CAPE COAST TECHNICAL UNIVERSITY

CAMPUS SECURITY POLICY

CCTU P NO. 24

CAPE COAST TECHNICAL UNIVERSITY

GAZETTE

CAMPUS SECURITY POLICY

December 18, 2024
CCTU P NO.24

PUBLISHED BY THE DIRECTORATE OF PUBLIC AFFAIRS

TABLE OF CONTENTS

1.0 PREAMBLE

The main responsible for the discharge of campus security in and around campus as defined by the Statutes of Cape Coast Technical University, which is an essential area within the University, is the Campus Security Section.

The basic functions of the Security Section are to preserve peace, protect life and property, prevent crime and ensure order. The Section has no judicial function and the decision of guilt or innocence and the punishment of offenders are not the responsibilities of the Security Section.

Every day, people from the surrounding communities, in particular, can visit faculty members and students, participate in a variety of recreational activities, conduct business, and use some of the university's services and facilities, like its medical center, FM station among other things. Open access to a University campus is widely seen as a necessary component of academic life, but there are risks involved. In order to provide a secure environment for our staff, students, and visitors, some security measures are required.

To ensure that the University achieves its strategic goals, it is essential to protect it from security flaws or incidents. To maintain the University's reputation as a safe, secure, and favorable environment for teaching and learning, security measures and policies are, therefore, not only necessary but highly desirable. In the light of the above, the management recognized the need for the creation of this Policy.

2.0 SCOPE OF THE POLICY

Personnel, physical facilities, informational, travel, visitor, and event security concerns are all covered by this policy. Additionally, it covers difficulties with sexual harassment, drug abuse and dependence, crisis management, and fire safety within the university (including violence in the workplace, domestic violence, and violence against students). The Policy aims to include all staff members and their dependents, students, contracted third parties, non-university personnel working on university property, including those involved in service provision, trespassers, and visitors due to its wide character. This policy would also address the University's interactions with third parties, including law enforcement organizations and companies that provide basic services and whose aid might be needed in the event of a security crisis.

3.0 PURPOSE AND OBJECTIVES OF THE POLICY

In order to realize its mission, the University is committed to making sure that a secure environment is created. This security policy aims to offer a safe, secure, and welcoming environment for all members of the university community, including students and other clients, staff, visitors, and contractors.

The aim of this policy document is to:

i. Spell out the functions, responsibilities and conditions for operations of Security on campus.
ii. Ensure that there is a coordinated system of security controls that allows the University to carry out its legal operations uninterrupted in the event of crises or emergencies.
iii. Describe how staff, students, outside parties, and visitors may help the university maintain a secure and safe environment.
iv. Achieve compliance with the university's vision, mission, and strategic plan in the management of security challenges.
v. Establish the procedures to guarantee the constant safety and security of the faculty, students, outsiders, and guests.
vi. Describe the University's obligations with regard to the upkeep of a secure environment for the University and the defence of people and property.
vii. Reduce the University's exposure to all levels of risk where the security of people and property could be in jeopardy.

4.0 POLICY AREAS

4.1 PERSONNEL SECURITY

Personnel security is the safeguarding of individuals from harm as well as the defence of university property from errant faculty, staff, and visitors. Personnel can provide security hazards and threats to the university community through intentional or unintentional behaviour, so the university must establish safeguards and regulations that must be followed by everyone

4.1.1 Policy Statement

All members of the university community must live in a safe and secure environment, and the University is responsible for making sure that everyone is aware of their security duties. The University will put in place security procedures and measures to stop anyone from taking advantage of their own weaknesses in order to compromise the university's security. Systems must be put in place so that the hiring, expiration, and termination of contracts can be closely monitored. This will help to guarantee that the proper staffs are hired and that sensitive data and/or assets are not misappropriated when employees leave the university. The University orders everyone to abide by the general guidelines given in order for this to be accomplished.

4.1.2 Procedures

The following are the procedures that must be taken to achieve the Personnel Security on campus:

i. The University Management shall see to it that employees and students receive on-going security awareness training on personnel security concerns and their effects on the university community.

ii. In order to reduce the risk of hiring criminals, people with criminal tendencies, or entering into contracts with unqualified third parties, University Management shall ensure that background checks are conducted on potential employees (permanent and contract), students, and third parties.

iii. The responsibility of University Management is to make sure that the proper individuals are hired as permanent and contract employees of the school.

iv. In order to reduce the risk of hiring criminals, people with criminal tendencies, or entering into contracts with unqualified third parties, University Management shall ensure that background checks are conducted on potential employees (permanent and contract), students, and third parties.

v. Staff and students who are experiencing difficulties should have access to guidance and counselling, according to university management. This is done to make sure that the difficulties faced by faculty, staff, and students don't turn into actions that endanger the university's security.

vi. For retirees, employees whose contracts have expired or been terminated, employees who have resigned, and third parties whose engagement with the university has come to an end, the Management shall conduct private exit interviews. This is to remind them to abide by the Confidentiality/Non-Disclosure Agreements (NDAs) they signed and to encourage them to disclose any dishonest or unethical behaviour on the part of other employees so that it may be corrected and problems that their Departments/Units are facing can be resolved.

vii. The University Management is responsible for creating broad and detailed codes of conduct for staff members.

4.2 PHYSICAL FACILITIES

For the purposes of this Policy, a Physical facility is defined as building or structure that forms part of an operational unit and are connected in location and function. Assets (people, information, and property) in University facilities need physical security measures to protect them from hostile attacks, including terrorist attacks. The security controls used to stop, discourage, detect, deny, delay, and disrupt criminal activity are known as physical security measures. It often consists of the deployment of security personnel, facilities protection measures, and access control measures.

An additional approach will be Crime Prevention through Environmental Design (CPTED), which is the physical design of the campus environment for the purpose of preventing crime and other security issues. To create a safe and secure environment for the University's mission to be realized, certain measures must be put into place.

4.3.1 Policy Statement

To protect facilities and assets from security incidents and to create a secure environment for academic and other activity, all members of the university community must implement physical security measures.

4.3.2 Procedures

The following steps will ensure that this policy is accomplished:

i. Building Security

a. All structures must have solid exterior doors that are challenging to remove or break into.
b. Solid building materials must to be used to construct exterior doors. ii. Appropriate locks that are challenging to pick or compromise must be installed on all doors.
c. Except for the last departure or emergency exit doors, all inside doors must be locked.
d. Establish key control procedures that will stop unauthorized key duplication and illicit key use.
e. Final exit door keys for buildings and facilities must be left to the security offices by an authorized permanent staff member after business hours and after all staff members have left. A copy of the keys to the last escape doors must only be kept by authorized staff.
f. All exterior doors must have steel gates or grilles installed on the interior or outside.
g. Building windows must be made of the proper glazing material, mounted in sturdy frames that are firmly fastened to the surrounding wall.
h. Window frames must have sufficient locks installed to prevent forced opening and must be locked by employees following the end of the workday.
i. All windows should be further protected by bars, retractable grilles, and shatters depending on the security threats. All windows that are less than five meters from the ground must have bars and grilles to protect them.

j. x. Secured metal cages or fences are to be used to protect electrical plants and external outdoor equipment like air conditioner units, transformers, and generators.

ii. Perimeter Security

a. Depending on the security risk to the facility, a wall or perimeter fence with a minimum height of 2.4 meters may be used to secure it. To discourage easy climbing or scaling over, perimeter fences and walls should include hostile toppings (barbed, razor wire, or electric fence).
b. To enable security patrols and observation, create a 3-meter clear zone on either side of perimeter fences or walls.
c. Perimeter intrusion detection systems need to be built, depending on the security threat and the sensitivity of the institution.
d. Install perimeter CCTV systems for monitoring, deterrence, evidence collection, and quick security response.
e. Install the proper perimeter lighting to discourage and catch trespassers at night.
f. Signage warning against trespassing and the presence of security systems must be hung or mounted to perimeter fences and walls in order to dissuade criminals and other users and to comply with legal requirements.
g. Appropriate gates with locks and well-equipped security gatehouses should be installed on facility perimeter fences and walls.
h. To prevent enemy actions, regular security inspections, routine maintenance of perimeter fences/walls, and security systems must be carried out.
i. To verify that the perimeter walls, fences, and security systems are operating properly, security officials and guards must do routine perimeter patrols.

iii. Private Hostel Security

a. Prior to allowing students to check into private hostels, the Office of the Dean of Students must confer with and receive approval from the University Security Services.
b. Private hostels cannot accept university students unless their security measures are approved and in accordance with this Policy.
c. The Office of the Dean of Students must publish a list of all private hostels that have been granted permission for University students to occupy them.
d. Students who stay in private hostels that have not been approved and made public by the Office of the Dean of Students are in charge of their own security and are not absolved of liability by the university.

iv. Deployment of Security Personnel

a. To carry out protection tasks, security officers/guards from the Security Services must be physically stationed on/inside sites. These responsibilities include patrolling, implementing access control measures, conducting searches, and testing the effectiveness of security systems.

4.3 INFORMATION SECURITY

The University deals with a lot of sensitive data (both personal and university data) that is subject to several risks and, if hacked, would have a negative impact on the institution's security and reputation. Information theft, unintentional disclosures, interception, and numerous cyber attacks are a few of these hazards.

The three characteristics of information—*confidentiality, integrity, and availability*—must be upheld in order to achieve information security. Information's confidentiality is violated if it is viewed by unauthorized individuals. When information hasn't been changed or modified without the necessary authorization, it has attained integrity. Availability of information occurs when there is a continual and uninterrupted accessibility to information by permitted users.

4.3.1 Policy Statement

The Data Protection Act (Act 843) of 2012, the Electronic Transaction Act (Act 772) of 2008, and all other rules, regulations, and laws that are in effect and binding on the University and third parties require the University Community, affiliate institutions, external clients, business partners, and contractors to protect the University's information. This protects the privacy, accuracy, and accessibility of information. All types of information under the University's control must be secured and protected from threats, cyber attacks, and unauthorized information sharing.

4.3.2 Procedures

To accomplish this policy, it is necessary to adhere to the general instructions provided below.

i. Classification of Information

a. Classified or sensitive information must be clearly labelled using the appropriate terminology.
b. All information related to the university shall be managed, classified, stored, shared, and revealed strictly in accordance with the level of classification and authority.
c. Classified and sensitive information must be communicated, preserved, declassified, accounted for, and disposed of properly.

ii. Physical Information Security

Information and Communication Technology (ICT)-using facilities and offices must implement physical control measures to thwart unauthorized access to, use of, and theft of IT equipment

iii. Awareness of Information Security

a. The university will see to it that users gain the necessary skills and knowledge to protect their use of IT systems and infrastructure.

b. The University shall see to it that workshops, seminars, and other information security awareness events are routinely held for staff, students, and other authorized users of information on the dangers, weaknesses, and retrieval of information belonging to and used by the University.
c. At all the University's colleges, institutes, departments, and units, a culture of information security must be established.

4.4 VIOLENCE ON UNIVERSITY PROPERTY

Violence is typically defined as acts that result in death, injury, or suffering. In a nutshell, there are three basic types of violence in a university setting. These include Domestic violence, Workplace violence, and violence involving students (both residents and non-residents).

Any behaviour that leads to havoc, misery, or pain in the home is considered domestic violence. Abuse of both the mind and body is included.

When someone is abused, intimidated, or assaulted at work, this is referred to as a workplace violence event. It involves physical assaults, such as physical harassment, stalking, theft, robbery, kidnapping, and assault, as well as verbal abuse and threats.

Student-related violence is defined as any behaviour by students that involves the use of physical force or not, with the use of any instrument or object or not, with the intention of injuring, frightening, or inflicting suffering on a fellow student, staff member, or third party, or to cause damage to properties inside or outside the University. It covers bodily harm such as fighting, bullying, stalking, sexual harassment, kidnapping, theft, and robbery, among other things. It also encompasses psychological and emotional abuse.

Violence in the workplace, in the home, and against students also includes killings and suicides. Violence is unavoidable at a university where there are many students from different racial and ethnic origins. Therefore, it is crucial that the proper actions be taken to lessen the impact of domestic violence, workplace violence, and violence against students, as well as the security challenges that follow. Thus, this would guarantee the tranquil and welcoming environment that the University requires to operate effectively.

4.4.1 Policy Statement

The University must maintain a secure atmosphere, thus any type of violence—physical, psychological, emotional, or otherwise—will not be tolerated. Harassment, verbal abuse, threats, bullying, the use of "drivers of violence," and disruptive

behaviour including alcoholism, drug misuse, and carrying a weapon are unacceptable behaviours and practices that will not be permitted.

Violence-related problems and occurrences must be considered as major security threats, and offenders must face disciplinary action, which may include administrative consequences like dismissals and possible legal action. The University urges staff, students, and other parties involved in violent events to report them to the proper authorities, who will handle them promptly and in the strictest confidence. Violent incidents can take any shape, including physical, psychological, or emotional, and can involve staff, students, or other parties.

4.4.2 Procedures

To guarantee that a violent-free environment is established, all members of the university community, including staff, students, and outside parties, shall abide by the aforementioned rules.

i. Under the supervision of CCTU Counselling Centre (CCC), the University shall hold at least once a year a Violence Awareness Training (workplace/domestic /student-related violence) for all employees and students. Procedures for reporting and resolving incidents must be covered in the training.

ii. The Dean must designate Focal Persons at the School who will serve as lecturers in the various departments and receive training in the detection and handling of violent incidents involving staff and students. Registrars must be appointed as Focal Persons for their units in non-academic departments.

iii. Anyone who has seen or heard of conduct that constitutes threats, harassment, or other undesirable behaviour toward people should report it to the appropriate focal person or head of department for prompt inquiry and resolution.

iv. As soon as feasible, have anyone making threats of any kind or acting violently or inappropriately be removed from the premises of the facilities with the assistance of security officers from the University or the Ghana Police Service (as needed). Such people shouldn't be permitted inside the facility until the preliminary investigations are finished.

v. Victims of violence must document such instances and support their complaints with specific information and supporting documentation.

4.5 TRAVEL SECURITY

The duty for travel security at the University is shared by the traveller (workers, students, and other parties), the various Heads in accordance with the University's travel policies, the Security Services, and the destination unit/office or host.

As part of the University's mission, staff, students, and outside parties may be required to travel for work-related or official purposes both domestically and abroad. They are exposed to dangers that could endanger their health and safety and cause the loss of priceless assets and information. Through the actions and inactions of employees, students, and third parties operating for and on behalf of the University, a lack of effective travel security protocols to safeguard the safety and security of travellers may place legal liability on the University.

4.5.1 Policy Statement

The University is responsible for ensuring the safety and security of its personnel, students, and third parties when on local, national, and international travel/assignments (both official and unofficial). It must put in place the right security measures to protect travellers from theft and other crimes while also ensuring their safety and security. The University wants to make sure that travels are free of security issues or that the effects of incidents are reduced to the absolute minimum.

4.5.2 Procedures

To maintain travel security, the University asks everyone to adhere to the measures listed below.

a. Travellers

i. Principal Officers of the University must avoid traveling together in the same mode of transportation as much as feasible (Car, aeroplane, train, ship). To provide the highest level of security controls, the University's Travel Desk must coordinate with the Security Services to plan the travel plans of Principal Officers.
ii. All travellers must have all the necessary travel-related documents (passports, proof of immunizations, identification cards, travel insurance, etc.) in their possession.
iii. All overseas travellers should make an effort to learn about the political, social, and economic environments of their destinations.
iv. When traveling for business or leisure, prohibited items must not be transported.
v. Any sensitive data and information on all personal and university electronic devices, including phones, laptops, and tablets, must be backed up and encrypted to prevent theft.
vi. For official or unofficial travel, staff must obtain authorization and security clearance from the relevant authorities.
vii. Prior to traveling, all student group outings must have initial permission and approval from the Dean of Students. The travellers must obtain a final security

clearance from the University Security Services prior to leaving after receiving approval.

viii. When arriving at their destination, travellers must notify the Security Services and the appropriate authorities, and they must also report to them when they return to campus.

ix. Prior to leaving on official business, travellers must ask the Security Services for security advice, tips, and briefings.

x. Travellers must refrain from engaging in behaviour that would damage the reputation of the university.

b. Heads of Department

The heads of department shall

i. Before letting any travellers (official or not) start their journey, make sure they have all the necessary approvals, travel plans, and security clearance.

ii. develop and maintain a tight relationship with the University Security Services until the travellers' return.

c. University Security Services

The University Security Services shall:

i. Provide security clearance prior to trip permission and on-demand protection while traveling.

ii. Give travellers official and unofficial emergency contact numbers along with safety and security briefings, advice, and ideas.

d. Destination Unit/Office/Host

i. Official travellers and the University Security Services are to establish a liaison through a university unit or office off-campus or abroad.

ii. Make sure the travellers are welcomed in a safe and secure manner when they arrive at their destination. These arrangements include things like safe housing, safe transportation, and secure airport arrival procedures.

iii. When visitors arrive, brief them about local security. The in-country or in-town emergency protocols should be covered in this briefing.

iv. The University will work with the host institution to safeguard the safety and security of its staff, students, and other visitors, and will offer support where it is needed in the areas of law, medicine, and immigration.

v. The University must make sure that the hosting institution agrees to be held accountable for any security lapse that causes harm, a loss of life, or damage to property.

4.6 VISITOR SECURITY

Visitors to the University premises can provide security risks if they are not handled and controlled, and they may also run across security obstacles. One of these threats is the unchecked entry of criminals into facilities and controlled locations for illegal activity. The University is vulnerable to illicit visitor activity and the associated security and safety hazards to its staff because of the magnitude and volume of visitors it receives.

There are four basic categories into which anybody attending any institution inside the University could be placed: Official visitors, Unofficial visitors, Staff and students traveling to other locations for personal reasons and intruders who plan to conduct crimes.

4.6.1 Policy Statement

The University is responsible for ensuring that a safe and secure environment is established to safeguard its staff, students, and third parties from criminals and to forbid unauthorized access to university premises. To lessen the threats to security and safety caused by malicious and unauthorized visitors, it must develop visitor management systems and procedures.

4.6.2 Procedures

To ensure the highest level of visitor security on all University campuses and in all University facilities, all staff, students, and outside parties are obliged to abide by the protocols laid out.

i. Each facility must provide a general reception room or space on the ground floor where guests can be greeted and screened. Principal Officers and other high profile executives who work in high-risk management positions should have their own greeting spaces.
ii. In every building, a waiting space or room for visitors should be set up with CCTV cameras. The design of new structures must contain a waiting space or room for guests.
iii. Visitors must be recognized by sponsors or hosts in order to enter facilities. Sponsors and hosts must notify the venue in advance of any guests attending the reception. If this is not done, receptionists are to ask the sponsor or host for permission before allowing any visitors entrance to the waiting room or area.
iv. Prior to being transported to the waiting area where they will meet their sponsors or hosts, visitors will be directed to the reception. It is strictly forbidden to host visitors in offices unless formal authorization has been granted. Sponsors and hosts are responsible for seeing that their guests are checked out at the front desk.
v. All visitors to facilities and controlled areas must check in at the front desk and get an identification tag that must be worn around the neck the whole time they are within or near the facility.

vi. The phrase "VISITOR" must be written plainly on visitors' identity tags, together with easily recognizable unique numbers.
vii. Visitors and workers may be subject to security screenings and inspections as necessary with their permission. Visitors and staff who refuse to give their approval will not be allowed into the institution. The searches must be conducted in accordance with established protocols. Prior to allowing visitors inside the premises, sponsors and hosts must inform them of any potential security search or inspection needs.
viii. Controlled facility entry and departure points must be marked with signs alerting visitors to searches and prohibited goods.

4.7 EVENT SECURITY

The security precautions put in place for workers, students, guests, outsiders, and to protect property before, during, and after events are known as event security. Large events including congregation, matriculation, investitures, public lectures, exams, demonstrations, processions, Hall Week celebrations, sporting events, religious meetings, etc. are all covered by the university's event security program. On all University campuses, this also applies to minor occasions like weddings, funerals, parties, etc.

Large crowds present during such events provide a number of security problems that could jeopardize the university's serenity. Therefore, it is necessary to manage these situations so that the University can continue to be a calm and welcoming place.

4.7.1 Policy Statement

The University is responsible for maintaining a secure, tranquil, safe, and welcoming environment for its staff, students, outsiders, and guests attending events held on its campuses. The University will make sure that any events held on its campuses are planned in a calm setting with the least amount of security concerns and greatest amount of safety.

4.7.2 Procedures

All stakeholders must adhere to these guidelines.

i. Every event planned on campus must get university approval. The authorization must be in writing and include the laws, rules, and ordinances that regulate the facility's release and use for the event.
ii. Before being allowed to take place, any events planned by students on campus must receive approval from the Office of the Dean of Students.
iii. At least seventy-two (72) hours before the event starts, all authorized events on university facilities must be brought to the attention of the University Security Services.
iv. In accordance with the Public Order Act of 1994 (ACT 491), event planners of special events, such as demonstrations, processions, Hall Week celebrations, etc.,

that are to be held on university campuses must obtain permission from the university fourteen (14) clear days in advance and notify the Ghana Police Service.

v. Event organizers are required to request security assistance from the University Security Services and the Ghana Police Service (if necessary) after gaining authorization in order to protect the events.
vi. Following event authorization, the Estate Office and Security Services must be called for any necessary discussions to ensure that any linked business activities run smoothly. This is to guarantee that campus activities that will draw retailers of goods, food and beverage vendors, and promotional sales are well-organized for reasons of space management and security.
vii. Event organizers must implement access control measures, such as event identification badges, press tags, signage, search and screening procedures, etc., in coordination with the Security Services to identify and deter unauthorized attendees and/or criminal activity before, during, and after events.
viii. Event organizers, estate offices, and security services must work with the necessary agencies to set up emergency and backup plans before, during, and after the events.
ix. If the event was organized by students, the event organizers must submit a Post-Event Report to the Dean of Students, University Security Services, and the Estate Office.

4.8 SEXUAL HARASSMENT,

To avoid sexual harassment escalating into severe criminal acts like sexual assault, rape, defilement, and to a greater extent suicide, it is critical that sexual harassment in an organization be dealt with appropriately and promptly. These affect the University and the staff, students, visitors, and other parties' health and safety, among other things.

4.8.1 Policy Statement

The University is required to provide a safe and secure environment free from sexual harassment and incidents connected to security. Sexual harassment will not be tolerated, and it will be dealt with quickly and firmly when it does.

In order to avoid and lessen the effects of criminal activity resulting from sexual harassment occurrences, the University will implement extra security measures. Additionally, it will offer the support required in cases of criminal activity stemming from sexual assault and harassment.

4.8.2 Procedures

To accomplish the goal of this Policy, staff, students, outside parties, and visitors to the University shall adhere to the below-listed procedures.

i. All staff, students, and outside parties must attend orientation sessions on sexual harassment and violence that the university administration conducts.
ii. All sexual harassment incidents must be reported to an Anti-Sexual Harassment Committee, but should be reported seriously to the University Security Services and the Police if it involves sexual violence and other connected criminal activity.
iii. In addition to promptly reporting occurrences of sexual violence (assault, rape, etc.), victims are required to save, preserve, and provide any relevant evidence to the police in order to aid in investigations.
iv. When sexual harassment may compromise workplace security and safety, action must be taken to bar the alleged abuser from entering any University facilities where the victim resides. The victim is to receive security protection while on University property, depending on the circumstances.
v. vi. When partners/couples work in the same office/unit yet sexual harassment may compromise workplace safety and security, efforts must be made to remove one party from that office/unit.
vi. vii. Sexual harassment victims must notify university management of any restraining or protective orders they obtain as a result of criminal proceedings and want to have enforced on university property. The Legal Department and Security Services will then be notified by Management of the restraining or protective order.
vii. To avoid being a victim of sexual assault, everyone must take personal safety and security precautions.

4.9 DRUG ABUSE/DEPENDENCE,

A pattern of dangerous use of any chemical (solid, liquid, or gas) for mood-altering objectives is referred to as substance misuse. These substances may be legal or illicit. These substances consist of:

i. Illicit drugs (narcotics), including heroin, marijuana, and opiates like cocaine.
ii. Amphetamines, synthetic opiates like tramadol and pethidine, and other stimulants and depressants.
iii. Sniffing volatile solvents like snuff and shoe polish.
iv. Additional prescription medications such benzodiazepines, codeine, etc.
v. Alcohol and drinks that are related to it.

In addition to having an adverse impact on users' health, drugs can change users' mental states, which can lead them to act in ways that are illegal or risk the safety and security of everyone. The user's and society's social, economic, and financial well-being are also affected by substance abuse or dependence. It is necessary to take action to stop employees, students, visitors, and other individuals from using these substances due to the detrimental effects and criminal repercussions on members of the university community.

4.9.1 Policy Statement

The University is responsible for maintaining a secure, safe environment free from substance abuse or dependence. The University will seek to prevent incidences of substance abuse and dependency on its campuses and in the surrounding area in an effort to sustain a productive workforce and student body. The university will not tolerate any type of substance abuse, and offenders will face disciplinary action, which may include reporting them to the relevant law enforcement agencies. A Health and Safety Policy has been created as a result for everyone's compliance. The purpose of this Security Policy is to implement extra security measures to prevent substance abuse on or off its campuses in furtherance of the aforementioned Policy.

When appropriate, the University will provide support and help to those who misuse drugs.

4.9.2 Procedures

All University employees and students, as well as visitors and other parties must follow the mentioned procedures.

i. Under the supervision of the CCTU Counselling Centre (CCC), the University must host seminars, educational talk shows, workshops, etc. on substance misuse and dependency at least once a year for all staff and students.
ii. The university will encourage the general public to report faculty and students who use, traffic, or possess illegal drugs or other substances improperly on or near university campuses. To that end, anonymous hotlines and media outlets will be created.
iii. The University must designate or nominate individuals to serve as focal points for complaints concerning substance abuse and related violations at the departmental and unit levels.
iv. The Focal Persons will receive training from CCC on how to manage and address reported cases.
v. The University will launch investigations into any reported incidences of substance abuse or related situations as soon as possible in order to take appropriate disciplinary action. During and during the investigation processes and/or disciplinary action, rigorous adherence to protection and confidentiality of suspected culprits, misusers, and/or witnesses is required.
vi. CCC will train heads of departments to recognize and handle early warning indicators of potential substance abuse by faculty and students.
vii. Persons who possess, cultivate, produce, provide, administer, and/or use illegal narcotics on or near the University's immediate property must immediately be reported to the Ghana Police Service. The Office of the Dean of Students must be notified if the person is a student.
viii. The CCC will design a program targeted at helping substance abusers in consultation with the pertinent stakeholders, experts, and professionals.
ix. The University shall conduct pre-employment drug testing for applicants to ensure that they are not substance abusers.

x. Staff and students who have a reasonable suspicion that they may be abusing drugs or other substances are to be subjected to drug testing, with necessary action being taken depending on the results of the tests, in order to maintain a drug-free, conducive, and peaceful work/study environment at the university.

4.10 FIRE SAFETY

The act of putting precautions in place to prevent fires from starting and potentially causing the loss of life or property is known as fire safety. Natural calamities, careless behaviour, and criminal activity are all potential causes of fire. Therefore, both safety and security control mechanisms are needed for fire safety management. Security control measures include actions for the efficient operation of fire emergency response operations as well as the implementation of fire safety preventative measures to safeguard lives and/or property.

The University runs the risk of losing staff members due to accidents, fatalities, and fire damage to buildings. This has an impact on the university's budget, operations, and human resources. The University must put in place fire safety measures that are supplemented by security and safety controls in order to prevent and manage this.

4.10.1 Policy Statement

The University is responsible for maintaining all of its facilities in a secure environment free from fire occurrences. To lessen the possibility of fire accidents occurring on university property and its detrimental effects on people and property, the university shall implement precautionary and although they are used interchangeably, the terms crisis and emergency refer to different situations. A crisis is a situation that threatens an organization's survival and calls for quick action to avoid the organization's operations from completely ceasing. Extensive violent protests, pandemics, catastrophic fire explosions at strategic assets, and extreme weather disasters and circumstances are a few examples. On the other hand, an emergency situation requires rapid action but is not as dangerous as a crisis because there is no imminent threat to health, life, or property.

4.10.2 Procedures

Members of the University Community are required to adhere to the listed fire safety procedures in addition to the Health and Safety Policy, which is already in effect.

i. The university is required to create a fire safety plan, which must contain things like a fire risk assessment, designated escape routes and exits, gathering areas in case of an emergency, etc.
ii. The University Fire Unit will train all university staff members in fire safety awareness in cooperation with colleges, faculties, departments, and units.
iii. The Fire Unit will regularly hold fire emergency drills for all employees, students, and other parties in cooperation with pertinent departments (Security Services, Health Services, National Fire Service, etc.).

iv. Facilities' fire safety equipment must undergo routine maintenance and inspection.
v. According to instructions and recommendations from the Fire Unit, chemicals and other fire-hazardous products housed at facilities must be properly stored and protected.
vi. Security guards and officers stationed at facilities are required to monitor the observance of fire safety regulations and notify facility officers/managers of any fire safety hazards for prompt corrective action.
vii. Fire extinguishers, smoke/heat/flame detectors, automated water sprinkler systems, fire alarm systems, fire hydrants at building areas, emergency exits, fire evacuation plans, etc. are required to be installed in all University-owned buildings.
viii. All University-owned vehicles must be equipped with fire extinguishers and adhere to DVLA safety regulations.
ix. The University shall have complete fire insurance on all of its structures, vehicles, and people (staff, students, and authorized individuals).

4.11 CRISIS MANAGEMENT

Although they are used interchangeably, the terms crisis and emergency refer to different situations. A crisis is a situation that threatens an organization's survival and calls for quick action to avoid the organization's operations from completely ceasing. Extensive violent protests, pandemics, catastrophic fire explosions at strategic assets, and extreme weather disasters and circumstances are a few examples. On the other hand, an emergency situation requires rapid action but is not as dangerous as a crisis because there is no imminent threat to health, life, or property. Emergency conditions do not cause the organization's operations to completely cease. Examples include epidemics, strikes, and fire outbreaks. The crises or emergencies in question could be brought on by both natural and man-made occurrences. To avoid and/or lessen the effects of crisis and emergency circumstances, the University will require that safety and security interventions and measures be put in place.

4.11.1 Policy Statement

The university must implement measures to guarantee a secure, tranquil, and stable atmosphere that is good for both teaching and learning. The University must also take precautions to prevent the loss of life or damage to property in times of crisis or disaster. In order to safeguard the safety and security of staff, students, and other parties during crises and emergencies, the university will implement an "Emergency Action Plan" that includes prevention, response, and recovery measures.

4.11.2 Procedures

These procedures must be followed and complied with by all members of the university community:

i. A "Crisis/Emergency Action Plan" for the whole university must be created by the university. Early warning systems, emergency reporting and communication procedures, reaction and evacuation procedures, and securing and recovery processes are all part of this strategy.
ii. To coordinate and handle crisis and emergency situations on and/or off campus, the university must create a Crisis Management Team (CMT). The Security Services Management Committee, representatives of the University Health Services, the University Relations Office, the CCTU Counselling Center, and NADMO are all members of the CMT.
iii. For their facilities, Schools, departments, and Halls of Residence must create unique and detailed Emergency Action Plans (EAPs). The direct coordination and liaison with crisis/emergency responders in their operational domains (Fire Service, Law Enforcement Agencies, Medical Services, NADMO, etc.) must be part of this.
iv. Departments, Schools, and other organizations must create Business Continuity Plans (BCPs Facilities must install emergency response equipment, such as standby electrical generators, fire detection and extinguishing systems, public address systems, and emergency alarms.
v. The University will help to supply Personal Protective Equipment (PPE) for the protection and safety of personnel during medical emergencies such epidemics, pandemics, etc.
vi. During such emergencies, all staff on university property must wear PPE, follow all safety procedures, and comply with all laws.
vii. The University Security Services will dispatch security guards to handle crisis and emergency situations with the help of the appropriate security agencies.). The University must practice its business continuity and incident response plans so that they can function normally in the event of an emergency or crisis.

5.0 DUTIES AND RESPONSIBILITIES

The security on campus is everyone's shared responsibility; nevertheless, the following are entrusted with specific strategic security tasks and responsibilities:

5.1 THE UNIVERSITY COUNCIL

The University Council must finally approve all university policies. They must also see to it that the relevant organizations charged with carrying it out are correctly identified and given the resources they require. The Council is responsible for ensuring that administration carries out all policies to safeguard the security and safety of students, employees, and visitors while they are on campus as well as the protection of university property both inside and outside the campus.

5.2 VICE CHANCELLOR'S OFFICE

The Vice-Chancellor's office is in charge of creating, putting into effect, overseeing, and, if required, reviewing the current University Security Policies. The Office is

responsible for making ensuring that enough resources are available to carry out this policy.

5.3 REGISTRAR'S OFFICE

All administrative procedures for the application and oversight of this Policy must be carried out, and that is the Office of the Registrar's obligation.

5.4 DIRECTORATES, DEANS, AND HALL MASTERS/WARDENS

The Security Policy will be implemented more easily in Colleges, Directorates, Faculties, Units, etc. by the Offices of Directors and Deans, etc. The Offices must make sure that the Departments have the assistance and resources they need to carry out the Security Policy. Priority should be given to steps that will increase security in crucial locations. Where necessary, specialized training to reach operational standards that are acceptable should be supported with adequate funding. The Offices are responsible for ensuring that new construction and renovated facilities meet security requirements.

5.5 HEADS OF DEPARTMENT

The heads of departments are crucial in fostering improved security. They are in charge of making sure the Security Policy is followed. The actual duties will change depending on the type, location, and nature of Departments' activities. In accordance with this policy, Heads of Department can be assigned a number of specific duties, including:

i. Make sure the Security Policy is available to staff and students, and that they are familiar with it. Pay particular attention to the sections that relate to the operations of each department.
ii. Under the direction of the Security Services, conduct a security risk analysis of the Department and take steps to mitigate any security concerns.
iii. Ensure that all employees and students in their Departments are aware of and taking responsibility for their security obligations as stated in this Policy.
iv. Ensure that the Departments' employees and students adhere to the application of this security policy.

5.6 THE HEAD OF SECURITY SERVICES

The Head of Security Services is in charge of carrying out, coordinating, and overseeing the security protocols and safety measures described in this Policy. His duties will encompass, but not be limited to, the following:

i. Ensure the processes and procedures required to operationalize this policy are put in place.
ii. Ensure that the Policy's administrative, financial, personnel, and logistical approvals are coordinated in order to assure successful implementation.

iii. With the help of departmental heads, conduct security risk analyses and provide the appropriate recommendations for the implementation of security measures.
iv. Perform security audits and surveys of security systems and procedures to evaluate their efficacy, find weaknesses, and implement corrective action in accordance with this Policy.
v. Report on the implementation of this policy on a regular basis.
vi. Ensure that the University and other pertinent stakeholders, such as law enforcement organizations, emergency services, etc., continue to have a positive working relationship.

5.7 STAFF

Every member of the staff must make an effort to understand and abide by this university security policy.
In addition, they must provide the help and cooperation that is required in accordance with this policy's security guidelines in times of crisis, emergency, and security.

5.8 STUDENTS

In addition to the rules of the University outlined in the Students Guide and Code of Conduct, all students are expected to follow and abide by this Security Policy.

During crisis, emergency, and security circumstances, they must also provide their best cooperation while adhering to the security protocols outlined in this policy.

5.9 VISITOR AND THIRD PARTY LIABILITY

When on University property, visitors and third parties (such as conference participants, attendees of external events, subcontractors, external consultants, etc.) are expected to follow this Policy as well as the general University regulations and to conduct themselves appropriately for both their own security and the security of others.

They are generally accountable for the security of University facilities while on campus and must take security concerns seriously. They must, in particular, adhere to security protocols intended to safeguard people and property. They must always wear their ID badges when it matters.

6.0 THE SECURITY SECTION

The need for security services at Cape Coast Technical University since its inception in 1984 could not be dispensed with. Consequently, watchmen were recruited to cater for the security situation on campus. The continued recruitment of watchmen gradually led to the formation of the Security Section, which was first headed by the first Chief Security Officer.

Today, the Security Section has become an essential unit within the University, which is responsible for discharging security duties in and around campus as defined by the *Statues*. The basic functions of the Security Section are to preserve peace, protect life and property, prevent crime and ensure order.

6.1 VISION

The vision of the Technical University Security Section is to provide adequate and protective security and expert guidance on security issues to the Technical University Community. To achieve this vision, day and night patrols are organised to ensure that life and property are protected at all times.

6.2 MISSION

The mission of the Technical University Security Section is to ensure the safety and security of lives and properties of resident students, teaching and non-teaching staff and others who stay within and outside the Technical University Communities. This mission is achieved through prevention, surveillance, intervention, training and education. Also, monitoring and risk assessment are conducted to provide help and guidance to the entire Technical University Community with a commitment to serve with excellence by treating teaching individual with compassion and respect.

6.3 PRINCIPLES AND VALUES OF THE SECURITY SECTION

The security section has the following principles and values:

i. Campus Security Section is an essential unit employed by the Technical University authorities to discharge security duties in and around campus.
ii. The prevention function applicable to both crime and disorder is paramount.
iii. Laws and regulations enforcement must be impartial.
iv. Force is employed only when persuasion fails and it must be the minimum necessary to achieve desired end.
v. Courtesy, friendliness and helpfulness must be shown to all staff, students, resident of the Technical University community and the authorities regardless of class or position as well as to visitors.
vi. The Security Section has no judicial function and the decision of guilt or innocence and the punishment of offenders are not the responsibilities of the Security Section.
vii. Preservation of peace and protection of life and property on the Technical University campus are the security function to be discharged regardless of personal danger.

6.4 RATIONALE FOR CAMPUS SECURITY

Prevention of crime is considered more important than its punishment because the property of the Technical University as well as the safety of the Technical University community, peace on campus and every other objects of the Security Section will better be achieved by prevention of crime than the punishment of offenders after they have committed a crime.

6.5 FUNCTIONS OF THE TECHNICAL UNIVERSITY SECURITY SECTION

The main functions of the Security Section of the Technical University are:

i. Protection of life and property of the Technical University
ii. Detection and prevention of crime on the Technical University campus
iii. Recommendation for apprehension and prosecution of offenders
iv. Preservation of peace and good order on the Technical University campus
v. The due enforcement of all laws and regulations of the Technical University with which is directly charged.

6.6 ORGANISATION AND ADMINISTRATION OF THE SECURITY SECTION

The Campus Security Section shall be headed by the Head of Campus Security and assisted by a Deputy Head of Security Section. There shall be two Line Officers, one personnel in charge of Operations and the other in charge of Intelligence. The Head of Intelligence shall report to the Security Head through the Deputy Head of Security. Below the two line Officers shall be Security Officers who shall largely perform bet functions in the following categories: Security Guards, Assistant Security Guards, Guard Grade I and II.

The Security Section of the Technical University shall consist of the following

- Head of Security
- Deputy Head of Security
- Principal Security Officer, Intelligence
- Principal Security Officer, Operations
- Senior Security Officer
- Security Officers
- Administrative Officer

1. Head of Security

The Head of Security shall be the head of the Security Section and shall be subjected to directives of the registrar. He /She will be responsible for exercising general day to day supervision over the operation and administration of the Security Section

The Head of Security shall command the Security Section with the assistance of officers of all ranks. He / She may delegate to any member of the Security Section such functions as he/she may deem fit.

2. Deputy Head of Security

There shall be a Deputy Head of Security who shall assist the Head of Security and shall act as head in the absence of the Head of Security.

3. Principal Security Officer, Intelligence

There shall be a Principal Security Officer in charge of Intelligence. He / She shall be responsible for the intelligent gathering and shall report directly to the Chief Security Officer.

4. Principal Security Officer, Operations

There shall be a Principal Security Officer in charge of Operation. He / She shall be responsible for operational duties in and around campus and shall report directly to the Head of Security.

5. Senior Security Officer

There shall be Senior Security officers who shall assist the Principal Security Officer

6. Security Officers

There shall be Security Officers who shall be responsible for men and women on the beat.

7. Administrative Officer

There shall be an Administrative Officer who shall be appointed by the Vice Chancellor on the advice of the Registrar.

These Officers shall be in the Senior Staff category of the Technical University.

8. Other ranks

There will be other Officers, such as Assistant Security Guards, Senior Guards, Guard Grade I, II who shall be in the Junior Staff category.

7.0 VIOLATION OF THIS POLICY

Anyone who violates this policy could face administrative, criminal, and legal repercussions. This includes members of the university community, consultants, contractors, and clients of the university.

8.0 CONDITIONS FOR OPERATIONS

SECTION 5 DESIRED ATTRIBUTES

i. **Efficiency and Thoroughness:** A Security Officer shall know his/her job and always be prepared to learn. An ignorant Security Officer and one who shirks responsibility is a disgrace to him/herself, his Superior Officers and the Technical

University community, and shall be dealt with according to the laws of the Technical University.

ii. **Courtesy:** A Security Officer shall always be polite, no matter how rude a person may be to him/her. Keep your temper and sense of humour.

iii. **Integrity:** The Security Section must have the trust of the Technical University community or the authorities. A security staff must also be trustworthy. Every complaint must be properly heard and investigated.

iv. **Smartness:** A Security Officer shall be smart in uniform, which is an outward sign of mental alertness. The Technical University community and the authorities shall judge a Security Officer first by his/her appearance and so it is important that a Security Officer's appearance is always a credit to the Section.

9.0 SECURITY OPERATIONS

9.1 DEFINITION OF BEAT

Beat is defined as a portion of land/area allotted to a Security Guard to patrol either by day or night.

For Security purposes, there shall be two types of Beat: namely; Fixed and Patrol

a. Fixed Beat in this case the Officer/Officers will be stationed at one place, whiles
b. Patrol beat in this case the Officer/Officers shall move around a designated area.

9.2 OBJECTS OF BEAT DUTIES

The objectives of the Beat include

a. For the good order of the area
b. Protection of life and property
c. Prevention and detection of crime

9.3 REQUIREMENTS FOR BEAT OPERATIONS

Beat operations basically must adhere to the following requirements:

a. A Security Guard must parade with other men at the appointed time to study current matters relating to his beat.
b. He must be sober, properly dressed and equipped with long baton, whistle and torchlight.

c. In order to walk a beat properly, a Security Guard shall walk at least two and half miles an hour.
d. He must visit all the sides of the streets and get unsecure offices or buildings secured in his area.
e. He shall not loiter or gossip, but to walk beat continuously and regularly with eyes and ears open and mouth shut.
f. He must move smartly and not slovenly.
g. He must answer all questions with civility and good temper.
h. He must act quietly and discreetly, not to interfere unnecessarily, but when the need arises, showing firmness and discretion.
i. He must ensure that doors, window and places through which a thief might enter or obtain access are properly secured.

9.4 CONDITIONS FOR A SECURITY GUARD TO LEAVE HIS BEAT

A security guard may leave his/her Beat:

a. When he/she is properly relieved.
b. When his assistance is required by another Security Guard
c. When he/she hears the cries of 'murder' or when he/she is satisfied with information received that a crime has been or his about to be committed.
d. In case of illness, he/she should report at once at the Technical University hospital or inform the Duty Supervisor at the charge office or some of the security guards on adjoining beats in order to keep an eye on his beat during his absence.

9.5 CHARGE OFFICE

a. All cases and complaints shall be reported or made to the charge office
b. It shall be the duty of the station orderly and the Duty Supervisor, any to receive all complaints, keep the Chief Security Officer informed of all cases and refer all genuine complaints to the Intelligent Unit.
c. The Station Orderly or the Duty Supervisor shall take charge of all the suspects brought to the charge office and prevent their escape.

9.6 DUTIES OF THE STATION ORDERLY

a. He/ She shall be responsible for the making of all necessary entries in the station diary during his tour of duty.
b. He/ She shall inform the Chief Security Officer immediately of any report of crime, accident or unusual occurrence is received.

c. In the absence of the Duty Supervisor, he/she shall be responsible for the safety of all articles on charge in the charge office and of any suspect detained.
d. He/she shall be responsible for the receipt and recording of all official telephone or message whilst on duty.

9.7 STATION DIARY

a. The Campus Security Office shall keep a Station Dairy.
b. The station diary, as a book kept at the charge office, shall contain all entries of occurrence, complaints, report of crime, accidents, property received, persons arrested, movements of staff and other usual occurrences.

9.8 COMMUNICATION SET-UP

Means of communication available in Security Set-Up shall be:

a. Telephone
b. Wireless or Motorola Set
c. Messenger
d. Whistle

9.9 HOW TO USE A TELEPHONE TO GIVE MESSAGE

a. Hold mouth-piece close to your mouth
b. Speak directly into it and do not shout
c. Announce your rank, name and location
d. Speak distinctly and slowly
e. Exercise care with difficult words and spell names if necessary
f. Find out who answers the telephone

9.10 ACTIONS IN CASE OF FIRE OUTBREAK

a. A Security Guard on duty seeing an office, bungalow or any building or any Technical University property on fire, shall first raise an alarm.
b. He/she shall sermon the assistance of the community or the public
c. He/she shall inform or telephone to the charge office and the Fire Service Station.

9.11 ACTIONS AT THE TIME OF FIRE OUTBREAK

a. To save life and property

b. To help in extinguishing the fire
c. To prevent theft of property
d. To enquire into the origin of the fire

9.12 ACCIDENTS

In case of an accident on the Technical University campus, the Security Guard should pay attention to the following:

a. The welfare of the injured person should be paramount
b. Where the injury is serious, call for an ambulance or the injure persons should be sent to hospital for medical treatment immediately.
c. Inform the security charge office
d. Take names and addresses of driver(s) involved in the accident including address, driving licenses number, number plate of the vehicle, insurance certificates, etc.
e. Note down the class and identifiable marks of vehicles
f. Take names and addresses of all possible witnesses.
g. Inform the police about the accident.

10.0 POWERS AND DUTIES OF A SECURITY OFFICER

10.1 ARREST

A Security person may arrest any person who commits the following offences in his presence (within the boundaries of Cape Coast Technical University) namely:

a. Any offence involving the use of force
b. Any offence whereby bodily harm is caused to any person
c. Any offence in the nature of stealing or fraud
d. Any offence involving injury to property of the Technical University
e. Any offence involving injury to property owned by, or in the lawful care or custody of an officer
f. Any person whom he reasonably suspects of having committed any of the offences indicated above (such suspicion must be reasonable)
g. Any person who commits any of the offences indicated in the Statute of the Technical University and the Students' Handbook
h. Any person whose conduct/behaviour can have negative impact on the peace, health, security, morality and the image of the Technical University.

10.2 GENERAL RULES ON ARREST

a. In making an arrest, the Officer shall actually touch or confine the body of the person to be arrested, unless the person submits to custody verbally, or by conduct.

b. The Officer shall immediately inform the person arrested in a language that he / she understands of the reason for her/his arrest and his fundamental rights.
c. The dignity of persons arrested must be upheld – torture, cruel, inhuman or degrading treatment must be avoided.
d. Any person arrested under the following conditions must be handed over to the appropriate authorities immediately.

10.3 SEARCHES AND SEIZURES

a. A Security Officer may search a person if he/she has reasonable cause to believe that a person has concealed on himself or conveying an article which has been stolen, unlawfully obtained or in respect of which a criminal offence has been is about to be committed.
b. Searches of persons shall be limited to pat-down or frisk until there is the need for detailed search.
c. An Officer shall search an arrested person to recover contrabands or items that may be helpful in further investigations
d. The search shall be made with strict decency and where a woman is to be searched, the search shall be made by a woman and vice versa.
e. A vehicle entering or leaving campus may be searched if the Officer has reasonable believe that it carries a contraband or is being used to covey a stolen item or property of the Technical University without the requisite permit from authority.
f. The search of a dwelling shall be done only with expressed permit of the appropriate authority. Such searches should be with *decency.*
g. Searches are not to be conducted in the company or presences of a complainant.
h. All searches must be done during daytime (6:30 a.m. – 6:30 p.m.) unless otherwise authorised by a Superior Officer.
i. An officer shall bring before his Superior Officer all articles or items seized under search as soon as possible. Under no circumstance should items be kept by the officer who conducted the search.
j. Vehicles used in criminal acts on campus shall be impounded for further investigations.

10.4 TRAFFIC CONTROL ON CAMPUS

a. It shall be the duty of Security Officers to control vehicular movement on campus. However on special occasions when a public function is to take place (Congregation, Matriculation and Open - Days) the Security Section shall liaise with the Regional / District Commanders of Police to plan traffic control for the event.

10.5 WEAPON USE

10.5.1 Definition

a. A weapon is any instrument or device used in attack or defence in combat or fighting such as a sword, rifle, or cannon.
b. Anything used against an opponent or an adversary.

10.5.2 Circumstances Under Which Weapons May Be Used

The use of firearms is not allowed on campus. However, the use of control devices or restraint devices that are not lethal such as truncheons, taser, mace, stun guns or baton, pepper spray may be allowed under the following circumstances:

a. When an Officer is attacked by an armed criminal
b. To effect the dispersal of riotous crowd
c. To prevent the escape or effect the arrest of a fugitive
d. To prevent felon from committing fleeing
e. When an Officer's life is in immediate danger.

11.0 CRIME SCENE MANAGEMENT AND EVIDENCE GATHERING

11.1 GENERAL PRINCIPLES

a. A Security Officer must note that, any action or activity either by the Officer or citizens, of the environment can alter or destroy the original scene.
b. The Officer must approach the scene with caution
c. The Officer must avoid tempering with scene
d. The Officer shall isolate by rope or cordon an area larger than the immediate area of the crime scene, including entries or escape routes.
e. The Officer shall deny public access to the scene by posting a guard
f. The Officer shall contact the police (CID Unit) as soon as possible for further action.

11.2 CONFESSION

a. For the purpose of this document, a confession is defined as any Statement made by a person admitting a matter which (a) constitute; or (b) forms an essential part of; or (c) taken together with other information already disclosed by him is a basis for an inference of the commission of a crime or a breach of the Technical University Security code.

b. These shall be considered valid only if:
   i. The statement was made voluntarily
   ii. The statement was made in the presence of an independent witness (other than a police officer or member of the Armed Forces) approved by the accused.

c. The Independent witness must be a person who:
   i. Can understand the language spoken by accused
   ii. Can read and understand the language in which the statement is made.
   iii. And where the statement is in writing the independent witness must certify in writing that the statement was made voluntarily in his presence and that the contents were fully understood by the person.

d. Where the person is blind or illiterate, the independent witness shall carefully read over and explain to him/her the contents of the statement before it is signed or marked by the accused, and shall certify in writing on the statement that he had so read over and explained its contents to the person and that the person appeared perfectly to understand it before it was signed or marked.

e. For the purpose of this Section, a statement that was not made voluntarily includes, but is not limited to, a statement made by the accused if:
   i. The person when making the statement was not capable, because of a physical or mental condition, of understanding what he/she said or did; or
   ii. The person was induced to make statement by being subjected to cruel or inhuman conditions, or by the infliction of physical suffering upon him/her by a public official, or by a person who has a direct interest in the outcome of the action, or by a person acting at the request or direction of a public official or such interested person; or
   iii. The person was induced to make the statement by a threat or promise which was likely to cause him to make such a statement falsely, and the person making the threat or promise was a public official, or a person who has a direct interest in the outcome of the action, or a person acting at the request or direction of public official or such an interest person.

f. A confession of a suspect does not present complete evidence when an officer takes a statement.

12.0 INTERVIEWS/INTERROGATIONS

12.1 GENERAL

The primary purpose or objective of all questioning is to obtain information from the person being interviewed in order to:

a. Establish the facts pertaining to a case or matter under investigation;
b. Determine the identity of the victim and the perpetrator;
c. Record the facts of a case for later testimony;

12.2 HOW TO CONDUCT INTERROGATIONS OR AN INTERVIEW

Before interrogating or interviewing, the officer must:

a. Identify him/herself as a security officer of the Technical University
b. Always be polite and courteous
c. Explain the purpose of the interview
d. Be straightforward and direct;
e. Begin with questions that the culprit/individual will not be afraid to answer such as their name, address and employment;
f. Remain neutral;
g. Use calm conversational voice;
h. Do not be judgmental;
i. Do not ask leading questions;
j. Do not be emotional;
k. Be aware that all victims are presumed to tell the truth
l. Be aware that the suspect is innocent until proven guilty;
m. Be clear and concise;
n. Do not use terms or words that the victims will not understand;
o. Take careful notes of all interviews/discussions.

12.3 TYPES OF INTERVIEWS

12.3.1 Interviewing a Complainant

The Interview of a complainant is normally the first information received about a crime or incident and therefore, the Officer must:

a. Try to obtain as much information as possible;
b. Be aware that the complainant may not be the victim;
c. Be aware that sympathy and understanding is the best approach;
d. Be aware that one should not rush through an interview.

12.3.2 Interviewing a Witness

In interviewing witnesses, the Officer must:

a. Try to find out the relationship between the witness and the crime
b. Be aware that a witness may be a victim, a passer-by, who saw nothing, someone who saw everything or even the suspect;
c. Avoid giving the witness information about the crime;
d. Be alert to any indication of deception.

12.3.3 Interviewing a Suspect or Defendant

When interviewing a suspect or a defendant, the officer must:

a. Deal with the person in a calm and objective manner;
b. Do not use false statement, promise or deceptions concerning particular benefits, exhaustion, threats or improper methods or approaches that influence freedom of choice;
c. Do not use will power of the person being questioned in order to obtain a confession or a statement;
d. Remember that the suspect has the right to avoid self-incrimination.

12.3.4 Interviewing a Child

In Ghana, a child is anyone under the age of 18 years of age. In interviewing a child, the Officer must understand that:

a. A child does not think, act or respond like an adult
b. A child is much more likely to be truthful and frank
c. Privacy is equally as important for the child as it is for the adult;
d. Avoid interviewing a child in public;
e. A child who is a suspect should never be interviewed alone;
f. If a child is incooperative or very frightened, the officer must make an attempt to interview him/her in the presence of a parent or a person in authority.

13.0 CODE OF DISCIPLINE IN THE SECURITY SECTION

13.1 GENERAL MISCONDUCT

It shall be a misconduct for a Security Officer to:

a. Be absent from duty without leave or reasonable excuse
b. Be late for duty or parade
c. Be insubordinate or use abusive words or insulting language, or quarrel with any other staff.
d. Use, without lawful authority, any property or facilities provided for the purpose not connected with his official duties

e. Desert his beat or leave point of beat or other place to which he has been assigned without permission or without sufficient and proper reason.
f. Malinger or feign sickness
g. Be drunk whilst on duty
h. Sleep whilst on duty
i. Disobey lawful order given by superior in rank whether verbally or in writing
j. Make any frivolous or vexatious complaints or join in making any anonymous complaints.
k. Cause disaffection amongst members of the Security Section or attempt to induce any member to commit breach of peace
l. Tip-off any person concerning orders received for his or her arrest
m. Lend money to, or borrow money from any other Security Guard
n. Incur debt without any reasonable prospect, more intention of paying it, or having incurred any debt making no effort to pay.
o. Loiter, idle or gossip while on duty
p. Smoke whiles in an official uniform
q. Display gross neglect of duty
r. Negligently allow a suspect to escape
s. Omit or fail to make any necessary entry in any official document or record.
t. Make or sign an false entry in any official document or record
u. Fail to work his beat or point of duty properly while on duty
v. Accept directly or indirectly any gratuity or present without the knowledge and permission of the Superior Officer whom he is serving
w. To pawn, sell, lose by neglect, damage or failure to report any loss of or damage to any article or clothing, or necessaries issued to him or any Technical University property committed to his charge.
x. Parade for duty dirty or untidy in person, clothing or accoutrements.
y. Exhibit oppressive or tyrannical conduct towards any person of a lower rank.
z. Display lack of civility to any members of the Technical University community or visitor.

13.2 DISCIPLINARY ACTIONS FOR THE MISCONDUCT OR UNSATISFACTORY OF SERVICE BY A SECURITY OFFICER

The following are the penalties that may be imposed in disciplinary proceedings in respect of misconduct or unsatisfactory service: Warning or reprimand, Withholding of increment, Suspension form duty without pay for a period not exceeding fourteen (14) days, Reduction in rank or grade, Interdiction, Dismissal without notice and Termination of appointment etc.

13.2.1 Warning or reprimand

a. A Head of Department shall query in writing, an employee whose work or conduct he has reason to be dissatisfied with. If the explanation is considered satisfactory, no further action shall be taken. If it is not considered satisfactory decision shall be recorded in writing against him.

b. If an employee is queried and a decision recorded against him in writing, a copy of each of the query and written decision shall be forwarded to the Registrar.
c. An employee should not be allowed to accumulate a record of warnings and censures for misconduct and faults before disciplinary action is taken against him.
d. In some cases, the faults may be of comparatively minor in significance in themselves, nevertheless, when it is clear that and sufficient material is available to warrant disciplinary proceedings, action should be taken against the person.
e. An employee who commits a minor offence may be queried and warned orally.

13.2.2 Withholding of increment

a. An employee's increment may be withheld on grounds of inefficiency or unsatisfactory service accounting to misconduct or failure to pass an examination prescribed by a scheme of service as a pre-requisite for the grant of increment.
b. Where a Head of Department is satisfied that an employee has not earned his annual increment and that it should be withheld, he shall inform the Registrar with a full statement or reasons for recommending the withholding of the employee's increment.
c. If it is proved that the employee has failed to fulfil the requirements for the granting of an increment has been withheld until such time as he will earn its restoration by an improvement in the standard of his work or conduct or will pass prescribed examination.

13.2.3 Restoration of withheld increment

a. When the Head of Department is satisfied that the employee's increment should be restored with effect from the due date, he will advise the Registrar, who in turn, will inform the employee that this increment has been restored.

13.2.4 Stoppage of Increment

a. If the increment is not restored before the 1st of January, it will be treated as stopped, in which case the next increment will not be awarded until it is earned.
b. An employee whose increment is stopped loses the amount of increment which he would have drawn for the period during which it was stopped.

13.2.5 Suspension from Duty

a. Whenever in the opinion of a Head of Department, misconduct which is of such a nature as to warrant dismissal has been committed by an employee, the Head of Department concerned shall recommend to the Registrar that, the employee should be suspended for a specified period. The employee, if so suspended,

shall be forbidden to carry out his duties or visit his place of work without the express permission of the Registrar.

b. When an employee has been suspended, he shall be called upon to hand over any uniform, account books and records, and any property of the Technical University in his charge to such other employee as the Head of Department shall order and he/she shall be deprived of his salary for that period.
c. Notice of suspension shall be conveyed in writing to the employee concerned by the Registrar

13.2.6 Reduction in Rank or Grade

a. If as a result of disciplinary proceeding against an employee, a major penalty other than dismissal is to be imposed, that employee may be reduced in rank. This means removal to a lower grade with an immediate reduction in salary.

13.2.7 Interdiction

a. Where an employee has been charged with criminal offence whether or not it is connected with the Technical University, the Registrar shall interdict him from his duties forthwith.
b. Where disciplinary proceedings which may result in an employee's dismissal are being taken or are about to be taken and the registrar considers that the interest of the Technical University requires that the employee should cease forth to exercise the duties and functions of his office, he shall interdict him from the exercise of those duties and functions.
c. Formal notice of interdiction shall be given to the employee concerned in writing. The notice shall state the date from which the interdiction take effect and reasons for such interdiction.
d. An employee who is under interdiction shall be required to handover any uniform, accounts books and records, and any other property of the Technical University in his charge to any such person as the Head of department shall order and he shall be forbidden to carry out his duties or visit his place of work except with the express permission of the Registrar.
e. An employee who is interdicted shall receive two thirds of his salary, normal deductions and the recovery of any loans shall also be made. He shall be paid any of the approved allowances to which he/she normally has been entitled to.
f. If disciplinary proceedings do not result in the employee's dismissal, the whole of the salary and appropriate allowances withheld from him/her shall be restored to him/her when the final decision is taken.
g. An employee under interdiction who is found guilty of any of the charges preferred against him may be dismissed, in which case, he/she shall not subsequently receive any part of the any short payment of his salary, notwithstanding at that he may have been found not guilty of some of the charges.

13.2.8 Dismissal

a. Failure to disclose any previous conviction for a criminal offence will lead to summary dismissal.
b. An employee who has falsified or who falsified testimonials or personal records will also be summarily dismissed.
c. An employee of the Technical University shall be summarily dismissed if he corruptly accepts to obtain from any person, for himself or for any other person, any gift of consideration as an inducement or reward for doing or for bearing to do any act in relation to the Technical University's affairs or business or for showing or for bearing to show favour or disfavour in relation to the Technical University's affairs or business.
d. An employee of the Technical University shall be summarily dismissed if he while employed in a full time or part time capacity, acts as an agent against the Technical University in any matter.
e. An employee who is confirmed in his appointment may be dismissed by the Technical University for misconduct but no such employee shall be dismissed until he has been given the opportunity of appearing before the disciplinary committee. In all proceedings of the disciplinary committee, the employee affected shall be entitled to a written notice of the basis on which the proceedings are initiated. He shall be entitled to call witnesses on his behalf and to hear the testimony of any witnesses against him.
f. A person adversely affected by a decision of the Vice-Vice Chancellor shall be entitled to appeal to the Technical University council.
g. An employee convicted of a criminal charge shall not receive any emoluments for the period following the date of his conviction. In the event of acquittal on appeal, all emoluments withheld shall be restored to the employee concerned.
h. Upon conviction of a criminal charge, an employee shall be dismissed or have his appointment terminated with effect from the date on which he was interdicted or convicted.
i. No notice or salary in lieu of notice shall be given to any employee dismissed for misconduct but dismissal shall take effect from the date on which he was interdicted or convicted.
j. An employee dismissed for misconduct shall vacate the Technical University premises immediately his entitlements are paid. He will not be entitled to any transport allowance.

13.2.9 Termination of Appointment

a. An employee who is confirmed in his appointment may have his appointment terminated by the Technical University on grounds of general inefficiency provided that he had previously been warned in writing by his Head of Department that his work had been unsatisfactory and a copy each of such warnings shall be forwarded to the Registrar on each occasion.
b. An employee who is confirmed in his appointment may have his appointment terminated on grounds of misconduct.

c. The appointment of a confirmed employee shall not be terminated until he has been given an opportunity of submitting representations through his Head of Department to the Registrar for consideration.
d. A confirmed employee whose appointment for inefficiency or months' pay in lieu of notice at any time, as well as any leave due him. He shall be allowed to continue to stay in the Technical University premises for a period not exceeding one month and be paid the appropriate transport allowance to his/her home town.
e. The Technical University may at any time and for any good reason terminate the appointment of any employee who is on probation. If the termination is not due to an employee's misconduct, he shall receive three calendar months' notice or three months' pay in lieu to notice. In addition, he will be granted his earned leave, and be paid the appropriate transport allowance to his home town.
f. An employee who terminates his appointment by resignation shall be required to give three months' notice or pay three months' salary in lieu of notice. He shall also be required to vacate Technical University premises immediately or at the expiry of his notice.

14.0 TECHNICAL UNIVERSITY CAMPUS DELINEATION AND ZONING

For the operations of this manual, the Technical University campus has been delineated and zoned as follows:

14.1 THE TECHNICAL UNIVERSITY CAMPUS

a. The Cape Coast Technical University Campus includes and land controlled and administered by the Technical University situated in or in the vicinity of the Technical University as described in Executive Instrument (EI), and particularly described in the attached appendix.

14.2 ACADEMIC AREA

a. The academic area of the Technical University shall generally be areas where only Teaching and Learning take place. They include the premises of all

faculties, Schools, Colleges, Academic Departments, Libraries and Study Rooms within halls of residence.

b. Technical University Libraries shall be accessed only upon production of valid Technical University identity Card or authorized permission from the Registrar,

c. For security and safety purposes the following restrictions shall apply in all academic areas: Only Students, Academic, Administrative and Support Staff, Members and Persons invited for academic purposes in the Technical University are allowed to access these areas as marked in the Schedule attached hereto.

d. The following shall not be allowed in academic areas
   i. Tooting
   ii. Hawking
   iii. Peddling
   iv. Demonstrations and / or Processions
   v. Excessive noise

e. In the academic area broken down vehicles must be towed within one hour at the cost of the owner.

14.3 TECHNICAL UNIVERSITY CENTRAL ADMINISTRATION AREA

a. Technical University Central Administration area shall be the area where the core Technical University Administration services are performed and includes the offices constituting the Central Administration of the Technical University irrespective of where it is located.

b. The following activities are not permitted in the Technical University Central Administration area.
   i. Hawking
   ii. Peddling
   iii. Horning
   iv. Tooting
   v. Parking in non-designated areas
   vi. Demonstrations and / or Processions
   vii. Excessive Noise

14.4 SECURITY ZONE

a. The Security Zone of the Technical University Campus shall be areas where prescribed security measures shall be enforced by Campus Security staff at all times or certain times as specified in this code.

b. For purposes of this provision, the entire Technical University Campus is hereby declared a Security Zone from 10:00 pm in the evening to 6:00 am in the morning.

c. The following security measures shall apply to all persons using and/or commuting on Technical University Roads.
d. All Halls of Residence of the Technical University are Security Zones from 10:30 pm in the evening to 5:30 a.m and as such the following security measures may apply:
e. Random searches at entrance and exit
f. Interview on reason for entering or leaving
g. There shall be other security zones which may be determined by the Technical University from time to time.

14.5 RESTRICTED AREAS

a. Restricted areas on the Technical University campus are those in which only authorised persons are allowed to access.
b. For the avoidance of doubt the following areas on the Campus shall be restricted to unauthorised persons:
    i. The Vice Chancellor's Lodge
    ii. The residence of the Pro-Vice-Chancellor
    iii. The residence of the Registrar
    iv. Science laboratories
    v. Science equipment stores
    vi. Computer laboratories
    vii. ICT Installations
    viii. Electrical installation
    ix. Water and Sewerage Facilities
    x. Anatomy Building and Laboratories of the Technical University.
    xi. Any restricted designated area within the Technical University Hospital or Restaurant/Workshops or as the Technical University may determine from time to time.

14.6 ASSEMBLY POINTS

a. Assembly Point shall be areas delineated for open assembly. Such areas shall be as marked as such.

b. The following activities are not allowed at Assembly Points:
    i. Hawking
    ii. Peddling
    iii. Parking
    iv. Waiting
    v. Any activity considered by the Technical University to be banned.

NB: It shall be an offence for a staff/student to patronize the wares of any hawker at the unauthorized places, including Technical University offices as stipulated in Part H (above).

14.7 CLAMPING AND TOWING

The Technical University reserves the right to clamp or tow any vehicle found to have been parked or stowed at an unauthorized location. Any cost associated with towing such vehicle shall be borne by the owner of the vehicle.

In conclusion, this policy seeks to enhance the operation of the security section and to improve security on campus.

15.0 SAFETY POLICY ON INFORMATION COMMUNICATION TECHNOLOGY

15.1 COMPUTER/ELECTRONIC SECURITY

Information and Communication Technology (ICT) system play important roles in supporting the Vision, Mission and critical activities of the Cape Coast Technical University. To have optimal use of the ICT facilities and services available, there is the need to adhere to basic security codes, which set out the practices and responsibilities for ensuring security of ICT systems. Confidentiality, integrity and availability form the bedrock of and ICT systems' security of any organisation or institution. The code deals with security, privacy regulations and compliance.

The Cape Coast Technical University ICT security and safety code is organised along five key areas:

15.2 TECHNICAL SAFEGUARDS

a. The Director of the ICT Directorate shall create user accounts for faculty, staff and students, which will authenticate and grant them access to the system or application.

b. The Director of the ICT Directorate shall deploy appropriate encryption techniques that will guarantee the confidentiality and integrity of the data and information of users.

   i. Firewalls, operated through the Technical University's Network Operating Centre (NOC), shall ensure the confidentiality, integrity and availability of the Technical University's ICT systems.

   ii. The Director of the ICT Directorate shall acquire and install appropriate anti-malware software. The software so acquired shall be updated regularly.

   iii. Whenever a user suspects that a computer system has been affected by malicious software, such as virus or spyware, he/she shall notify the Computer Centre.

   iv. The Director of the ICT Directorate shall educate users on the need to run up-to-date virus protection programmes in order to safeguard their computers.

   v. The Director of the ICT Directorate shall design and operate the appropriate software which will incorporate techniques and controls that will protect and secure the system as wells make it difficult to be abused by users and hackers.

15.3 DATA RIGHTS AND SAFEGUARDS

a. Data rights refer to respect for the rights of the person who collected the data and about whom the data was collected.

b. Users of already collected data (referred to secondary data) shall always seek assistance from the ICT Directorate or the person who collected the data.

c. Sensitive data or information shall be adequately protected by the data user or the data custodian. Sensitive data or information is one of the following:

   i. Administrative, research or planning data

   ii. Personal data

   iii. Data protected by confidentiality agreement.

d. Data collected shall be sued for the purpose for which they were collected. If they are to be used beyond the purpose from which they were collected, approval shall be sought using laid down procedures. Where data are about individuals, the data shall be anonymised before being given out.

e. The Technical University's ICT resources shall be used in a responsible, ethical and legal manner.

f. The ICT facilities of the Technical University shall not be used to display, store, receive or transmit images or text which could be considered offensive

such as pornographic, paedophilic, libellous, threatening, and defamatory materials.

g. Users shall be discreet with their usernames and passwords.
h. Whenever a user suspects that his/her account has been compromised, the user shall be required to change his or her password.
i. Users shall be required to report password compromises to the ICT Directorate.
j. In the event of a major security breach, users shall be required to change their passwords.
k. Owners of laptops and other portable devices shall ensure that they are secured at all times.
l. ICT Staff working in some sensitive offices such as the Network Operating Centre (NOC) shall not admitting unauthorized persons to their offices.
m. The Directors of ICT Directorate and the Directorate of Physical Development and Estate Management and the Head of Security shall ensure that there are adequate physical security measures in place to secure ICT facilities against fire, flood, theft, defacing, unauthorized entry, etc.
n. The account of any employee leaving the Technical University shall be deactivated.
o. The Head of Computer Centre shall deploy the appropriate encryption techniques to protect data from being tampered with during transmission.

15.4 INTELLECTUAL PROPERTY RIGHTS (PLAGIARISM, COPYRIGHT, PIRACY)

a. It is a criminal offence to make a copy of software with the intention of obtaining a commercial advantage or profit.
b. Users shall use someone else's work when they have:
    i. Obtained permission from the person who holds copyright to that material
    ii. Ensure that the materials is in the Public Domain;
    iii. Ensure that the material is not protected by copyright.

15.5 SYSTEMS CONTINUITY

a. The Director of the ICT Directorate shall ensure that any unit in the Technical University disposing of a computer system deletes all sensitive data, operating system and Copyrighted Applications on the system.
b. Hardware meant for disposal shall be stored in a safe place, destroyed, or recycled.

15.6 COMPUTER RELATED OFFENCES

To protect the Technical University's ICT systems from cybercrime, the following shall be observed:

a. It shall be an offence to use the Technical University's computers or network as a tool to commit crime e.g. hacking, fraud, identity theft, or cyber stalking.
b. It shall be an offence to undertake any act that is intended to destroy, deface, vandalise, temper with data, hack into restricted areas, infest the system with obnoxious materials – worms, virus – of any of the Technical University's IT facilities.
c. It shall be an offence to use ICT services or network for incidental purposes related to crime.
d. It shall be an offence to cause a computer to perform any function with the intent to secure access to any programme, information, or data held in the computer that has not been authorized for use.
e. It shall be an offence to undertake any act which causes unauthorized modification of the contents of a computer or database.
f. It shall be an offence to use the Technical University's computers to facilitate the commission of a crime.
g. A disciplinary committee shall prescribe the appropriate penalty for persons found guilty of committing any of the offences identified under