SUNYANI TECHNICAL UNIVERSITY

SECURITY POLICY

DECEMBER, 2022

Table of Content

Introduction

Sunyani Technical University is one of the most successful Technical Universities among the ten established in the country. The University's main campus is located on a site spanning the southern boundary of the Sunyani-Kumasi high-way between the STC yard and Sunyani High School, extending south to close to the main refuse dump, with Sunyani Senior High School to the east and the main GETFund Hostel Road to the west. Facilities scatter over 1.5km land mark interspersed with a mixture of facilities of the local community in some portions. Founded in 1967 as the Sunyani Technical Institute, it was upgraded to a Polytechnic in 1997 and subsequently to a Technical University in September 2016 following the promulgation of the Technical Universities Act, 2016 (Act 922) and has since been a unique and successful Technical University combining a "can-do" entrepreneurial spirit with a commitment to absolute academic excellence in line with the University's 2020-2025 Strategic Plan.

Open egress to the University is an essential ingredient of everyday academic life. In view of this, it is very important that STU is seen to be a good neighbour adding value to the community. In that respect the campus offers excellent sporting facilities such as; acres of football, basketball and volleyball pitches. It also has a clinic, computer center, a restaurant, lunch counters, a library complex, an ultra-modern auditorium and a mechanical workshop, which are all open to the general public. In terms of transport, the University is accessed by of all forms of transport except the tricycle popularly known as tricycle. On a working day there may be in excess of 100 bicycles, 100 motorbikes and 200 vehicles accessing the Campus.

The University is easily accessible from several directions since it is not fenced. These open accesses carry inherent security risks, and if the general invitation to the public onto the campus is not to be abused regularly, some security measures are not only inevitable but highly desirable to maintain the University's reputation as a safe and secure place. This Security Policy therefore seeks to formalize an overall integrated approach to security on STU campus.

Policy Statement

Sunyani Technical University is committed to providing and maintaining, as far as reasonably practicable, a safe, secure and crime-free environment for all students, staff, visitors and contractors, whilst within or situated on University premises. Our Security Policy ensures that we have in place effective procedures to enable us to achieve this aim.

Principles of the Security Policy

This policy provides the following set of guiding principles:

Principle	Demonstrated by:
The University aims to eliminate or minimise security risks to its community and its property by adopting a planned and systematic approach to security management across all its premises and activities.	i. Ensuring strong leadership where responsibilities for the security of all members of the University community and for University property are clearly defined and implemented across all levels of management ii. Applying the principles of the Risk Management Framework in the identification of security risks and the implementation of appropriate preventive/protective measures iii. Managing the proper use of the University's security systems, such as electronic access cards, CCTV, alarms, etc. iv. Actively managing behaviours of concern that arise on University premises or in University activities v. Developing and implementing security measures to control chemicals, alcohol, drugs and weapons on University premises or in University activities without impinging on the rights of academic freedom or freedom of speech as expressed in the University's Academic Freedom and Freedom of Speech Policies vi. Devising and implementing measures for the effective management of security-related incidents and emergencies at STU
The University communicates and	Consulting with relevant stakeholders when reviewing security risks and security management measures

consults with members of its community to encourage constructive participation in security management.	
The University utilizes appropriate internal and/or external security services or personnel.	i. Securing professional security services providers and/or personnel who are suitably licensed, qualified, trained and experienced to perform security duties ii. Managing contracts for the provision of security services in accordance with all legal, procedural and ethical requirements iii. Allocating sufficient security support and resources to achieve acceptable standards of operation iv. Ensuring that appropriate security patrols, escorts and crowd control are provided for University premises and activities
The University monitors, measures, evaluates and regularly reports on security management activities, security-related incidents and emergencies.	i. Monitoring the effectiveness and efficiency of security management measures ii. Encouraging all members of the University community to immediately report security incidents appropriately recording and investigating incidents to prevent recurrences as far as practicable iii. Compiling, distributing and reviewing monthly, quarterly and annual security management reports

Purpose

This policy sets out the commitments of Sunyani Technical University in relation to security, and provides a framework for security management. The objectives of this policy shall be;

1. To ensure strategic leadership to promote a collaborative and coordinated response to risk management consistent with the vision, mission and the strategic plan of the University.
2. To provide rules, regulations and guidelines to govern and regulate security within campus and as well as satellite facilities.
3. To implement a system for the analysis of the potential risks, including the completion of a Risk Analysis Questionnaire (RAQ) which will examine safety and security issues in the University.
4. To have in operation a report system for consideration by Governing Council which will consider what resources are, or will be made, available to deal with the recommendations set out in reports.
5. To minimize the University's exposure to all levels of risks where the safety and security of staff and property are potentially compromised.
6. To ensure the professional development of all security staff of the University

Scope of the Policy

STU is committed to ensuring a conducive and friendly academic environment for the University community to engage in all legitimate activities without fears of harm, threat to self and properties, intimidation, or harassment. Accordingly, the policy shall apply to all members of the University community including:

1. All University premises;
2. All activities taking place on University premises, whether they are University activities or not; and
3. All members of the University community whilst planning, managing or engaging in any University activity, whether this activity takes place on University premises or not.

Policy Exceptions

i. The policy excludes private halls/hostels of residence and tenants unless specifically agreed.
ii. The policy does not also govern the behavior of non-University Staff who occupy leased space owned by the University.
iii. The policy does not as well cover property secured at locations that the University does not own or control.
iv. The policy does not cover the security of University information, financial assets or reputation, or the management of emergencies and critical incidents as these matters are comprehensively covered by other relevant University policies and procedures.

Legislative Context

i. Ghana Constitution 1992
ii. Criminal Offences Act, 1960 (Act 29)
iii. Technical University act, 2016 (Act 922)
iv. Public Order Act. 1994 (Act 491)
v. Anti-Terrorism (Amendment) Act. 2014 (Act 875)
vi. Security and Intelligence Agencies Act.1996 (Act 526)

Definitions

The following definitions apply to the terms used in the policy.

TERM	Definitions
Academic freedom	i. The freedom of academic staff to teach, discuss, research and to disseminate and publish the results of their research; ii. The freedom of academic staff and students to engage in intellectual inquiry, to express their opinions and beliefs, and to contribute to public debate, in relation to their subjects of study and research; iii. The freedom of academic staff and students to express their opinions in relation to the higher education provider in which they work or are enrolled; iv. The freedom of academic staff to participate in professional or representative academic bodies. v. The freedom of students to participate in student societies and associations; vi. The autonomy of the higher education provider in relation to the choice of academic courses and offerings, the ways in which they are taught and the choices of research activities and the ways in which they are conducted.
Behaviour of concern	i. Behaviour that creates a reasonable apprehension of harm, including self-harm. ii. Behaviours of concern include making threats, bringing a weapon on campus, persistently glaring at a person, adopting a menacing posture, etc.
Drug	As defined by the Drugs, Narcotics Control Commission Act, 2020 (ACT 1019), as applicable. For the purposes of this policy and its associated procedure, includes non-prescribed possession of prescription-only medicines.

Emergency	Any sudden danger that requires immediate action to prevent severe injury, illness, damage or distress, e.g., life-threatening violence on University premises or in University-related activities, deliberate and serious damage to University property such as arson, large-scale civil disturbance, etc.
Freedom of speech	The freedom of staff, students, and invited visitors to the University to express lawful opinions publicly, without undue restriction.
Event	An activity held on a campus of Sunyani Technical University that meets all the following criteria: i. It is not a timetabled teaching activity (such as a lecture, practical class, or tutorial) or a routine business meeting of a School/Directorate/tenant. ii. It does not form part of the usual academic life of the University, such as exams, graduations, seminars, or Open Days. iii. It does not form part of the usual business activities of the University, such as maintenance works, or refurbishment/ construction projects. iv. It involves numbers of participants greater than 50 (staff and/or students) or 10 (external parties). v. It introduces foreseeable hazards or risks on campus (e.g. serving of alcohol, use of hazardous substances or equipment, hazardous physical/sporting activities, security threats, presence of children, presence of VIPs, etc.).
Incident	Any actual or suspected event or behaviour that causes, or has the potential to cause, harm, damage or loss to any member of the University community or property, e.g. behaviour of concern, disruption to public order, vandalism, theft, etc.

Security (in relation to this policy and associated procedure)	The protection of the University community and/or property from intentional or reckless injury, harm, distress, threat, damage, theft, misuse or loss.
Security management	The range of procedural, technical, physical, personnel and other measures designed to achieve the purpose of this policy.
University activity	Any program, course, research, service, operation, project, function or event conducted by or for Sunyani Technical University, whether on University premises or not.
University community	All persons who have an association with Sunyani Technical University, including staff, members of Council and committees, students, tenants, visitors, contractors, consultants, volunteers and people representing the University off-campus.
University premises	Any property owned or occupied by the University, either wholly or in part, and includes all buildings, student and staff residences and all land defined and/or associated with the University. It includes any public area located within University premises and can include a public area adjacent to University premises if relevant to this policy and its associated procedure.
Weapon	Any item covered by the provisions of the Arms and Ammunition (Amendment) Act, 2001 (Act 604) as applicable.

Campus Security Committee

The purpose of the Security Committee is to review security policies and procedures and make recommendations for improvement. This advisory committee is responsible for ensuring that the procedures for educational programs on safety, sexual assault, and crime prevention are in place and that reporting, referral, counselling, and response mechanisms for security and safety are also updated and monitored regularly. The Committee shall report, in writing, to the Vice-Chancellor on its findings and recommendations on security situation on University Campus at least twice yearly and such report shall be available upon request.

Composition of Membership:

i. Pro-vice chancellor – Chairman
ii. Representative of the Registrar not below the rank of Senior Assistant Registrar
iii. Representative of Director of Finance
iv. Director of Works and Physical Development
v. Dean of Students
vi. Chairman of Inter Halls Committee
vii. Deans of Faculties
viii. Medical Director
ix. Information Communication Technology (ICT) Officer
x. Chief security officer
xi. Public Relation Officer (PRO) – Member/Secretary

Functions of Security Campus Security Committee

The Committee Shall:

i. Advise on security around the University's academic and residential areas; specifically, to consider and advise on:
    a. The University's security strategy and the resources required to support it.
    b. The assessment and management of security risks.
    c. Links between security and other University functions.
    d. Staff and student training in the area of security.
ii. Identify loopholes in the present security arrangement with regard to security personnel's competence, training and placement.

iii. Draw up new methods of 'policing' or monitoring security, especially at night on the campus.
iv. Enforce University security and safety policies on campus and among security personnel.
v. Maintain active contact with all aspects of the University community, including students, faculty, staff, spouses/dependents and visitors.
vi. Ensure that the community's safety and security concerns are properly addressed in a professional and courteous manner.
vii. Collate, review and present reports and other necessary correspondence to Management through the Office of the Vice-chancellor.

Meeting

i. The committee shall at least meet once a semester
ii. The quorum for a meeting shall be at least fifty one percent (51%) of the membership including the chairman.

Responsibilities

Responsibility for security rests with all students, staff (including contractors and agency staff) and with visitors to the University. In particular, everyone should report all activity (suspected or real) of a criminal nature, unacceptable behaviour, or any suspicious activity immediately to the Chief Security officer or Registrar. Security on STU campus shall be a shared responsibility for all; however, certain strategic security activities and responsibilities shall be vested in the following staff categories;

The University Council

The University Council is the highest governing body and shall have the ultimate responsibility to design policies to govern the University's safety by ensuring that management implements policies that guarantee total safety of students, staff, visitors and University properties both within and outside campus. The Council therefore has a key role to play, not only by approving this policy, but also, to empower, resource, and ensure that all relevant bodies and individuals responsible for its implementation do so appropriately and efficiently.

The Vice Chancellor

The Vice-Chancellor is the Chief Executive officer, academic head and chief disciplinary officer of the University and has overall responsibility for the smooth running of the University, not only in terms of administration and academic issues; but also, the health and safety of students, staff, and visitors. By his/her position, the Vice Chancellor is responsible for the implementation of this policy, a responsibility he/she may exercise directly or indirectly through the Registrar or any assignee of the University.

The Registrar

The Registrar has overall responsibility for the provision of administrative services to the University as the Chief Administrative Officer, and shall be responsible for the day-to-day administration of the affairs of the University. The University's Statutes puts the security services unit under the office of the registrar. The Registrar is, thus, directly responsible for supervising the operational aspects of this security policy, and shall ensure, through the Chief Security Officer (CSO), that the security system works efficiently and effectively for maximum security of the University.

Deans/Heads of Department/Units/Sections

The pivotal role in promoting enhanced security lies with Deans, Heads of Departments, Units and Sections. Security is not intended to be a hindrance to academic activity but to assist with the smooth operation of a department, particularly when financial constraints mean that stolen equipment might not be replaced immediately or even at all. The actual responsibilities will vary according to the location of the department and the nature of the activity, but a number of specific responsibilities can be identified for Heads of Department Units and Sections:

i. Ensure that all members of staff and students in the department understand and exercise their security responsibilities; including the displaying of identification cards (ID) where appropriate whilst on campus and have due regard to University property, in particular the security of equipment.
ii. Undertaking a security risk analysis of the department, in liaison with the Head of Security, and acting to remove or reduce, as far as possible, any security risks.

iii. Maintaining an inventory of all equipment, especially those which require particular protection. A record should be kept of the product name, the manufacturer's name, the model number and serial number.
iv. Authorizing access to the department by confirming in writing to the Security which staff may have access to areas which are locked out of office hours.
v. Notify the Campus Security Supervisor of any potential security risk (including the purchase of expensive equipment), who will advise on any additional security or protection and investigate any crime or incident.
vi. Ensure that all Staff, including all those with a contract of work, are familiar with and follow the procedures set in the University Security Policy; paying particular attention to those issues which are relevant to their activities.
vii. It is recognized that Heads of Department, units and sections will wish to delegate responsibility for the routine operational matters involved in these tasks to a nominated individual in their Departments, but the overall responsibility for security matters will still remain with them.

Chief Security Officer (CSO)

The Chief Security Officer is responsible for operational and administrative security issues including, but not limited to the following;

i. Plan and ensure execution of security arrangements as required by the University
ii. To look after all the security arrangements in the campus
iii. To supervise and control the work of security personnel
iv. To assist the University authorities in maintaining law and order
v. To maintain liaison with the police and district authorities regarding law-and-order problems on campus and investigation of criminal cases/security breaches affecting the University
vi. To assist the University hostel administration in day-to-day functioning, e.g., eviction of unauthorized occupants/intruders
vii. To attend to fire incidents and other calamities and incidents on the campus11. Act on occurrences as reported in the occurrence book that requires action.

Security Supervisors

The responsibilities of the Security Supervisors include the following;

i. To report to the Chief Security Officer on issues concerning guards while at post.
ii. To go round regularly to check and ensure that the guards are at post.
iii. To document all incidents in the occurrence book.
iv. To report to the Chief Security Officer every morning to take fresh mandates.
v. To ensure that all officers are properly assigned to posts.
vi. To write periodic reports on the major activities of the Section to the Chief Security Officer.

Security Guards

The practical duties of providing security on the campus of the University rest with the Security guards supervised by the security supervisors. They are responsible for the coordination and monitoring of security procedures and protection systems.

They perform guard duties at various parts of the University as determined by the CSO, undertake foot and mobile patrols of the campus, observe and detect security risks and breaches, take necessary steps to ensure the safety of University staff, students, visitors, and to protect University property from theft or damage.

The detailed Standard Operation Procedures (SOPs), Code of ethics and professional Conduct have been designed to ensure that Security Staff perform their duties professionally, efficiently, and effectively. The SOPs will be revised and updated periodically by the CSO to deal with new and emerging security threats to the University.

Staff of the University

Security of the University is a collective responsibility of the entire community. Therefore, all Staff (including those with a contract of work, including research staff, visiting fellows, anyone employed as lecturer, researcher even on an ad hoc basis) must ensure they are familiar with and follow the procedures in the University Security Policy. They must also co-operate with security-related requests from the chief security officer or other staff, especially with emergency or evacuation instructions and in relation to all security procedures (e.g., showing ID cards on request). The responsibilities of the staff in ensuring this include:

i. Ensuring that they take all the necessary steps and care to prevent the loss and damage of any University property that they use
ii. Ensuring that the area they work in is properly secure at the end of the working day with all windows closed and doors securely closed and locked.
iii. Making sure to do the settings provided for devices such as alarm or protective systems where they are fitted;
iv. Where offices or work places are temporarily left unoccupied, employees must ensure windows are secured and doors properly locked.
v. Staff should note that the responsibility for personal property always remains with the owner of the property. The University takes no responsibility for such property left on the premises, and this includes motor vehicles and cycles, although Security staff will do their best to provide a security presence across the campuses at all times.
vi. Ensuring that if they use University property that its security has been properly considered and that effective measures are taken to prevent loss in appropriate cases.
vii. Ensuring that the area they work in is properly secure at the end of the working day with all windows and doors securely closed and locked.

Students

All students who make use of University property and facilities have a general responsibility to look after these facilities properly and to give due consideration to security issues. They must follow security procedures designed to protect University property, in particular, regulations governing access to science and computer labs or areas with other sensitive equipment. The responsibility for personal property always lies with the owner of the property.

The University takes no responsibility for such property left on the premises and this includes motor vehicles and cycles, although the Security staff will do their best to provide security presence across the campus at all times. Students who are resident on campus are advised to ensure that they secure all windows and doors when leaving their residences. Advice on information on security issues for students shall be provided by the Security department as and when necessary.

Visitors to the Campus

All visitors, including conference delegates and event attendees, who make use of University property and facilities have a general responsibility to look after these facilities properly and to give due consideration to security issues. In particular they must follow security procedures designed to protect University property. Responsibility for personal property lies with the owner of the property. The University takes no responsibility for such property left on the premises and this includes motor vehicles and cycles, although the Security staff will do their best to provide security presence across the campus at all times.

Contractors and Non-Staff Workers

All contractors, sub-contractors or individuals who make use of or work on STU premises shall comply with all security procedures designated to them by the department. They shall be required to wear their designated ID cards or tags at all material times on campus.

Like other members of the University community however, responsibility for personal property lies with them. The University takes no responsibility for such property left on its premises and this includes motor vehicles and cycles, although the Security staff will do their best to provide security presence across the campus at all times.

Common or Shared Areas

Where areas of buildings are common or shared with other Departments, the security risks in those areas are shared by all the Departments that use that area. Heads of Departments in these areas are asked to draw the particular risks or issues to the attention of the Head of Security so that effective solutions can be proposed in conjunction with all interested parties.

Section 1- Campus Security: Crime Prevention/ Awareness

Procedure: Crime Prevention

i. All suspicious activity should be immediately reported to the chief security officer or the Security Reception staff in the first instance (who will contact appropriate dean or head of department officers).
ii. Personal valuables should be locked away, placed out of sight or kept on the person. Personal property should never be left unattended
iii. Offices must be locked upon leaving, with windows closed and locked
iv. Laptops should not be left unattended and must be locked out of sight when not in use, particularly overnight. In open areas, laptops should be either secured to the desk with a steel enclosure or security cable or locked away when not in use in a secure cabinet
v. Ground-floor windows (and curtains or blinds) should be closed at dusk and lights should be turned off when leaving.
vi. All incidents of crime on University premises, real and suspected, must be reported to the security reception staff and an Incident Form completed.
vii. The evening security reception staff will do their rounds in the evening to ensure that appropriate doors are locked. They will also patrol common areas of main University to aide in the identification of security risks, monitor public safety and to act as a deterrent against crime.
viii. Remind staff and students each term to close doors and windows.

Procedure: Security Awareness

Campus safety programs can only be successful with the full co-operation, involvement and support of entire University community. In view of this, the Security Unit in collaboration with the Counseling unit, Students' Halls Representatives, and the SRC, shall create security awareness on campus using the following measures:

i. The use of Parrot Fm to educate and make announcements
ii. During staff orientation
iii. During orientation of students
iv. Periodic publications of University security update
v. Orientation for all persons using the premises and the facilities of the University at any material time

Incident Reporting

It is the responsibility of all staff and students of the University to report all activity, suspected or real, of a criminal nature, suspicious and/or unacceptable behaviour. Incident reporting is crucial to the identification of patterns of criminal activity. It permits investigation and recommendations to be made to prevent a reoccurrence. Comprehensive reporting of incidents provides an accurate picture of the level of crime throughout the University and thus ensures that adequate resources are provided to combat that crime. Success in the University's fight against crime is greatly enhanced by fast, efficient and detailed reporting.

Procedure: Reporting of Security Incidents

i. All security incidents and requests for emergency services including suspicions of breach of University security shall be reported to the security officer at the main security post either in person or on 0352023681, (emergency short code) or the nearest security post.
ii. All reported incidents shall be logged in the station diary and an incident report form generated (See Appendix "A" attached). The chief security officer is then informed for appropriate action to be taken. All suspected criminal cases shall however be reported to the police after consultation(s) with the Vice Chancellor or whosoever is at the helm of affairs at time of the incident.
iii. The security department shall be duly notified of any operations of Ghana police or any other security personnel on campus.
iv. All suspected thefts and/or losses of property on STU campus shall be promptly reported to the security department.
v. An Incident Report form is available from Security Reception. The form should be completed as soon as possible after an incident by the person reporting the incident
vi. The local Police should be informed in all cases of reported crimes of assault, indecency, fraud, theft (including car or cycle theft) and burglary. In cases of doubt, advice on Police involvement may be sought from the Duty Officer. All Police involvement on University property is to be notified to the chief security officer during weekdays day or the Duty Officer at night or weekends to enable effective University management of any subsequent actions on University premises.

vii. All serious crime or major incidents must be managed in accordance with the University's Emergency Plan. In the first instance, any serious crime or incident must be immediately reported by dialing 192.

Crime Investigation

All crimes that occur on University premises will be investigated appropriately to prevent re-occurrence and aid crime prevention. The security committee and other personnel as appropriate will be responsible for carrying out internal investigations of security related incidents, producing written reports for circulation where necessary and providing follow up crime prevention advice.

Staff or students alleged to be involved in any crime within the University or crime affecting the University community may be referred to the Vice Chancellor, who has the power to suspend and/or ban staff or students from entering the University premises pending investigation and/or disciplinary action.

Section 2 – Access Control

Accessibility of STU Facilities /Campus

i. All staff and students are issued with a Sunyani Technical University card which is used as an identity card, a student registration card, and a library membership card. Students are required to carry their cards with them at all times and to show their cards to officers or employees on request. Staff are required under the terms of their employment contracts to carry their card at all times whilst on university premises. The loss of one of these cards should be reported, as soon as possible to the Security team or Departmental office.

ii. All staff and students are required to show their University cards to security staff, upon request. Failure to do so may result in an immediate request to leave University premises if a person's identity cannot be confirmed.

iii. Visitors and ad-hoc Contractors will be issued with a 'visitor's pass at the point of entry and should wear these passes which contain emergency and health & safety information, throughout their visit to the University. The member of staff responsible for the visitor/contractor should ensure that they collect the visitor's pass when signing out upon leaving the campus.

iv. Contractors who will be on-site for more than a week will generally be issued with a University 'Contractor' card to allow them access to the building they are working in.

Arrangements for these cards are to be agreed upon by the Contract Project Manager. Contractor identity cards must be displayed at all times whilst on university premises.

v. The contractor's access to university buildings will be strictly controlled by the security team according to agreed access control procedures.

vi. All applications for new barrels or keys should be made via a request to the Security Help Desk, as appropriate. Additional locks & keys and replacement keys are chargeable to the Faculty/Department.

vii. All issues of keys will be subject to satisfactory fulfilment of criteria to ensure need, use and availability.

Control of Locks, Keys and Access Control Cards

i. The security unit controls the issue and use of all locks and keys. For all premises and refurbishments, the University operates a suited key system which allows various levels of access. No other make of lock or key should be installed on university premises without the authority of the security unit as appropriate.

ii. Departmental administrators should keep a record of all keys issued and ensure that staff return keys when they move offices or leave the University's employment. It is the responsibility of all individuals who are issued keys or cards to ensure their safekeeping at all times and report any loss immediately to security staff.

Procedure: Request for Locks & Keys

i. All keys belong to the Sunyani Technical University and are not exclusive. Security carries out duties over 24hrs, 365 days per year and requires access to all areas, especially in emergencies. In exceptional circumstances, certain restrictions may apply to sensitive areas but the agreement should be achieved between interested parties regarding access in any emergency.

General Procedure

i. All losses of keys must be reported immediately to the Security Team.

ii. Persons leaving the University or transferring to another Department are to return their keys direct to their Departmental office. They should not pass keys directly to their replacement.

iii. Where building refurbishment is carried out, the cost of new locks and keys should be included in overall project costs, otherwise, the costs of replacement or additional locks and keys will be recharged to departments.

iv. Replacement keys will only be issued after an investigation of the loss. The cost of replacement will be charged to the Faculty, Department or individual concerned.

v. Any loss of master or sub-master keys will be the subject of an inquiry, with all resultant costs for replacement of locks and keys borne by the Faculty or Department concerned. If loss of master or sub master keys is suspected to have arisen through negligent action by a member of staff, then an investigation under the appropriate Disciplinary Procedure should be undertaken. Further disciplinary action may be taken if appropriate, following the completion of the investigation.

vi. All STU facilities shall be accessible between the standard working hours of 8: 00 am to 5:00 pm on working days, except the cleaners and labourers whose work at times requires them to work outside this period

vii. A person shall be granted access to a facility outside working hours if such a person produces his/her STU ID Card or upon a recommendation from the HOD, either in writing or verbally.

Section 3 – Asset Protection Equipment/Documentation

Security of Equipment

i. All valuable equipment such as laptops and other portable devices shall be locked away out of sight when not in use, especially overnight.

ii. The University shall adopt, if it hasn't, a uniform labeling system for all items/materials issued to staff and staff shall at all material times adopt the labeling system.

iii. Pre-printed headed paper (letter head) and other stationery displaying the University's logo, staff names/designations and telephone numbers should be locked up in cabinets when not in use.

Security Hardware

i. All technology installations relating to security on any premises on STU campus shall be undertaken in consultation with the security unit.

ii. All technology installations relating to security shall be done on the advice of the campus security committee and shall be done in compliance with the Data Protection Policies of the University

iii. All the components of the University WIFI should be pass-worded, especially when the University is on break. This is to check the rate at which outsiders enter the campus to browse freely.

Security of STU Buildings

i. The security guards shall go round and ensure all doors and windows to facilities are locked and electrical equipment switched off, after the close of work. Offices where doors/windows are found not locked and/or electrical equipment not switched off shall be taken note of and the heads informed on the next working day.

ii. If these are found to be committed by officers who take their keys home however, such officers shall be called to come back to campus to get the doors locked or gadgets switched off or both.

iii. Under no circumstance should any staff other than the designated ones, take a key or keys of STU facility home.

SECTION 4: Perimeter Vehicle Entry and Parking

Traffic on Campus

i. Barriers, one-way streets, limited ingress, street bumps and signage shall be introduced to discourage over speeding, wrongful parking and other avoidable intrusions and obstructions on campus.

ii. With the exception of designated parking lots, the entire STU campus shall be a pedestrian-only zone.

iii. Only authorized vehicles shall be allowed access to the STU campus

iv. All streets, parking lots, sidewalks and crosswalks on campus shall be clearly marked to keep pedestrians on sidewalks and cross walks and out of traffic in the streets and parking lots.

v. Strict speed limit of not more than 25km/h shall be observed and this would be enforced on the University campus

SECTION 5: Prohibited/Disruptive Activities on STU campus

The following activities shall be considered as prohibited/disruptive activities on STU campus:

i. Forcible entry (breaking of doors to have access) into any office(s) on campus, including but not limited to doors installed with technology access systems. Disabling automatic door closers, locking door hardware, exit devices etc.
ii. Disabling security device(s) such as CCTV cameras, local sounder exits alarms, smoke alarms etc.
iii. Obstructing stairways, building exits, hallways and doorways.
iv. Locking emergency exit doors in the path of free outlet travel.
v. Unauthorized installation of security equipment, accessories and systems, security devices, cameras and fake cameras.
vi. Unauthorised accumulation, duplication, or possession of STU facilities' keys.
vii. Unauthorised use of an assigned STU ID Card or permitting another person to use one's designated STU ID Card.
viii. Unauthorised use of an assigned STU Pin code or permitting another person to use one's designated STU Pin code.
ix. False activation of fire alarm manual pulls stations or emergency telephones etc.,
x. Noise on campus during working days without authorisation from Vice-Chancellor
xi. Use of illicit drugs/involvement in any conduct under the influence of intoxicants etc.
xii. Possession of weapons and/or any instrument that constitutes a threat to other members of the University community
xiii. Violence against any student, employee or guest of the University.
xiv. Theft or willful destruction of STU property or the property of any member of the University.
xv. Forcible interference with the freedom of movement of any student, staff or guest of the University
xvi. Obstruction of the normal processes and activities essential to the proper functioning of STU community.
xvii. Organise event on STU premises without prior approval by the Vice Chancellor

SECTION 6: Sanctions for Breach of Security obligations

i. STU reserves the right to take appropriate legal action against any person(s) who act(s) negligently, dishonestly, or commits a crime against the University.

ii. Any violation of this University Security Policy shall be treated as a disciplinary offence and any criminal offence committed thereof shall be treated as a criminal offence under the laws of Ghana.

SECTION 7: Lost and Found Items

i. Any property deemed as lost and /or found item shall be reported and/or deposited at the main security post of the University.

ii. The reporter/depositor shall complete a form designed for that purpose

iii. Where such deposited item(s) are claimed by any person, such claimant shall be required to provide details of the item, including but not limited to details of ownership of such item.

iv. The security officer in charge shall, when satisfied with the claims of ownership of a deposited item, require the claimant to fill a prescribed form prior to delivery of the item to the claimant

v. The chief security officer shall ensure the amicable resolution of any disputes with respect to the ownership of a lost and/or found item.

SECTION 8- MISCELLANEOUS ITEMS

Visibility and Surveillance

Three methods of surveillance should be considered:

i. Natural – the area is visible to other occupants or passers by

ii. Formal – using technology and/or people to monitor the area and deter

iii. Informal – encouraging employees to be vigilant

Environmental Design and Perimeter Control

A range of security measures should be considered at the design or planning stage of a building or refurbishment. Perimeter controls or surveillance methods should be considered.

i. Garden areas should be studied to ensure that unnecessary 'hiding spots' can be minimised, especially those close to doors.

ii. External lighting needs to be risk assessed and enhanced as required.

iii. Bin collection points need to be assessed for the risk of providing unmonitored access to the University.

Security Operation

The security operation at Sunyani Technical University shall consist of patrol and static security at all time. The main purpose is to maintain the security of the premises under the security guard's duty. A security patrol involves the review and surveillance of premises to ensure they remain safe from any potential threats. They also help make sure staff, visitors, customers or guests are monitored and protected from potential threats. Patrol security comprises the following;

Foot patrol

A foot patrol involves a security guard, or guards depending the size of property, walking the grounds on foot to check for any potential threats or issues. This range from checking windows and doors are locked, to ensuring there are no fire hazards or safety issues on the site. An effective foot patrol solution will identify any potential risks quickly and efficiently respond to and rectify them.

This type of security guard patrol is perfect for spaces where vehicles cannot go and can be customised depending on your needs. It can also be well-suited to locations that receive high levels of external visitors, as security officers delivering foot patrols are discreet and can even enhance service delivery.

Mobile patrol

Mobile patrols are a great alternative to static security, perfect for those larger sites with more ground to cover. These involve regular site-wider surveillance and it is a cost-effective visual deterrent against crime and ideal for multi-site or larger premises.

Mobile patrols allow security officers to cover a large amount of ground quickly, perfect for any emergency situations like an alarm being triggered or a potential fire hazard.

Observation post

Another type of effective security patrol is an observation post, or watchtower, which allows for 24 hours security surveillance by a trained security officer.

The type of security patrol is ideal for larger properties and premises that have a more specific set of security and protection requirements. The high-up vantage point offers security officers full visibility of the site, allowing them to respond quickly and efficiently to any potential threats.

Camera surveillance or CCTV

CCTV security systems are a great way of providing 24/7 monitoring of your site, without having to invest in round-the-clock security officers.

Well-signed CCTV systems not only act as a visual deterrent to any potential criminals but can also contribute to reductions in your insurance premiums as you have hard evidence of any criminal activity.

Training of security personnel

There shall be continuous career enhancement training for all campus security staff to raise their capability and competency levels in:

i. Logbook/station diary entries
ii. Security Report writing
iii. First aid
iv. Identification of fires and firefighting techniques
v. Types of crowd and crowd control techniques
vi. Basic intelligence and Intelligence gathering techniques
vii. Security code recital
viii. Traffic control mechanisms
ix. Legal limitations of the private security guard
x. Reception duties including directions to visitors.
xi. Basic human rights

Review of University Security Policy

The campus security committee shall, subject to the approval of the vice chancellor, review the University policy for such periods and in such manner as shall reflect international best practices required to safeguard security on STU campus.

Conclusion

The contemporary education landscape makes security detachments a key pillar in the smooth running of educational institutions across the globe, STU not an exception. The conversion of the erstwhile Sunyani Technical Institute into a Polytechnic in 1997 and the corresponding increase in student enrolment called for a robust mechanism to safeguard the enlarged new community, hence the creation of a security unit to replace the watchman system operated under the former.

The upgrading of the Polytechnic to a University in 2016 came with new challenges including larger student populations, increased staff numbers and expansion of facilities. This called for the

re-engineering of the security architecture culminating in the strengthening of the security unit with additional guards and more resources. This policy is therefore a blueprint to guide the University management in their quest to ensure safe academic environment to achieve the vision and mission of the University.