.

### **2.14.7 CCTV Policy**

More information on CCTV management is found in the detailed CCTV Policy.

### **2.15 Intrusion Detection Management**

As a standard practice, the University is required to employ two categories of intrusion detection system: Perimeter Intrusion Detection Systems and Building Intrusion Detection Systems. The Perimeter Intrusion Detection System (PIDS) uses dedicated electronic systems which detect and warn of an intrusion or attempted intrusion, through an external line of protection like a perimeter wall or fence. Building Intrusion Detection Systems (BIDS) shall be geared towards a provision of detection towards detecting breakthrough (shell), detecting an unusual energy pattern in a monitored space (volumetric), or detecting an adversary interfering in some way with a specific object (target) in a building in the University.

### **2.16 Dangerous Weapons**

Possession of any type of weapon for example, firearms, explosives, machetes, knives, crowbars, clubs, whips, etc. on any TUM facility is strictly prohibited. This prohibition applies to all facilities owned, leased or otherwise controlled by TUM and whether academic, residential or otherwise. Failure to comply with this Policy may lead to disciplinary action by the University (up to and including, in the case of a Student, suspension or expulsion and, in the case of Staff, termination of employment) and also may result in criminal prosecution. In addition, the University reserves the right to confiscate the weapon and hand it over to the relevant authority. This Policy applies to all members of the University community. Any exceptions shall be sanctioned by the Vice Chancellor and/or the Chief Security Officer otherwise licensed weapon holders shall surrender the same to Security at the gate for safe custody and returned to the owner on exit. The necessary handover/takeover forms shall be duly filled.

### **2.17 Trespass**

TUM is a public Institution of higher education that is open to the general public. However, the University has the ability to determine the expectations and parameters for an individual's presence on any University property. The University

retains the right to restrict access to University property due to safety consideration to its University community.

Any University community member whose behaviour poses a threat to the safety of persons or property or who is considered a serious disruption to the educational or working environment of TUM may be asked by an appropriate University personnel to leave any University location until otherwise notified. Any person who does not comply may be subject to trespass and/or arrest by the University security operatives or any other University member and action taken in accordance with the applicable Act.

### **2.18 Property Damage, Misuse, or Theft**

University property and services may be used for University, public or and private functions during the hours and at the locations that have been approved. Inappropriate use of University property or services may result in disciplinary action against the Staff or Student or replacement/repair for other University Community Members.

Attempted or actual theft or damage/vandalism of University property or the property of Staff, Students or any other University community members are prohibited. In addition, knowingly possessing or utilizing stolen property, or being a bystander to damage or vandalism is a violation of this Policy. Students or Staff reported for property damage and/or theft are subject to one or more of the following:

- a) Prosecution for criminal charges;
- b) Assessment of the costs for repair, replacement or recovery of the property;  
and,
- c) Disciplinary action.

### **2.19 Preventing Workplace & Campus Violence**

The University strives to provide a safe and secure working environment to its Staff and Students. Verbal threats, threatening behaviour, or acts of violence by Staff, Students or other members of the University community shall not be tolerated. Persons found to have violated this Policy are subject to appropriate disciplinary action. Arrest and criminal prosecution by the Police are also possible.

Reported threats and acts of violence shall be investigated by the University.

### **2.20 Prohibited Behaviour**

The following behaviours are strictly forbidden in the University:

- a) Using threatening, intimidating, or abusive language and/or gestures;
- b) Using or possessing firearms, explosives, knives, or any other type of weapon;
- c) Stalking or similarly harassing behaviour toward Staff, Students, or Visitors;
- d) Destroying or damaging University property, computer files, and/or other acts of workplace sabotage;
- e) Assaulting or physically attacking another person;
- f) Verbally threatening to harm another person or destroy property;
- g) Possessing or consuming alcohol and illegal drugs;
- h) Working under the influence of alcohol or illegal drugs;
- i) Illegal parking within the University;
- j) Illegal behaviour using TUM internet connection;
- k) Taking part in unauthorised commercial activities within the University;
- l) Gambling;
- m) Seeking gifts or favours of any kind for work done;
- n) Any other behaviour that affects the security and safety of the University.

### **2.21 Reporting Requirements**

Staff, Students and other University community members are required to notify Security immediately if they observe the following:

- a) A life-threatening situation that is in progress (physical confrontation, robbery, etc.)
- b) An act of violence or threat in the workplace, hostels or on campus property; and
- c) Any action or conduct that is imminently threatening or violent, or that has the potential to become threatening or violent.

### **2.22 TUM Owned Student Hostels**

TUM Students' hostel rooms are their private areas of residence. All Staff, and Students, should respect this right to privacy. From time to time however, it may be necessary for University accommodation officers, Janitors or member of Staff to gain

access to Student rooms as a matter of urgency, whether or not they are present. Whenever practicable and reasonable, information will be given in advance of the need to gain entry into the accommodation.

The University shall:

- a) Develop and publish standard operating procedures to guide access to such premises considered private in the event of posing or thought to cause breach of security and safety of the occupants and other residents of the University.
- b) Ensure each Student signs an Agreement relating to the occupation of his/her room and to be retained at the Accommodation office.
- c) Expect all Students to have read and abided by the terms and conditions of the room occupancy.
- d) Prepare a Student Accommodation Handbook and a dedicated Web Portal on Student accommodation.
- e) Once every year conduct a survey to establish effectiveness of the security and safety measures in Student hostels and collect views to enhance such measures.
- f) Require that Staff working in the Students hostels be identified by the uniform they wear and Staff Identity Cards.

Visitors, contractors and other guests shall be issued with identification passes if they need to access Student hostels.

In instances where the access to Students' rooms is un-announced the Student will be briefed on reason for accessing their room/premises.

### **2.23 Students' Accommodation Owned by Private Landlords**

Due to limited bed space in TUM owned hostels, some Students seek accommodation owned by private landlords. The University shall:

- a) In collaboration with the community and local security agencies establish the viability of Student accommodation.
- b) Require the Students to register their accommodation premises with the University Security Department and the Dean of Students' office.
- c) Ensure the owners of the Student accommodation premises to declare the particulars of Students residing in their premises.

- d) Have regular meetings with the local administration and other security agencies for the welfare and security of the Students.
- e) NOT be held responsible for the security and safety management of hostels owned by private landlords.

### **2.24 Missing Students**

It is the obligation of TUM to actively investigate any report of a missing Student who is enrolled at the University. If a member of the TUM community has reason to believe that a Student is missing, all possible efforts are made to locate the Student to determine his or her state of health and well-being. This effort is coordinated by the TUM Security Department, in collaboration with the Dean of Students and the missing Student's family and friends.

If not located within 24 hours, appropriate family members, associates, or a University officials will make an official missing person report to the nearest Police Station. TUM Security Department in conjunction with the office of the Dean of Students will cooperate with, aid, and assist the primary investigative agency in all ways prescribed by law.

### **2.25 Information Management**

Staff, Students and suppliers of TUM shall follow ICT and information security procedures. At the end of the working day all University sensitive information will be locked away or encrypted. During the working day, computers will be secured by use of passwords. Out of working hours, they will be shut down and be properly secured. Non-University, non-encrypted portable flash memory devices shall be prohibited from use in University computers. All University sensitive waste will be securely disposed of by cross-shredding and implementation of a clear desk Policy. More information on ICT is found in the TUM ICT Policy.

### **2.26 Confidentiality of University Information and Documents**

TUM requires all members to safeguard classified and confidential information. This includes (but not limited to) Students' academic records, internal classified University documents, patents and copyrights and trademarks (intellectual property).

## 2.27 Privacy

TUM shall comply with all the national laws, statutes and regulations governing individual privacy in its endeavour to maintain a safe and secure learning and working environment.

## 2.28 High Risk Personnel Management

TUM shall provide adequate additional appropriate security for senior managers as and when need arises such as during emergencies and high security alerts. The Security Team should come up with an evacuation plan for the University senior management, Senate or Council in times of calamities, unrest, or emergencies.

## 2.29 Risk Management

### 2.29.1 Risk Analysis

TUM shall carry out risk analysis for all its facilities on an annual basis. Where possible, quantitative assessments (to measure the financial cost of potential loss) shall be made. The process is collaborative and shall involve representation from across the University. The SRAM (Security Risk Analysis Matrix) shall be the standard tool used, and the results of the process shall feed into the strategic risk management plan, and cascade locally into risk management action plans.

All security risks will be identified, documented and managed to ALARP (As Low As Reasonably Practicable). Vulnerabilities that present a life-safety hazard shall be mitigated in accordance with legal, regulatory, University best-practice and moral responsibilities, with attention given to litigation exposures. Contingencies shall also be in place for high impact risks.

### 2.29.2 Risk Audit

Risk audit is an important tool that is used to verify whether all security measures which are supposed to be in place are in fact in place, functioning and documented correctly. It examines and documents the effectiveness of risk responses in dealing with identified risk and their root causes, as well as the effectiveness of the risk management.

To protect Staff, Students, assets and other TUM community members, therefore, a quarterly risk audit for all TUM facilities shall be conducted.

### **2.30 Assets and Material Management**

TUM shall ensure that its assets are properly coded and recorded and that their movement is closely monitored. Procedures on the same shall be developed.

### **2.31 Sexual Assault/Harassment**

TUM shall comply with all the national laws, statutes and regulations concerning sexual assault and harassment. This may include but not limited to sexual harassment; sexual violence; gender based bullying; hazing; stalking; domestic violence and dating violence. For more information refer to the TUM Sexual Harassment Policy.

### **2.32 Lost and Found**

The Lost and Found Policy intends to ensure that items reported lost or found on University premises are properly accounted for and, in the case of items found, returned to their rightful owner or disposed of by the University in accordance with the laid down procedures. TUM assumes no responsibility whatsoever for the care and/or protection of any personal belongings left unattended on University premises and for loss, under any circumstances, including theft, vandalism, or malicious mischief of such belonging. TUM Security Department is designated as the central repository and controlling agency responsible for lost and found property for the University. All found items shall be turned into TUM Security Department for identification of the rightful owner if possible.

All found items turned into the TUM Security Department will be logged as found and posted monthly on the TUM web (<https://www.tum.ac.ke>) and in the designated noticeboards. All unclaimed items will be held for a period as prescribed in the Unclaimed Financial Asset Act No. 40 of 2011.

Any individual making a request on recovery of a lost item must present documentation, picture identification or any other proof of ownership, and/or a description of the item before it is returned to them. If the item has no identification on it but the individual can describe or open (log in) it (i.e. phone, tablet, laptop), the item will be returned once the transfer of ownership form has been completed.



### 2.33 Parking

- a) TUM seeks to provide and maintain a safe campus environment for the vehicular, pedestrian, and bicycle traffic. Parking and driving regulations are created and enforced to establish a climate of safety and order. Penalties may be issued for failure to observe these regulations and in some cases the vehicle may be towed from the campus at the owner's expense. The University shall use the existing traffic laws and regulations to enforce the Policy.
- b) All motorized vehicles and bicycles parked or operated within the University campuses by Students and Staff must be registered with the TUM Security Department and display a current Gate Pass. Double/wrong parking is prohibited and motorized vehicles and bicycles not displaying a current gate pass may be towed from the campus at the owner's expense and/or may incur a fine.
- c) TUM will endeavour to provide ample parking for vehicles and racks for bicycles under shade structures which will be covered by CCTV cameras on a 24-hour basis. All bicycles must be secured to these racks.
- d) Campus speed limit allowed is 10km/hr unless otherwise stated. Vehicles/motorbikes and bicycles are parked at the University at the owners' risk.

### 2.34 External and Out-Sourced Security Assistance

#### 2.34.1 External Assistance

In order to promote security awareness and seek assistance in dealing with criminal incidents, the University Security Department shall maintain a close contact with the local security agencies and other relevant authorities. The University Chief Security Officer shall liaise with such agencies and relevant authorities on behalf of the University on matters of mutual interest.

#### 2.34.2 Out-Sourced Security

To create a security-compliant environment for the University community, TUM shall contract security services from a reputable registered private security firm in Kenya in accordance with the Public Procurement and Asset Disposal Act, 2015 and the Private Security Regulation Act, 2016.

### 2.35 Alcoholic Beverages and Illegal Drugs

- a) TUM is committed to the well-being of each member of the University community. In order to further Student learning and promote the University's academic mission, TUM fosters an environment of personal responsibility and respectful citizenship. This means that all members of the University community have a shared responsibility in creating and maintaining an alcoholic and drug-free environment.
- b) All members of the University community are strictly prohibited from the use, consumption, possession, manufacture, sale, furnishing and/or distribution of alcoholic beverages, controlled substances and illegal drugs on any University premises or at any of its activities.
- c) Violation of this Policy will amount to disciplinary action against the offender and shall lead to legal consequences.

### 2.36 Key Control Guidelines

These guidelines shall be used for key control:

- a) All keys, electronic access cards and access codes are the sole property of TUM and will be issued to Students and employees based on their needs for access.
- b) Procedures shall be in place to control the issuance of keys issued to authorized persons once they sign in the key movement register.
- c) Registers shall be kept documenting all keys issued and returned. The registers shall be monitored on a daily basis.
- d) Keys shall be signed back in by any authorized person from the respective Department.
- e) Lost, stolen or unreturned keys shall not be replaced until a report has been filed with the University Security Department who shall in turn liaise with the Estate Department to replace the same immediately. Replacement keys will only be issued after an investigation of the loss. The cost of replacement will be charged to the School, Department or individual concerned.
- f) Procedures shall be implemented to control duplication of keys and to provide for a periodic rotation of replacement of locks.

- g) Persons leaving the University or transferring to another Department are to return their keys directly to their Departmental Office. They should not pass keys directly to their replacement.
- h) No Staff shall change locks or duplicate keys for their office without the knowledge and consent of the Security Department.
- i) All keys shall be kept at the Security Department for monitoring.

### 3.0 SAFETY POLICY

#### 3.1 Fire

Fire is probably the biggest danger in multiple-occupancy buildings. This could arise from unsupervised or dangerous electrical equipment, whether in offices or the rooms of individual Students. The University shall:

- a. Expect Staff and Students to be and always remain vigilant to pick, identify or detect fire and fire threats
- b. Require that all personal electrical items are safe and kept under surveillance when in use.
- c. Develop fire regulations and procedures

The University shall from time to time make arrangements to ensure Staff; Students and visitors are aware of potential dangers of fire. They shall be required to follow these guidelines:

- a) Familiarise themselves with escape routes and assembly points;
- b) No blocking of fire escapes;
- c) No leaving or storing personal belongings in corridors or hostel rooms;
- d) Use of candles or other naked flames is expressly forbidden;
- e) Not hanging of electrical posts or lampshades or holders in hostel rooms or offices;
- f) Cooking in hostel rooms and offices (including the use of sandwich makers, toasters or similar) is prohibited;
- g) Keeping flammable materials away from heat sources such as kettles, blow dryers, radiators, light bulbs, and any supplementary heating provided to Students; and
- h) Tampering with electrical circuits is prohibited and reporting of live wires without proper insulation must be done immediately to the Security Officer or Janitor immediately.

#### 3.2 Fire Extinguishers

Fire extinguishers are fitted in communal areas to assist Students and Staff to deal with fires. The University views with concern any interference with fire safety equipment, which is provided and maintained for the safety of all members of the

University. This includes letting off, or tampering with, fire extinguishers (except in the event of a fire), the jamming open of fire doors, the improper use or removal of keys to emergency exits, and interference with, or improper use of, fire escapes and fire exits. Tampering with fire safety equipment is an offence.

### **3.3 Fire Detectors and Alarm**

Fire detectors and alarms shall be fitted in some sections of the University buildings and infrastructure. Staff, Students and visitors should avoid leaning up against such devices, or in any way causing damage.

Each alarm which goes off **MUST** be treated by all as a potential fire, and Staff and Students are required to evacuate all the buildings. Each year Management shall conduct a test-drill of these detectors and alarms to assess their effectiveness.

### **3.4 Fire Escape**

Each building shall have its means of escape clearly marked. The escape routes are in the form of the open staircases for faster speed of escape and cater for the spread of smoke. Escape routes shall be kept clear of personal property, furniture and other items. Regular inspections will be made of these areas, and action taken regularly to ensure escape routes are not blocked.

It is essential that all members of the University understand the actions that need to be taken in the event of a fire alarm. Fire instructions shall be provided behind the door in each Student room and other vantage locations. Staff, Students and visitors have a responsibility to know their escape routes, fire exits and fire assembly point.

### **3.5 Terrorism**

The University shall ensure that:

- a) Suspicious activities and items in the University are reported promptly to the Security Department;
- b) Security procedures are heightened at the entry/exit points of the University;
- c) Staff and Students undergo life skills training on safety measures in the event of terror attacks;
- d) Information is collected on security risks in regard to impending terror attacks; and

- e) Classified University information is only shared as and when necessary and by authority of the Vice Chancellor.

### **3.6 Lightning**

The University shall install lightning arresters at all University high-rise buildings and train Staff and Students on safety procedures in the event of lightning.

### **3.7 Earthquakes**

The University shall ensure that all its buildings conform to the national building guidelines related to earthquakes.

### **3.8 Floods**

The University will ensure that a proper drainage system is in place in all University premises.

### **3.9 Road Safety**

The University shall:

- a) Ensure that all its vehicles are properly serviced and are roadworthy;
- b) Ensure that in University roads, road signs are put at designated points;
- c) Ensure that the speed limit of vehicles driven on University roads is marked and maintained at 10km/hr;
- d) Ensure that its drivers comply with the provisions of the Traffic Act with regard to road safety; and
- e) Encourage Students and Staff to use designated road-crossing points.

More information on Road Safety is found in the TUM Road Safety Policy.

### **3.10 Disposal of Hazardous Waste**

The University will ensure that disposal of hazardous materials is done in an environmentally sustainable manner and in line with the applicable environmental laws.

### **3.11 Outbreak of Diseases**

The University shall:

- a) Train Staff and Students on causes of diseases and measures to be taken to prevent and control outbreaks of diseases,
- b) Ensure that adequate medical Staff are deployed and equipments put in place to curb outbreaks of diseases, and

- c) Encourage Staff and Students to maintain high levels of hygiene within the University.

### **3.12 Public Disorder (Strikes and Riots)**

The University shall ensure appropriate strikes/riots preventive mechanisms are put in place to adequately address Students and Staff needs. In the event such strikes/riots occur, the University shall deploy enough security personnel to contain the situation and seek support from external security agencies if things get out of hand.

### **3.13 Chemical, Biological and Radiological Attacks**

TUM shall design and implement proactive and responsive measures to mitigate against CBR threats. This should include principles of building design for risk reduction related to chemical, biological, and radiological threats.

## 4.0 IMPLEMENTATION MECHANISMS

### 4.1 Operationalization of the Policy

TUM will operationalize this Policy through formulation of Standard Operating Procedures.

### 4.2 Implementation Framework

The University Management under the stewardship of the VC shall be responsible for implementing this Policy. The University Council shall play a pivotal role in monitoring and evaluation of the same.

## 5.0 REVIEW OF THE SECURITY AND SAFETY POLICY

This Policy shall be reviewed after every three (3) years or when the need arises.

**THIS POLICY IS EFFECTIVE FROM THIS 14<sup>TH</sup> DAY OF APRIL 2021.**

SIGNED..........

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](mailto:vc@tum.ac.ke)

Website: [www.tum.ac.ke](http://www.tum.ac.ke)



TUM IS ISO 9001: 2015 CERTIFIED

*A Centre of Excellence*