KNUST POLICY 0037

Kwame Nkrumah University of Science and Technology, Kumasi

KNUST Security POLICY

KNUST SECURITY POLICY

KWAME NKRUMAH UNIVERSITY OF SCIENCE
AND TECHNOLOGY, KUMASI-GHANA

**QUALITY ASSURANCE AND
PLANNING OFFICE**

ISBN: 978-9988-2-8487-9

Quality Assurance and Planning Office
Vice-Chancellor's Office
Kwame Nkrumah University of Science and Technology
KNUST, Kumasi
PMB UPO, Kumasi-Ghana

Tel: +233 322060319

Email: info.qapo@knust.edu.gh

Layout Design by
Frank Boadu, University Press, KNUST

Cover Design
Francis K. N. Nunoo, Department of Publishing Studies, KNUST

FOREWORD

The Kwame Nkrumah University of Science and Technology, Kumasi has a mission to advance knowledge in science and technology through creating an environment for undertaking relevant research, quality teaching, entrepreneurship training and community engagement to improve the quality of life. In order to achieve this mission, there is the need to have a Policy on Security.

Protecting the University from security vulnerabilities or incidents is vital to ensuring that it meets its strategic objectives. Security measures and policies are, therefore, not only inevitable but highly desirable to maintain the University's reputation as a safe, secured and conducive environment for teaching and learning. It is in the light of this that management saw the need for the development of this Policy.

The Security Policy has been developed to ensure that security issues are managed to conform with the University’s vision, mission, and strategic plan. This Policy seeks to ensure that all members of the University community, including students and other clients, staff, visitors, and contractors, are provided with a safe, secure, and friendly environment to function.

The University is grateful to all those who ensured the initiation, development, and approval of this Policy.

PROFESSOR (Mrs.) Rita Akosua Dickson
VICE-CHANCELLOR
KNUST

ACKNOWLEDGEMENT

As part of the strategic planning mandate of the Quality Assurance and Planning Office (QAPO), University policies are initiated and proposed for approval by the Academic Board.

The Quality Assurance and Planning Office is grateful to the Committee consisting of Lt. Col. Richard Cobba-Eshun (Rtd), Head of University Security Services, Chairman, Professor Francis Kofi Ampong, Hall Master of Republic Hall and Representative of the Committee of Hall Administrators (CoHA), Mr. Kwabena Jnr. Yeboah-Asuama Esq., Legal & Welfare Division, Supt. Mr. Maxwell Antwi, District Commander, KNUST District Police Command, Members and Mrs. M. V. D. Appiah-Castel, Secretary who provided inputs for the development of this Policy. They are deeply appreciated for their enormous contributions.

Also, we are grateful to the experts, students and student leaders who were consulted in developing this Policy.

We are equally indebted to the staff of QAPO and the Publications and Documentation Unit of the University Relations Office (URO) who facilitated the technical review and publication of this Policy.

Lastly, we wish to appreciate the contributions of all staff of the University who contributed in diverse ways to the development and approval of this Policy.

PROFESSOR Jerry John Kponyo
DEAN, QUALITY ASSURANCE AND PLANNING OFFICE
April, 2022

OFFICIAL COPY CAN BE OBTAINED FROM:
Telephone Number: 0322060319
E-mail: info.qapo@knust.edu.gh

Contents

1.0 INTRODUCTION

The Kwame Nkrumah University of Science and Technology (KNUST) is a world-class academic centre of excellence, located inside the city of Kumasi, the Ashanti Regional capital. Generally, the University advances knowledge in the Sciences, Technology, Arts and in the Humanities through creating an environment for undertaking relevant research, quality teaching, entrepreneurship training and community engagement to improve the quality of life. KNUST currently has 6 Colleges, 14 Faculties, 4 Schools, 14 Research centres, and 98 Departments. The University also has a satellite campus at Obuasi, in the Ashanti region.

The University is governed by a 15-member Governing Council which is responsible for policy direction. The Vice-Chancellor who is a member of the Governing Council is responsible for the implementation of policies. Currently the University has total staff strength of 3,277 (teaching and non-teaching) with 79% (2,593) males and 21% (684) females. It has a student population of about 70,000 pursuing various undergraduate and graduate programmes. The composition of both staff and students reflects the diversity that the University promotes, comprising; women, men, the able and physically challenged, Ghanaians, and foreigners of different ethnic and religious background.

The University campus is accessible to all manner of persons on daily basis, especially those from the surrounding communities to visit staff and students, attend various recreational programmes, do businesses, access some of the services and facilities the University provides such as healthcare and so on.

Although open access to a university campus is rightly seen as an essential ingredient of academic life, it is not without risks. Some security measures are therefore necessary to maintain a safe and secured environment for our staff, students and visitors.

Protecting the University from security vulnerabilities or incidents is vital to ensuring that it meets its strategic objectives. Security measures and policies are, therefore, not only inevitable but highly desirable to maintain the University's reputation as a safe, secured and conducive environment for teaching and learning. It is in the light of this that management saw the need for the development of this Policy.

2.0 SCOPE OF POLICY

This policy covers physical (facilities), information, personnel, travel, visitor and event security issues. It also includes violence within the University (workplace violence, domestic violence and student-related violence), sexual harassment issues, substance misuse/dependence, crisis/emergency and fire safety. Taking into account its extensive nature, the Policy seeks to apply to all staff and their dependants, students, contracted third parties, non-university employees located within the University premises including those engaged in service provision, trespassers and visitors. This policy would also cover the relationship between the University and other stakeholders such as law enforcement agencies and essential service providers whose assistance would also be required in times of security incidents.

3.0 PURPOSE OF POLICY

The University is committed to ensuring that a safe and secured environment is established to achieve its vision. This Security Policy seeks to ensure that all members of the University community, including students and other clients, staff, visitors and contractors, are provided with a safe, secure and friendly environment in which to function.

4.0 POLICY OBJECTIVES

This security policy has been developed to:

i. Ensure that security issues are managed to conform with the University's vision, mission and strategic plan.

ii. Provide procedures to ensure safety and security of staff, students, third parties and visitors at all times.

iii. Outline the University's responsibilities in relation to the maintenance of a safe and secured environment for the University and the protection of lives and properties.

iv. Minimize the University's exposure to all levels of risks where safety of lives and properties are potentially compromised.

v. Ensure that there is a cohesive system of security controls, which permit the University to continue its legitimate operations without disruption in the event of crises/ emergencies.

vi. Outline the role and responsibilities of staff, students, third parties and visitors in ensuring a safe and secured environment within the University.

5.0 GENERAL SECURITY POLICY STATEMENT

The University is committed to ensuring that a safe and secured environment is established to achieve its vision. A comprehensive security policy covering physical, information and personnel security and other workplace related security issues is developed for the compliance of all. The University shall provide all the needed resources for the implementation of the various area-specific security policies and measures for the safety and security of staff, students, clients and physical assets. Appropriate disciplinary actions and enforcement measures shall be put in place to ensure the attainment and maintenance of a safe and secured environment.

6.0 POLICY AREAS

6.1 Security Survey and Risk Assessment

Security survey is an inspection and evaluation exercise to determine whether there are baseline security measures and standards in place and assess their effectiveness and vulnerabilities for remedial actions. The security baseline standards includes security policies and procedures; physical, personnel and information security measures; etc.

Security risk analysis and assessment of assets of the University is to identify current security threats and to determine whether new security measures should be introduced or existing ones upgraded. The process will ensure that appropriate security measures to be implemented corresponds with the exact security risks and threats and also to ensure returns on security investments.

6.1.1 Policy Statement

The University through the Security Services and in conjunction with relevant internal and external stakeholders will conduct regular security surveys, security risk analysis and assessment of University assets and submit reports to the relevant authorities for implementation.

6.2 Physical Facility Security

A facility, for the purpose of this Policy, is one or more buildings or structures that are related in function and location, and form an operating unit. Facilities of the University have assets (personnel, information and property) that need physical security measures to safeguard and prevent them from malicious attacks including terrorist attacks. Physical security measures are the security controls implemented to prevent, deter, detect, deny, delay and disrupt criminal activities. It generally incudes facility protection measures, access control measures, and deployment of security personnel.

The physical designing of the campus environment to prevent crime and other security incidents known as Crime Prevention through Environmental Design (CPTED), will be an additional measure. These measures are to be implemented to ensure a safe and secured environment for the achievement of the vision of the University.

6.2.1 Policy Statement

All members of the University Community are to implement physical security measures to safeguard facilities and assets therein against security incidents and to ensure a safe environment for academic and other works. This will be achieved by the adherence to the following procedures:

6.2.2 Procedures

6.2.2.1 Perimeter Protection

i. A facility may be protected by a perimeter fence or a wall of at least 2.4 metres in height, depending on the security threat posed to the facility. Perimeter fences/walls should have hostile toppings (barbed, razor wire, or electric fence) to prevent easy climbing or scale over.

ii. Create 3 meters clear zone on both sides of perimeter fences/ walls to allow for security patrolling and surveillance.

iii. Depending on the security threat and the sensitivity of the facility, perimeter intrusion detection systems are to be installed.

iv. Install perimeter CCTV systems for the purposes of surveillance, deterrence, evidence, and quick security response.

v. Install the appropriate perimeter lighting to deter and detect intruders in the night.

vi. Perimeter fences/walls are to have caution signage against trespassing and presence of security systems hanged or affixed to deter criminals and other users in line with legal requirements/compliance.

vii. Facility perimeter fences/walls should have appropriate gates with locks and well equipped security gatehouses.

viii. Regular security inspections and routine maintenance of perimeter fences/walls and security systems shall be conducted to deter adversary activities.

ix. Security officers/guards are to conduct regular perimeter patrols to ensure proper functioning of perimeter fence/walls and security systems.

6.2.2.2 Building Protection

i. All buildings are to have strong external doors that are difficult to remove or break into. External doors should be made of solid construction materials.

ii. All doors are to be fitted with appropriate locks with locking mechanisms difficult to circumvent or compromise.

iii. Doors are to be locked inside except the final exit or emergency exit doors.

iv. Establish key control measures that will prevent illegal use of keys and unauthorised copying.

v. Final exit door keys of buildings and facilities are to be deposited by an authorised permanent staff at the Security Offices after close of work and after the exit of all staff. No staff is to have a copy of the final exit door keys unless authorised to do so.

vi. Steel gates or grilles are to be fitted to the inside or outside of all external doors.

vii. Building windows are to be built into strong frames and mounting well secured in the surrounding wall and constructed with appropriate glazing material.

viii. Window frames are to be fitted with adequate locks to prevent forced opening and secured by staff after close of work.

ix. Depending on security threats all windows are to be additionally protected with bars, retractable grilles and shatters. All windows within 5 metres of the ground are to be protected with bars and grilles.

x. External outdoor units of equipment (e.g. air conditioner units) and electrical plants (e.g. generators, transformers, etc.) are to be protected in secured metal cages or fences.

xi. Both internal and exterior of building and surroundings should be well illuminated using the appropriate lighting systems.

xii. CCTV system should be installed in and on all buildings to improve surveillance and to deter criminals.

xiii. Plants and flowers are to be planted more than 5 meters from building walls and maintained or trimmed to allow for visibility by occupants in buildings.

xiv. Car parks are to be created for all buildings. Car parks are to be clearly marked to take care of senior management and staff, people with special needs, visitors, drop of points, and exit and entry points. Car parks are to have paved pedestrian walk way that leads to access control entry point of buildings. They are to be well illuminated with appropriate lights and covered with CCTV surveillance.

xv. Security officers/guards are to conduct regular patrols around buildings to ensure the security of building attachments and installations and inform facility officers/managers of any security lapse for correction.

6.2.2.3 Access Controls

i. Directional and route signage are to be erected or affixed at vantage positions to direct movement of persons and vehicles to a controlled exit/entry points and within facilities.

ii. Install automated access gates and turnstiles with card readers at main entry/exit points into facilities.

iii. Personal biometric ID cards are to be used to identify persons accessing locations in facilities. It is compulsory for all staff, students and visitors to wear around their necks and visibly display ID cards except for health and safety reasons before allowed entry into facilities.

iv. Staff and students are to politely challenge strangers and visitors without authorised identification cards worn on them to help detect unauthorised persons.

v. Number of entry and exits portals should be reduced to the minimum according to the operational requirement of a facility.

vi. Critical areas in facilities such as IT server rooms, Research and Development spaces, cash/accounts offices, etc, are to be labelled 'Restricted Areas/ Authorized Personnel Only.'

vii. Removal of any University property out of facilities and the campus should be accompanied by an authorisation note which will be checked by security officers before allowing its exit.

viii. All University assets are to be clearly marked and visible to all.

ix. Key-control register/book should be maintained at facilities, and that of the final entry/exit key controlled by the security office.

x. University vehicles and staff vehicles with stickers will be allowed by security officers into facilities whiles all others will be treated as visitors and be subjected to the appropriate controls.

6.2.2.4 Crime Prevention through Environmental Design

i. In designing facilities within the campus, the environment of these facilities should be designed to ensure natural surveillance and access control.

ii. Measures to increase visibility to expose would-be perpetrators and provide safety for legitimate users of facilities have to be undertaken. These measures include lighting, maintenance of bushes and lawns, landscaping, and well defined areas for public and private purposes through signage.

iii. Maintain the physical environment to give the impression of care which wards off criminals. Ensure the regular maintenance of lighting systems, painting, fences, walkways, etc.

6.2.2.5 Facility Counter-terrorism

The University is a critical national infrastructure and strategic asset and, therefore, vulnerable to terrorists, bombs, firearms, chemical, biological, and radiological attacks. The following counter-terrorism measures and procedures are to be strictly implemented to mitigate the effects of such attacks on University assets and operations:

i. Depending on the threat level, corresponding access control measures are to be implemented in University facilities. These control measures include; limiting number of entry points into facilities, visitor control, personnel and vehicles screening and searches for early detection of terrorist activities.

ii. Search equipment for small arms and Improvised Electronic Devices (IEDs) are to be procured for facilities. These equipment includes metal detectors, x-ray machines, and under-vehicle search mirrors.

iii. Facility and building plans on campus are to include Counter-terrorism Protective Security Measures in the design stages. These measures include; construction of car parks at blast stand-off distances, perimeter fencing, vehicle checkpoints, anti-ram bollards, raised planters, jersey barriers, vehicle speed reduction measures (e.g. speed humps, chicanes and vehicle speed breakers at kerbsides), etc.

iv. Depending on the threat level, mail/post rooms are to be established away from main premises and strict mail-handling procedures implemented.

v. Implement Crime Prevention through Environmental Design (Paragraph 6.2.2.4 supra), and good housekeeping in facilities to help detect and deter terrorist activities.

vi. Install alarm warning and public address systems on facilities for emergency signals and announcement of imminent terrorist attacks.

vii. Consult the Head of Security Services for physical counter-terrorism inputs when planning new facilities.

viii. University Security Services is to deploy uniform and plain cloth security officers and guards on facilities to gather intelligence, detect terrorist activities and deter terrorist.

ix. The Security Services with the support of experts from external security agencies are to conduct physical security survey, risk and threat assessment in respect of terrorist activities against facilities on campus.

6.2.2.6 Security at Private Hostels

i. The Office of the Dean of Students shall in consultation with and advice from the University Security Services approve private hostels before students are admitted into the hostels.

ii Private hostels shall not be allowed to admit students of the University without approval of their security arrangements in line with this Policy.

iii. All private hostels approved for occupation by students of the University shall be published by the Office of the Dean of Students.

iv. Students who occupy private hostels not approved and published by the Office of the Dean of Students shall be responsible for their own security and liability not shifted to the University.

6.2.2.7 Deployment of Security Officers

Security officers/guards from the Security Services are to be physically deployed on/in facilities to perform protection duties. These duties are patrolling, implementation of access control measures, searches, and inspection of security systems to check their functionality.

Powers of the Security Officer/guard during deployment

The Powers of the University Security Officer/guard shall be derived from the University Security Services Standard Operating Procedures 2021.

6.3 Information Security

The University works with a lot of sensitive information (University's information and personal data) that faces a lot of threats, and if compromised would have serious consequences on the security and reputation of the University. Some of these threats include; information theft, inadvertent disclosures, interception, and various forms of cyberattacks.

To achieve information security, the three qualities of information; confidentiality, integrity and availability must be maintained. If an information is viewed by unauthorised persons, the confidentiality of the information is breached. Integrity of information is achieved when it has not been altered or modified without appropriate authorization. Availability of information is when there is a continued and uninterrupted accessibility to information by authorised users.

6.3.1 Policy Statement

The University Community, affiliate institutions, external clients, business partners, and contractors shall be obliged to protect the University's information under the Data Protection Act (Act 843), 2012, any other transaction under the Electronic Transaction Act (Act 772), 2008 and any other rules, regulations and laws in force and binding on the University and third parties. This is to ensure the confidentiality, integrity and availability of information. The University shall secure and protect all forms of information in its custody against threats, cyberattacks and unauthorised dissemination of information. To achieve this, directives on the general procedures outlined herein shall be followed.

6.3.2 Procedures

6.3.2.1 Physical Security of Information

i. Facilities/offices using Information and Communication Technologies (ICT) shall put in place physical control measures to prevent unauthorised access, use and theft of IT equipment (refer to Paragraph 6.2 Physical Facility Security for guidance).

6.3.2.2 Information classification

i. All University information should be classified, handled, stored, and shared/disclosed strictly according to the level of classification/authorization.

ii. Classified/sensitive information shall be conspicuously and appropriately marked.

iii. Classified/sensitive information shall be securely stored, transmitted, declassified, accounted for, and correctly disposed of.

6.3.2.3 Information Security Awareness

i. The University shall ensure that Information Security Awareness workshops/seminars etc, are organised periodically for staff, students and other authorised users of information on the threats, vulnerabilities and retrieval of information belonging to and used by the University.

ii. The University shall ensure the development of requisite skills and knowledge of users to safeguard the use of IT infrastructure and systems.

iii. A culture of information security is to be created at all Colleges/Institutes/Departments/Units of the University.

6.3.2.4 Non-Disclosure/Confidentiality Agreements

i. Non-disclosure/confidentiality agreements shall be included in every contract that the University enters with third parties.

ii. Staff and students that work on highly classified/ sensitive information shall be required to sign Non-Disclosure/ confidentiality Agreements.

iii. Subject to (i) and (ii), upon completion/termination of contract, exit of an office, dismissal, completion of programme of study, etc. all users of classified/sensitive information belonging to and used by the third party, staff and/or students shall be made to appear for exit interviews and be reminded of the Non-disclosure of information and the confidentiality contained in the agreements.

iv. To mitigate the risk of insider disclosures of classified/ sensitive information, background screening on all prospective employees, prospective users (current employees and students), and third-parties are to be conducted.

6.3.2.5 General Information Security Procedures

i. Passwords shall be created as prescribed by the KNUST ICT Policy (ICT4KD2008).

ii. Passwords shall be stored securely. Passwords or login details shall not be given to anyone or displayed.

iii. Passwords or login details suspected to be compromised shall be reported to the ICT administrator at the various Colleges, Faculties, Departments, Units and/or at the UITS Helpdesk.

iv. Sensitive information shall not be disclosed to anyone without authorization in writing.

v. Sensitive information shall be accessed on a strict need-to-know basis. Strict physical access controls shall be implemented at sensitive locations.

vi. Visitors and unauthorized personnel shall not be allowed into ICT restricted areas.

vii. The University shall establish a “Clean Desk Policy” and all staff, students and authorized personnel shall adhere to the said policy.

viii. Colleges/Faculties/Departments/Units shall maintain good housekeeping to prevent information theft and its attendant consequences on the University.

ix. Staff, students and third parties shall not relay any sensitive information to third parties whether official or unofficial without the express authorization of the University.

X. Staff, students and third parties shall take added precautions when on official or unofficial travel to protect sensitive information in their possession (refer to KNUST ICT Policy, ICT4KD2008).

xi. All persons (staff/students/consultants/contractors/etc.) shall be cautious and prevent falling prey to social engineering (the use of deliberate tactics by adversaries to manipulate or deceive unsuspecting persons to illicit information from them through telephone enquiries and phony calls, emails, social networking sites and platforms, etc.)

6.3.2.6 Intellectual Property Security.

The University shall ensure intellectual property (patents, trademarks, and copyrights) of the University are legally protected (refer to KNUST Intellectual Property Policy, Policy 0012).

6.3.2.7 ICT Systems Security.

The University shall adhere to the KNUST ICT Policy, ICT4KD2008.

6.4 Personnel Security

Personnel Security is the protection of people from harm and protection of the University assets against deviant staff, students and unauthorized persons. Personnel through deliberate or inadvertent behaviours become security risks and threats to the University community and, therefore, the University must provide the protective measures and guidelines to be complied with by all persons.

6.4.1 Policy Statement

The University shall create a safe and secured environment for all persons within the University community and ensure that all staff and students are cautious of their security roles and responsibilities. The University will institute security measures and processes that will prevent exploitation of vulnerabilities of persons aimed at compromising the security of the University. Systems shall be put in place so that hiring, expiration, termination of employment/contracts can be critically monitored to ensure that rightful personnel are employed and when departing from the University, sensitive information and/or assets shall not be misappropriated. For this to be achieved, the University directs all to follow the general procedures outlined.

6.4.2 Procedures

i. University Management shall ensure that continuous security awareness training on personnel security issues and its impact on the University Community is organised for staff and students.

ii. University Management is to ensure that rightful persons are recruited as staff (permanent and contract) into the institution.

iii. University Management shall ensure that background checks are carried out on potential employees (permanent and contract), students and third parties to mitigate the risk of engaging/employing/admitting criminals, people with potential criminal traits or enter into contracts with unqualified third parties.

iv. University Management shall develop a general and specific Ethical Behaviour and Standard Policies or Codes of Conduct for staff.

v. University Management should ensure that staff and students with some challenges have access to guidance and counselling. This is to ensure that life challenges faced by staff and students do not degenerate into activities that pose security threats to the University.

vi. University Management shall conduct confidential exit interviews for retirees, staff whose contracts have terminated/ expired, staff who have resigned and third parties whose engagement with the University has come to an end. This is to remind them to comply with Confidentiality/Non-Disclosure Agreements (NDAs) they entered into and also to encourage them to reveal dishonest and unethical behaviour of personnel for correction and challenges confronting their Departments/ Units.

6.5 Violence within the University

Generally, violence is said to be actions which causes destruction, pain or suffering. Basically, there are three main violence within a University setup. These are workplace violence, domestic violence and student-related violence (residential and non-residential students).

Workplace violence is an incident in which persons are abused, threatened or assaulted within the work environment. It includes verbal abuse or threats and physical attacks some of which are; physical harassment, stalking, theft, robbery, kidnapping, assault, etc.

Domestic violence is said to be any actions which causes destruction, pain or suffering in the domestic environment. It includes both psychological and physical abuse.

Student-related violence can be said to be any behaviour involving students using physical force or not, with the aid of any instrument, object or not, intended to hurt, cause fear or pain to a fellow student/staff/third parties or to cause damage to properties in or outside the University. It includes physical attacks like fighting, bullying, stalking, sexual harassment, kidnapping, theft, robbery, etc. It also includes emotional and psychological abuse.

Workplace, domestic and student-related violence, also covers incidents such as suicides and homicides. Violence is inevitable for a University with a large number of people from diverse backgrounds. It is therefore important that necessary steps are taken to mitigate the effect of violence at the workplace, domestic violence and student-related violence and its attendant security issues. This would therefore ensure the peaceful and congenial environment needed for the University to function properly.

6.5.1 Policy Statement

The University shall provide a safe and secured environment and will, therefore, not tolerate any form of violence whether physical, psychological, emotional or otherwise. Unacceptable behaviours and practices such as harassments, verbal abuse, threats, bullying, robbery and the use of ”drivers of violence” and disruptive behaviours such as alcoholism, drug abuse and carrying of weapons, shall not be tolerated.

Issues and incidents of violence shall be treated as serious security incidents and perpetrators shall be subjected to disciplinary actions, including but not limited to possible prosecutions and administrative sanctions which may include dismissals. The University encourages the reporting of violent incidents involving staff, students and third parties in whatever form (whether physical, psychological or emotional) to the appropriate authorities which shall be quickly attended to and treated with utmost confidentiality. All staff and students of the University community and third parties shall follow these outlined guidelines to ensure that a violent-free environment is achieved.

6.5.2 Procedures

i. The University shall organize Violence Awareness Training (workplace/domestic /student-related violence) for all staff and students under the auspices of KCC at least once every year. The training must include Incident Reporting and Resolution Procedures.

ii. At the College, the Provost shall appoint Focal Persons who shall be lecturers in the various departments and shall be trained in the identification and management of Violent Incidents involving staff and students. In the case of non-academic departments, Registrars shall be appointed as Focal Persons for their units.

iii. There shall be a "College Violent Incident Management Team (CVIMT)" at the Colleges headed by the College Registrar. Other members of the Team shall include the College Counsellor, one (1) Focal Person from the College, a legal officer, medical officer, student representative (where necessary), and a representative of the University Security Services.

iv. The functions of the "College Violent Incident Management Teams (CVIMTs)" are to accept violence reports, investigate, and recommend/take the appropriate disciplinary actions.

v. The functions of the CVIMT are to be widely publicised. The publication shall make available the names and contacts of the Focal Persons in the Colleges. The Focal Persons shall receive initial incident reports and forward same to the CVIMT. Information on how and where to report violence and the support to victims should be included in the publication.

vi. The CVIMT shall ensure the protection and confidentiality of victims, witnesses and findings after investigations.

vii. The CVIMT is to conduct regular violence risk assessment at respective workplaces to develop a Workplace Management Plan to prevent or control the risks.

viii. All persons, who have witnessed, received or heard of any conduct by any person that amounts to threats, harassments or unacceptable behaviours towards persons are to report to the respective Focal Persons or Heads of Departments for immediate investigations and resolution.

ix. With the help of security officers of the University or the Ghana Police Service (where necessary), remove from the premise of facilities as soon as possible any person who engages in threats in any form or exhibits violent or unacceptable behaviours. Such persons should not be allowed into the facility until initial investigations are completed.

x. Victims of violence are to keep records of such incidents and backup their complaints with detailed information and evidence.

6.6 Travel Security

The University by the nature of its mandate will require its staff, students and third parties to travel beyond the confines of the campus either nationally or internationally for official or business purposes. This exposes them to risks that may result in the loss of valuable property and information, and may be detrimental to their health and safety. Lack of a proper travel security procedures to ensure the safety and security of travellers may present legal liability on the University through the actions and inactions of staff, students and third parties acting for and on behalf of the University. Travel security in the University is a shared responsibility by the traveller (staff, students and third parties), the various Heads in line with the University's travel requirements, the Security Services, and the destination unit/office or host.

6.6.1 Policy Statement

The University shall ensure that its staff, students and third parties on local and national official travels, and international travel/assignments (official/unofficial) are safe and secured. It shall institute appropriate security measures to reduce the vulnerability of travellers against criminal activities and loss of properties and ensure their safety and security. The University aims at ensuring that travels are security incident free or impacts of incidents are mitigated to the lowest level. The University requires all to follow the procedures outlined below to ensure travel security.

6.6.2 Procedures

6.6.2.1 Travellers

i. Principal Officers of the University shall not as much as possible travel in the same vehicle (car, aeroplane, train, and ship). The Travel Desk of the University is to liaise with the Security Services to arrange the travel schedules of Principal Officers to ensure maximum security control measures.

ii. All travellers shall have in their possession complete and valid documentations (passports, vaccination cards, ID cards, Travel Insurance, etc.) required for their travel.

iii. All international travellers should endeavour to research and read about the legal, culture and economic conditions of the destination countries.

iv. Prohibited substances shall not be carried when on official/unofficial travels.

v. All personal and University electronic equipment such as phones, laptops, and tablets are to be well secured against theft, and any sensitive information and data on them are backed up and encrypted.

vi. Staff are to seek authorisation and security clearance from the appropriate authorities for official/unofficial travels.

vii. For student group travels, individual students should express their consent in writing or by signatures for travelling. For international travels consent of the guardian or parent shall be sought by the University.

viii. All student group travels shall seek initial clearance and approval from the Dean of Students before travelling. On securing the approval, the travellers shall seek final security clearance from the University Security Services before departure.

ix. Travellers are to update the Security Services and the relevant authorities on arrival at their destination and report to same on return to campus.

x. Travellers shall request for security tips/advice/briefings from the Security Services prior to embarkation on official travel.

xi. Travellers shall not engage in acts that shall bring the name of the University into disrepute.

6.6.2.2 Heads of Department

Heads of Department shall:

i. Ensure that they have received the approvals, travel itineraries as well as security clearance of all travellers (official/unofficial) before allowing them to embark on the travel.

ii. Establish and maintain a close liaison with the travellers and the University Security Services until their return.

6.6.2.3 University Security Services

The University Security Services shall:

i. Provide safety and security briefings/advice/tips including emergency contact numbers for travellers (official/unofficial).

ii. Give security clearance prior to approval of travels, and on request provide security throughout the travel.

6.6.2.4 Destination Unit/Office/Host

i. University Unit or Office outside campus or overseas are to establish a liaison between official travellers and the University Security Services.

ii. Ensure safe and secured reception arrangements for the travellers on arrival at destination. These arrangements include; secure airport arrival procedures, safe lodging, safe transport arrangements, etc.

iii. Provide briefings on local security to travellers on arrival. This briefing should include in-country/town emergency procedures to be followed.

iv. The University shall liaise with the Host institution to ensure the safety and security of its staff, students and third parties and provide where necessary legal, health, or immigration assistance.

v. The University is to ensure that the host institution commits to be held responsible for any security breach resulting in injury, loss of lives and property.

6.7 Transport Security

Transport security refers to measures taken to protect passengers, vehicles and equipment and to make sure violations do not occur. The University owns a lot of vehicles as part of the logistics it uses to achieve its mandate. These vehicles are of different make and capacities and they travel the length and breadth of Ghana and sometimes outside Ghana conveying staff, students, third parties and equipment for various purposes. The vehicles as well as their passengers are exposed to security risks that may result in security incidents such as the loss of the vehicles, theft of equipment, unauthorized use or misuse, and associated safety related issues to passengers, etc. Therefore, movement of University vehicles, equipment and passengers have to be subjected to adequate security control measures to ensure their security and safety and also prevent their misuse.

6.7.1 Policy Statement

The University shall ensure that its transport system operates in a safe and secure manner to ensure the security of its vehicles, passengers (staff, students and third parties) within and out of campus on official travels. Consequent to that, the “Regulations on the use of University Vehicles,” (Recorder No. 405 Nov. 2011 Vol.45 No.3) has been published for the compliance of the University Community. It shall further institute appropriate security measures to control movement and usage of vehicles in and out of campuses to ensure that transport related security incidents are reduced to the minimum. The University requires all to follow the procedures outlined below to ensure transport security.

6.7.2 Procedures

i. All University vehicles leaving the campus are to be subjected to security screening and searches at the main gates when entering and exiting the campus.

ii. Drivers in charge of University vehicles exiting the campus are to show proof of authorisation for the use of the said vehicle for any transaction whether within campus or journey outside the campus at the main gates before allowed to exit.

iii. No persons are to carry any form of weapon (whether licensed or unlicensed) when on board a University vehicle.

iv. All drivers are to immediately report any road traffic accident on campus to the University Security Services for onward report to the KNUST MTTD. Accident outside campus are to be reported directly to the MTTD and thereafter follow the reporting procedure spelt out in “Regulations on the use of University Vehicles”, (Recorder No. 405 Nov. 2011 Vol.45 No.3).

v. University vehicles shall not be used to carry or cart prohibited substances.

vi. Drivers of University vehicles shall adhere to all traffic laws and regulations when driving on or off campuses.

vii. Drivers of University vehicles should operate in a manner to avoid injury to persons and property.

viii. All University vehicles that are on and off campus shall be parked at locations spelt out in "Regulations on the use of University Vehicles", (Recorder No. 405 Nov. 2011 Vol.45 No.3).

ix. An authorised driver of a University vehicle shall not give control of the said vehicle to third parties (whether a colleague driver of the university, a staff, or any other person) without express authorisation.

x. All university drivers shall be trained in defensive driving and first aid caregiving.

xi. Members of the University community and third parties when using commercial vehicles within the University campuses are to comply with the directives on movement and control of such commercial vehicles.

xii. All commercial vehicles ('trotros', taxis, despatch cars and motorcycles) are to register at the Transport Department and be issued with permit and stickers to be allowed to operate on University campuses.

6.8 Visitor Security

Visitors to organisations and facilities pose security threats if they are not controlled and managed, and they can also encounter security challenges. Some of these threats includes, movement of miscreants into facilities unchallenged, and criminals entering controlled areas for criminal acts. The size of the University and the number of visitors it receives make it prone to activities of criminal visitors and their attendant security and safety risks to its personnel.

People entering any facility within the University could be classified into three main groups:

i. Official visitors.

ii. Unofficial visitors.

iii. Staff/students visiting other facilities for private engagements.

iv. People entering to commit crimes.

6.8.1 Policy Statement

The University shall ensure that a safe and secured environment is created to protect its personnel, students and third parties from criminals and prohibit unauthorised entry to facilities in the University. It shall establish Visitor Management Systems and Procedures to reduce the security and safety risks posed by malicious and unauthorised visitors. All personnel, students and third parties are required to follow the procedures outlined to ensure maximum visitor security in all the University campuses and facilities.

6.8.2 Procedures

i. All facilities shall have a general reception area/space on the ground floors to receive and screen visitors. Special reception areas should be created for high-risk management staff (Principal Officers and other high profile executives).

ii. Visitors waiting room/area, installed with CCTV cameras should be created in all buildings. New buildings are to be designed to include a visitors' waiting room/area.

iii. Visitors shall have recognised sponsors or hosts before entries into facilities are allowed. Sponsors/hosts are to give advance notice about their visitors to the reception. If not done, receptionists are to seek clearance and consent from the sponsor/host before any visitor is granted access to the waiting room/area.

iv. Visitors shall be directed to the reception before taken to the waiting room/area where they shall meet their sponsors/hosts. Hosting of visitors in offices is strictly prohibited unless given express permission to do so. Sponsors/hosts are to ensure that their visitors are checked out at the reception.

v. All visitors to facilities and controlled areas are to sign-in their details at the reception, and issued with a visitors' identification tag on a unique coloured neck strap that shall be worn around the neck as long as he/she remains within and around the facility.

vi. Visitors' identification tags shall have the word 'VISITOR' boldly written, with easily recognized unique numbers on them.

vii. When necessary, visitors and employees shall be subjected to security searches/inspections with their consent. Refusal of consent by visitors/employees shall warrant refusal of entry into the facility. The searches shall be done according to laid down procedures. Sponsors/hosts are to give prior information to their visitors of possible security search/inspection requirements before being allowed into facilities.

viii. Signs for searches and prohibited items are to be posted at entry and exit points of controlled facilities for visitors notice.

ix. Delivery drivers and couriers shall be subjected to the same visitor registration procedure and searches/inspections at Receptions.

x. Facilities are to have clearly marked slots or spots reserved for visitors' cars. All car parks are to be equipped with physical security access control systems including but not limited to searches of vehicles with the consent of the person in charge of the vehicle. Disclaimer signs should be conspicuously displayed at every Car Park denying liability for any damage, theft, and/or loss of items.

xi. In times of high visitor volume periods such as admissions, payment of fees, enquiries, etc., temporal offices shall be created by the University to manage the crowd.

xii. Staff, students and third parties contracted by the University shall not entertain personal and unofficial visitors in their offices at all times.

xiii. Entertaining guests in the Halls of Residence by students shall be in accordance with the KNUST Students' Guide and Code of Conduct.

xiv. Staff, students and third parties of the University Community shall always wear their identification tags to help identify unauthorised persons on the University premises. Any persons not wearing the prescribed identification tag are to be politely challenged and escorted to the Security for further action. This is essential to detect unauthorised persons.

6.9 Sexual Harassment Issues

The KNUST Sexual Harassment Policy (KNUST Sexual Harassment Policy 0027) has copiously given a definition and scope of what is termed as sexual harassment. It is, therefore, important that Sexual harassment in an organisation be properly handled in a timely manner to prevent it from escalating into violent criminal incidents such as sexual assault, rape, defilement and to a larger extent suicide. These have consequences on the University as well as the health and safety of staff, students, third parties, visitors, etc.

6.9.1 Policy Statement

The University shall ensure a safe and secured environment devoid of sexual harassment and its related security incidents for all persons. It shall not entertain any sexual harassment issues and will deal swiftly and decisively when it occurs. Consequent to that, a Sexual Harassment Policy (KNUST Sexual Harassment Policy 0027) has been developed to be complied with by all. In furtherance to this, the University will institute additional security measures to prevent and mitigate the effects of criminal activities borne out of sexual harassment incidents. It will also provide the necessary assistance in respect of criminal activities borne out of sexual harassments and violence. Staff, students, third parties and visitors to the University shall follow the procedures outlined below to achieve the aim of this Policy.

6.9.2 Procedures

i. The University Management shall conduct sexual harassment and violence orientation, seminars, etc., for all staff, students and third parties.

ii. All sexual harassment incidents shall be reported to the Anti-Sexual Harassment Committee (KNUST Sexual Harassment Policy 0027), but when the harassment involves sexual violence and other related criminal activities, report in earnest to the University Security Services and the Police.

iii. Victims of sexual violence (assault, rape, etc.) are to in addition to timely reporting of incidents, to protect, preserve, and present the evidence to the Police to facilitate investigations.

iv. Any unwelcomed sexual advances, unsolicited relationship that causes emotional stress or psychopathic experience shall be reported to the Anti-Sexual Harassment Committee and/or Counselling Centre for assistance (KNUST Sexual Harassment Policy 0027 refers).

v. When sexual harassment might affect workplace security and safety, steps must be taken to prevent the suspected abuser from accessing any facility that houses the victim in the University. Depending on the circumstances, the victim is to be given security protection whiles on University premises.

vi. When sexual harassment might affect workplace security and safety in situations where the partners/couples work within the same office/unit, steps must be taken to transfer one party from that office/unit.

vii. Victims of Sexual Harassment shall inform the University Management of any restraining or protective order received out of a criminal proceedings by a victim for enforcement on University facilities and premises. Management shall subsequently inform the Security Services and the Legal Department about the restraining or protective order.

viii. All persons must employ personal safety and security measures to ensure they do not fall victim to perpetrators of sexual violence.

6.10 Event Security

Event Security are the security measures put in place to ensure the safety and security of staff, students, third parties and visitors and to safeguard properties before, during and after events. Event Security for the University includes security for large events such as congregation, matriculation, investitures, public lectures, examinations, demonstrations, processions, Hall week celebrations, sporting events, religious gatherings, etc. This also includes smaller events like weddings, funerals, parties, etc. on all the campuses of the University.

The presence of large crowds during such events come along with a lot of security challenges that has the potential to breach the peace of the University. These events, therefore, need to be managed in order to maintain a peaceful and conducive environment in the University.

6.10.1 Policy Statement

The University shall maintain a safe, secured, peaceful and a conducive environment for its staff, students, third parties and visitors to events held on its campuses. The University will ensure that events held on its campuses are organised in a peaceful environment with minimal security risks and maximum safety. All persons are therefore to follow these outlined procedures.

6.10.2 Procedures

i. All events organised on campus shall be authorised by the University. The authorization shall be in writing indicating the rules, regulations and laws governing the release and use of the facility for the event.

ii. All events organised by students on campus shall be approved by the Office of the Dean of Students before authorised to take place.

iii. All authorised events on any facility on campus are to be brought to the notice of the University Security Services at least seventy-two (72) hours prior to the commencement of the event.

iv. Event organisers of special events such as demonstrations, processions, Hall week celebrations etc., which are to be held on University campuses shall seek authorization from the University fourteen (14) clear days and notify the Ghana Police Service in line with the Public Order Act 1994 (ACT 491) before commencement of the event.

v. Organisers of events after receiving authorization are to further request for Security Assistance from the University Security Services and the Ghana Police Service (when necessary) to provide security for the events.

vi. After seeking authorization for events, the Estate Office and Security Services shall be contacted for the necessary consultations needed for the smooth running of commercial activities related to the events. This is to ensure that events on campus that will attract vendors of food and beverages, retailers of items, and promotional sales are well organized for space management and security purposes.

vii. Event organisers shall in consultation with the Security Services put in place access control measures such as; event identification badges, press tags, signage, search and screening procedures, etc. to detect and prevent unauthorized attendees and or criminal activities before, during and after events.

viii. Event Organisers, Estate Office and Security Services shall in consultation with the relevant agencies put in place contingency and emergency measures during and after the events.

ix. Event organisers shall submit a Post-event report to the Estate Office, University Security Services and the Dean of Students (if it was a student organised event).

6.11 Substance Misuse/Dependence

Substance misuse is said to be a pattern of harmful use of any substance (solid, liquid and gas) for mood-altering purposes. These substances can be legal or illegal. Such substances include:

a. Illicit drugs (narcotics) such as cocaine, opiates like heroin, marijuana, etc.

b. Stimulants and depressants such as amphetamines, synthetic opiates such as tramadol and pethidine, etc.

c. Sniffing of volatile solvents like shoe glue and polish, snuff, etc.

d. Other prescriptive drugs such as benzodiazepines, codeine etc.

e. Alcohol and its related beverages.

Aside the effect on the health of users, drugs alter the state of the mind resulting in the committal of extreme acts that may be criminal or detrimental to the safety and security of everyone. Substance misuse/dependence also has consequences on the social, economic and financial state of the user and the society. The harmful effect and criminal consequences on members of the University Community from misuse of these substances require that, measures are taken to prevent their use by staff, students, visitors and third parties.

6.11.1 Policy Statement

The University shall ensure a safe and secured environment devoid of substance misuse/dependence. The University in collaboration with other stakeholders shall endeavour to maintain a healthy and productive workforce and student body by ensuring that substance misuse/dependence incidents do not occur in and around its campuses. The University shall not condone any form of misuse of substances and will take disciplinary actions against any culprit including but not limited to reporting them to the appropriate law enforcement agencies. Consequent to that, a Health and Safety Policy (KNUST Policy 0009) has been developed for the compliance of all. In furtherance to the said Policy, this Security Policy is to institute additional security measures to prevent misuse of substances on or off its campuses. The

University shall offer assistance and support to substance misusers (where necessary). All staff and students of the University, visitors and third parties are to follow the procedures outlined.

6.11.2 Procedures

i. The University shall organise seminars, educational talk shows, workshops, etc. on substance misuse and dependence at least once a year under the auspices of the KNUST Counselling Centre (KCC) for all staff and students.

ii. The University shall encourage whistleblowing from the general public on staff and students who possess, traffic, and/or use illicit drugs or misuse substances in and around the University campuses. Anonymous Hotlines and media platforms are to be established for that purpose.

iii. The University shall appoint or nominate persons at the Departmental and Unit levels who would serve as Focal Persons for complaints about substance misuse and related offenses.

iv. KCC is to train the Focal Persons on how to manage and handle reported cases.

v. The University shall institute investigations into any reported substance misuse or related incidents as quickly as possible for disciplinary actions where necessary. Protection and confidentiality of suspected culprits, misusers and/or witnesses are to be strictly adhered to during and after the investigation processes and/or disciplinary action.

vi. Heads of Departments are to be trained by KCC to be able to identify and manage early warning signs of possible substance misuse by staff and students.

vii. Where a person possesses, cultivates, manufactures, supplies, administers and/or uses illicit drugs in or around the immediate premises of the University, that person shall be reported to the Ghana Police Service forthwith. If the person is a student, the Office of the Dean of Students must be informed.

viii. The KCC in collaboration with the relevant stakeholders, experts and professionals is to establish a programme aimed at assisting substance misusers.

ix. To ensure that prospective employees are not substance misusers, the University shall conduct pre-employment drug screening for them.

x. To ensure a drug-free, conducive and peaceful work/study environment in the University, staff and students under reasonable suspicion and/or involvement in substance misuse are to be subjected to drug testing and subsequent appropriate action taken based on the outcome of the tests.

6.12 Crisis /Emergency Security

Crisis and Emergency are used synonymously but they refer to different situations. A crisis situation is one that affects an organization's existence and needs immediate resolution to prevent the total collapse of operations of the organization. Examples are major fire explosions at key installations, widespread violent demonstrations, pandemics, and extreme weather disasters and conditions. An emergency situation on the other hand poses serious and immediate risk to health, life or properties, and requires urgent intervention but not to the scale of a crisis. Emergency situations do not lead to the total collapse of the operations of the organization. Examples are fire outbreaks, epidemics, strikes, etc. Crises or emergencies being referred to may be caused by natural phenomenon or manmade events. The University will require safety and security interventions and measures to be implemented to prevent the occurrence and/or mitigate the impact of crisis and emergency situations.

6.12.1 Policy Statement

The University shall put in place measures to ensure stable, peaceful and secured environment conducive for teaching and learning. In addition to this, the University shall ensure that lives and properties are not lost or damaged during crisis or emergency situations. It will institute an ‘Emergency Action Plan’ that includes prevention, response and recovery measures within the University to ensure the safety and security of staff, students and third parties in times of crises and emergencies. Persons of the University community are to follow and comply with these procedures.

6.12.2 Procedures

i. The University shall develop a ‘Crisis/Emergency Action Plan for the entire University. This plan is to include; early warning signals, emergency reporting/communication procedures, response and evacuation procedures, and securing and recovery processes.

ii. The University shall establish a Crisis Management Team (CMT) to coordinate and manage crisis and emergency situations on and/or off campus. The composition of the CMT shall include but not limited to the following; the Security Services Management Committee, representatives of the University Health Services, University Relations Office, KNUST Counselling Centre, and NADMO.

iii. Colleges/Institutes/Departments and Halls of Residence are to develop individual and specific Emergency Action Plans (EAPs) for their facilities. This has to include direct liaison and coordination with crisis/emergency responders in their areas of operations (Fire Service, Law Enforcement Agencies, Medical Services, NADMO, etc.)

iv. Colleges/Institutes/Departments shall formulate Business Continuity Plans (BCPs). The BCPs are to be rehearsed for business continuity and incident response so that during emergencies/crisis, key business functions of the University can continue.

v. Facilities shall install emergency response systems; emergency alarm and public address systems, fire detection and extinguishing systems, standby electrical generators, etc.

vi. In times of medical emergencies such as epidemics, pandemics etc., the University will assist to provide Personal Protective Equipment (PPE) for protection and safety of personnel (where necessary). All personnel on University premises during such emergency situations are to wear PPEs and comply and observe any safety protocols.

vii. The University Security Services with the assistance of relevant security agencies are to deploy security officers/guards to perform crisis and emergency duties.

6.13 Fire Safety

Fire safety is the act of putting measures in place to eliminate or reduce the conditions that have the potential to cause fire, and lead to the destruction of life and/or property. Fire can occur out of natural disasters, negligent behaviours or criminal activities. Fire safety management, therefore, require both safety and security control measures. Security control measures are the enforcement of fire safety preventive measures to protect lives and/or properties, and activities for the smooth conduct of fire emergency response operations.

The University can easily loss personnel through injuries and loss of lives in addition to the destruction of properties by fire. This has its attendant consequences on the human resource, operations and finances of the University. To forestall and manage this, fire safety measures complimented by security and safety controls need to be implemented by the University.

6.13.1 Policy Statement

The University shall ensure a safe environment devoid of fire incidents on all its facilities. The University shall institute precautionary and preventive fire safety measures to reduce the likelihood of fire incidents on University facilities and its harmful effect on persons and properties. In addition to the Health and Safety Policy (KNUST Policy 0009) which is already in force, members of the University Community are to follow the outlined fire safety procedures herein.

6.13.2 Procedures

i. The University shall develop a Fire Safety Plan which shall include but not limited to Fire Risk Assessment, designated escape routes and exits, fire emergency assembling points, etc.

ii. The University Fire Unit in collaboration with Colleges/ Faculties/Departments/Units, shall conduct fire safety awareness training for all personnel of the University.

iii. The Fire Unit in collaboration with relevant departments (Security Services, Health Services, National Fire Service, etc.) is to conduct regular fire emergency drills for all staff, students and third parties.

iv. All buildings belonging to the University are to be installed with fire safety equipment and measures namely; fire extinguishers, smoke/heat/flame detectors, automatic water sprinkler systems, fire alarm systems, fire hydrant at building area, emergency exits, fire evacuation plans, etc.

v. All vehicles belonging to the University are to have fire fighting equipment and comply with DVLA requirements for vehicle safety.

vi. All buildings and vehicles belonging to the University, and human lives (staff, students and authorized persons) should be insured comprehensively against fire.

vii. Fire safety equipment at facilities are to be regularly inspected and maintained.

viii. Fire hazardous materials and chemicals kept at facilities are to be well stored and secured in accordance with directions and advises from the Fire Unit.

ix. Security officers and guards deployed on facilities are to ensure the compliance of fire safety measures and report fire safety risks to facility officers/managers for immediate corrective actions.

7.0 DUTIES AND RESPONSIBILITIES

Security on the University campuses shall be a shared responsibility for all; however, certain strategic security activities and responsibilities are vested in the following:

a. The University Council

The University Council is ultimately responsible for approving all policies in the University. It is also their responsibility to ensure that all relevant bodies responsible for its' implementation are appropriately identified and given the necessary resources. The Council shall ensure that management implements all policies to guarantee the security and safety of students, staff, visitors within the University and, the protection of University properties located in and out of the University.

b. Office of the Vice-Chancellor

The Vice-Chancellor's office has the responsibility of developing, implementing, monitoring, and reviewing (where necessary) the existing University's Security Policies. The Office is to ensure that adequate resources are provided for the implementation of this policy.

c. Office of the Registrar

The Office of the Registrar has the responsibility to ensure that all administrative processes for the implementation and monitoring of this Policy are carried out.

d. Office of the Provosts, Directors, Deans, Hall Masters/Wardens

The Offices of Provosts, Directors, Deans, etc. shall facilitate the implementation of the Security Policy in Colleges, Directorates, Faculties, Units, etc. The Offices shall ensure that support and resources are available to the Departments for the implementation of the Security Policy. Necessary measures to improve security in essential areas should receive priority consideration. Where appropriate, specific training to achieve acceptable standards of operations should be supported and properly resourced. The Offices shall ensure that security specifications are included in new buildings and refurbished facilities.

e. Heads of Department

The pivotal role in promoting enhanced security lies with Heads of Departments. They are responsible for ensuring adherence to the Security Policy. The actual responsibilities will vary according to the type, location, and the nature of activities of Departments. However, a number of specific responsibilities can be identified for Heads of Department in line with this policy:

i. Ensure that staff and students have access to and are familiar with the Security Policy, paying particular attention to those issues which are directly relevant to the activity of their respective departments.

ii. Undertake a security risk analysis of the Department, under the auspices of the Security Services, and act to remove or reduce as low as possible any security risks.

iii. Ensure that all staff and students in their Departments understand and exercise their security responsibilities as outlined in this Policy.

iv. Ensure that staff and students in the Departments comply with the implementation of this Security Policy.

f. Head of Security Services

The Head of Security Services is responsible for the implementation, co-ordination and monitoring of security procedures and protection systems outlined in this Policy. His responsibilities shall include but not limited to the following:

i. Ensure the implementation of the processes and procedures necessary to operationalise this Policy.

ii. Ensure that all the logistics, financial, personnel, administrative approvals, etc. for the Policy are coordinated to ensure its effective implementation.

iii. Conduct security risk assessments with the assistance of Heads of Departments and make the necessary recommendation(s) for the implementation of security measure(s).

iv. Conduct security surveys and audits of security systems and measures to assess their effectiveness, detect vulnerabilities and put in place corrective measures in line with this Policy.

v. Give periodic reports on the implementation of this policy.

vi. Ensure a healthy relationship is maintained between the University and other relevant stakeholders such as law enforcement agencies, emergency services, etc.

g. Staff

All staff shall strive to be familiar with and adhere to this University Security Policy.

They shall also give their necessary assistance and co-operation in line with the security procedures contained in this policy during crisis, emergency and security situations.

h. Students

All students shall strive to follow and adhere to this Security Policy in addition to regulations of the University as set out in the Students Guide and Code of Conduct.

They shall also give their maximum co-operation in line with the security procedures contained in this policy during crisis, emergency and security situations.

i. Visitors and Third Parties

Visitors and Third parties (conference delegates, external event attendees, sub-contractors external consultants, etc.) are to comply with the general University regulations and specifically this Policy anytime they are on the University premises and to ensure they carry themselves well for their security and the security of others.

They have a general responsibility to the security of University facilities whilst on campus and to give due consideration to security issues. In particular, they must follow security procedures designed to protect lives and properties. They shall at all material times wear their identification badges.

8.0 VIOLATION OF THIS POLICY

All members of the University community, consultants, contractors and clients of the University who violate this Policy may be subjected to disciplinary actions which may include administrative, criminal, and civil actions.

9.0 RELATED POLICIES

The University recognises that, security threats and issues continue to evolve and emerge into complex and unpredictable situations and incidents. As such, other policies which are already in existence and related to security issues shall be used in addition to this Policy.

This Policy is however directly linked and related to specific security issues that have been stated herein. Members of the University Community are, therefore, to read, use, and interpret portions of this Policy in conjunction with the under listed policies already in force.

A. KNUST Health and Safety Policy, Policy No. 0009.

B. KNUST Sexual Harassment Policy, Policy No. 0027.

C. KNUST ICT Policy (ICT4KD2008).

D. KNUST Intellectual Property Policy, Policy No. 0012.

E. KNUST Students' Guide and Code of Conduct.

F. KNUST Graduate Student Handbook 2017.

G. KNUST Recorder No.405 Nov. 2011 Vol.45 No.3.

H. KNUST Security Services Standard Operation Procedures, 2021.

10.0 INTERPRETATION OF THIS POLICY

The interpretation of this Policy shall be subject to the existing Laws of Ghana, the KNUST Act (Act 80 as amended), the KNUST Statutes 2004 and any other KNUST policies.

11.0 EDUCATION, IMPLEMENTATION AND MONITORING

i. The University through the University Security Services shall develop training programmes for all Security Services staff to ensure understanding and effective implementation of this Policy.

ii. The University Security Services, shall be directed by the Vice-Chancellor to sensitise, monitor, and evaluate the effectiveness of this Policy.

iii. The University Security Services shall submit annual or periodic reports on the implementation of this Policy to the Vice-Chancellor.

iv. The University Security Services shall set the performance standards of its operations and bench marked against internal and international best practices in the management of security within the University community.

12.0 POLICY ALIGNMENT, VALIDITY, EFFECTIVE DATE AND REVIEW

12.1 Alignment with Other Policies

The Quality Assurance and Planning Office (QAPO) shall be responsible for monitoring the implementation of this Policy to ensure that it is in alignment with other policies and strategies of the University. Actions and strategies of this Policy should not conflict with other policies of the University.

12.2 Validity of Policy Provisions

This Policy does not seek to replace other provisions in the KNUST statutes. In the event of conflict, appropriate measures shall be taken by the Academic Board to address them. The Policy becomes operational after approval by the University Academic Board.

12.3 Effective Date

This Policy was approved at the 406th (Regular) Meeting of Academic Board held on 18th July, 2022

12.4 Review of the Policy

Taking due cognisance of the current global trends in security issues particularly on university campuses, it is recommended that the Security Policy document be reviewed every five (5) years to address changes in its operations.

The Quality Assurance and Planning Office (QAPO) shall liaise with the appropriate Units for such reviews.