UNIVERSITY OF ILORIN, ILORIN, NIGERIA

SECURITY POLICY

2024

1.0 Introduction

The University of Ilorin, Nigeria, situated on about 15,000 hectares of land has over 50,000 undergraduates and 7000 graduate students pursuing various programmes across its three campuses: Main, Mini and School of Preliminary Studies, Fufu. The University, in the last 15 years, remains the most subscribed by admission seekers in Nigeria. The workforce is put at 4000. As a university of repute, it boasts students and staff from all parts of the globe. Similarly, thousands of visitors throng the University. To provide adequate security for the vast space and the large population, the University has a well-equipped security Division.

Campus safety is of paramount importance. Universities are places of learning, personal growth, and community services; ensuring the safety and well-being of students, faculty, and staff is fundamental to maintaining this environment. A safe campus fosters a conducive atmosphere for education where individuals can pursue academic and extracurricular interests without undue fear or concern. Families, when selecting an educational institution, often prioritise campus safety as a deciding factor, reflecting its central role in academic experience. The emphasis on campus safety underscores the commitment to protect the future of the nation - its young minds and leaders.

One of the cultures of any University which Unilorin keys into, is to allow open access to its campus but this is not without its attendant risks. Therefore, this policy describes the approach to ensure security across many areas of the university's campuses. This Security Policy formalizes a cohesive and integrated approach to security and all associated activities across the campuses.

There are two stakeholders identified in this policy document, these are both the internal and external stakeholders. These different categories of stakeholders are put into consideration in drafting this policy document and architectural designs for its implementation to enhance its utmost success.

2.0 Justification for Campus Security Policy

In view of the emerging security threats, it has become imperative to have a campus security policy guideline for the protection of lives and properties in the University because:

i. the campuses harbour mass gatherings of people which provides opportunity for those with criminal intents to carry out nefarious act;

ii. the movement of people for events within the campuses is highly predictable with a precise timeline for campus activities;

iii. most people within the campuses are not security conscious, believing that campus security is the sole responsibility of the Security Division; and

iv. important data and other security information are stored and transmitted electronically which may be susceptible to unauthorized access.

3.0 Aim and Objectives of Campus Security Policy

Aim

The security policy aims to prevent, respond and manage security threats and challenges to promote a safe and secure work, study and living environment.

Objectives

The objectives of the University of Ilorin Campus Security Policy are to:

i.   provide the platforms and policy direction for a safe academic environment for campus stakeholders;

ii.   relieve parents/guardians of fear and concern for the safety of their children/wards by making the campuses a home away from home;

iii.   prevent, reduce, or de-escalate violence of all kinds within the campuses;

iv.   tone down tension arising from campus stakeholders' diversities, which, sometimes, are a source of conflict generation; and

v.   build a good reputation for the University. With the right security systems in place, the campus will not only look great to prospective students and parents but also significantly assure them of adequate security.

4.0 Policy Statement

The Policy statement shall be based on five principles namely deterrence, detection, delay, assessment, and response. The University Security Committee and the Security Division, the University Legal Unit and COMSIT shall be responsible for the effective operation and implementation of the Security Policy and for procedures and compliance with all associated laws and legislations. Anybody who violates the standards of behaviour set out by the University shall be made to face disciplinary action in line with the relevant laws of the University. Where behaviour on our campuses may constitute a crime, the University will work collaboratively with Law Enforcement Agencies to support any criminal investigations.

5.0 Scope

The scope of this policy covers:

i. the personal security and safety of the University's staff, students, contractors, tenants, clients, visitors, and members of the public at all the campuses;

ii. information and data security including reference to cyber security and the protection of personal data; and

iii. the physical security and safety of the University's campuses, buildings, and other assets.

6.0 Policy Implementation

The provision of security requires a balanced approach to ensure that security and safety are provided efficiently. The University will also complete a security risk assessment in advance of relevant events within the University to ensure that reasonable and proportionate security measures are in place. Events requiring risk assessments will be defined using judgment based on their size, type, and potential risks, with advice from relevant experts.

In implementing this policy, the University of Ilorin will adopt a layered approach to security and will:

i. reserves the right to limit access to areas within its campuses to students, staff and other stakeholders;

ii. take additional security measures to protect its high-value assets, high-risk facilities, and confidential document storage areas;

iii. Provide additional security measures to ensure the protection of stakeholders, equipment as well as digital assets of the University. These measures include but not limited to:

(a) the provision of digital locks on doors where necessary;

(b) the requirement for all IT equipment to be marked with a unique identification code and all servers to be installed in secure locations; and

(c) liaison with staff who work off-site to ensure appropriate measures are taken to minimise the risk to their safety and the security of any equipment being transported.

(d) safeguard and protect all electronic storage and data asset, using the approved University guidelines

iv. provide a range of Personal Protection Security measures for those staff who work in high-risk situations; these measures may include the:

(a) introduction and operation of CCTV surveillance in sensitive or higher-risk areas in or around the

University as agreed in conjunction with the management team and the University's CCTV Policy and Code of Practice;

(b) provision of security patrols around the three campuses in buildings, accommodation spaces, and other university-owned property; and

(c) provision of personal (panic) alarm systems at strategic and higher-risk locations or on persons.

v. adopt the use of covert cameras which are not in general use around the campus. However, on occasion, it may be necessary to operate such cameras to detect crime and/or apprehend offenders. Before use, permission to use covert cameras will be obtained through the head of the relevant department or division.

The University's layered approach shall be defined as follows:

i. the built environment of the University should have a minimum of two means of security; in practice, this will mean locks on doors and windows along with a suitable and efficient intruder alarm system to be utilised when the building/area is not in use; some areas on the University premises will require additional measures, such as the focused use of monitored CCTV and security personnel on hand to test that they are secure;

ii. internally, buildings should have easy open access to public areas as appropriate; access from open areas to secured areas within a building should be incremental and appropriate to the use, contents, and sensitivity of the area to be protected; and

iii. where there is a wide range of means to secure movement from one area to another, a threat and risk assessment process should be carried out by the Security Unit through which building users and other interested parties may raise issues, concerns, threats, and challenges to enable the Security Unit implement appropriate security measures. Some areas of the University estate will require greater restriction and stronger access control to safeguard University assets or to comply with the requirements of external regulatory bodies.

The University shall also:

a. reserves the right to require individuals on university premises to show verification of identity to confirm that they are entitled to have access;

b. reserves the right to require individuals who cannot verify their identity and entitlement to be on the University's campuses to leave the university and premises;

c. requests for the assistance of Security Agencies in the event of any criminal offense being committed on the University premises, following appropriate protocols for requesting assistance from the policy;

d. provide advice to staff, students, and visitors on personal safety and the security of items and equipment; and,

e. exercise campus-wide security control and direction and shall issue procedures that will be widely communicated. The Security Unit shall continue to work closely with the Federal Security Agencies to ensure the safety and well-being of the University. The University Security Committee will keep procedures and practices under regular review in the light of evolving local and national challenges and guidance.

7.0 Campus Security Implementation Skills

Having strong security guard skills will help the Security unit improve on its operational capacity and boost the expertise of security personnel to handle security situations more effectively within the campus. Thus, the training programmes of the security unit will be focused on the specific skills of security personnel and their areas of specialisation.

a. Communication Skills

Effective communication skills will improve the ability of security personnel to express their ideas and thoughts to other people, especially to the campus stakeholders using expressions, words, sign language, or actions to:

i.   communicate responsibly (without using insulting or abusive language on the guests)

ii. develop the skills of multilingual capability, especially in the popular languages within the operational environment; and

iii. apply dynamic communication skills toward writing and producing detailed reports.

b. **Analytical and Foresight Skills:** Developing the analytical and foresight skills of the relevant University personnel will enhance their capability of taking appropriate security actions.

c. **Developing digital skills on criminal call codes and swindling styles;**

d. **Developing Strong patrol and Surveillance skills:** intense physical exercises, adequate food in-take for duties which involve embarking on foot and vehicle patrols of campus grounds, buildings, and residence halls designed to detect any crimes in action as some areas cannot be accessed by vehicles;

e. **Knowledge Skills and Abilities (both academic and practical experiences);**

f. **Physical Skills and Ability;**

g. **Teamwork Skills;**

h. **Leadership Skills;**

i. **Organizational Skills:** for proper coordination, documentation, and precision in time management; and

8.0 Use of Technical Surveillance

8.1 Reasons for Use

The use of Technical Surveillance has been recognized as a powerful tool in the fight against crime, both in its prevention and detection. The University will engage CCTV systems around the campus covering many access points and adjacent streets. This objective will be met through the monitoring of the system to:

i. Assist in the prevention and detection of crime;

ii. Facilitate the identification, apprehension, and prosecution of offenders about crime and public disorder; and as an aid to public safety;

iii. Assist in the University's emergency procedures;

iv. Assist in civil emergencies;

v. Assist with traffic management;

vi. Promote safe communities;

vii. Provide a training facility; and

viii. Provide and operate the system in a manner which is consistent with respect for the individual's privacy.

8.2 CCTV Operating Procedures

These procedures ensure that concerns over integrity, confidentiality, and ethics are not compromised. It is intended that the information obtained from CCTV will give the public confidence that the rights of individuals are being fully protected, and the requirements of Nigeria Data Protection Regulations are complied with. Access to the CCTV monitoring and recording system is strictly controlled and is limited to duty security staff or authorized management.

9.0 Organisation and Responsibility:

A. The Vice-Chancellor is the overall chief superintendent and custodian of all security matters in the University. He shall give policy direction regarding the issue of security.

B. The University Security Committee shall receive regular reports of the activities of the Security Unit. The Committee reviews reports and, as appropriate, communicates concerns about identified issues and regulatory compliance to the Vice-Chancellor, through its Chairman, the Deputy Vice-Chancellor (Management Services). The Committee provides support to facilitate the ongoing activities of the Security Unit.

C. The Director of the Security Division shall, in collaboration with the Deputy Vice-Chancellor: Management Services, establish and oversee all aspects of the Security Programme. The Director of the Security Unit shall convey through the Security Committee security issues that may necessitate changes to policies, orientation or education, or purchase of equipment to the Vice-Chancellor.

D. Staff, students, and visitors are responsible for learning and following University procedures on security. Where necessary, the Director of Security ensures that the security programmes of the university have the essential buy-in of all critical stakeholders to ensure campus-wide public safety.

9.1 Responsibilities

The responsibility for security and personal safety rests with all persons who work and study at or who visit the University. In addition, the following designated members of the University community shall carry these additional responsibilities:

9.1.1 Staff

All staff must ensure they are familiar with, and follow, the procedures in the University Security Policy and pay particular attention to those issues that are relevant to their activities. They must also cooperate with requests from Security Officers, especially in emergency or evacuation situations, and about security procedures. Staff are requested at all times when on university premises to carry their University ID cards.

9.1.2 Students

Students have a responsibility to look after the University facilities and their personal property and to give due consideration to their personal security issues. They must follow security procedures designed to protect University property. Students must cooperate with requests from the security team, especially with emergency or evacuation instructions and on security procedures.

9.1.3 Visitors

All visitors, including conference delegates and event attendees have a responsibility to look after University facilities properly and to give due consideration to security issues. In particular, they must follow security procedures designed to protect University property. It is the responsibility of

the host to ensure all visitors are informed of, and comply with, the University Security Policy at all times, especially during emergency procedures.

9.1.4 The Deputy Vice-Chancellor (Management Services)

He shall be the Chairman of the University Security Committee and complement the Vice-Chancellor in the day-to-day monitoring of the security situation on campus. He/she manages and monitors the implementation of the security policy and ensures its full implementation and works with the Security and Fire Services Units and other Federal Security Agencies to ensure the safety of the campus. He shall be responsible to the Vice-Chancellor.

9.1.5. Dean of Student Affairs

The Dean of Student Affairs shall ensure the safety and protection of the students while on campus. The Dean shall monitor the living conditions of the students and deploy strategies to ensure that their safety and well-being are not compromised.

9.1.6 Director of Works

The Director of Works has responsibility for ensuring that facilities including hostels and offices, staff accommodation, roads, and vehicles (both public and private) operating in the University campuses are safety compliant, and in line with global best practices.

9.1.7 Director of Physical Planning Unit

The Director of the Physical Planning Unit shall ensure the safety compliance of all buildings (either public or private) on campus through monitoring and offering professional services during their design and construction.

9.1.8 Director of Health Services

The Director of Health Services shall ensure the public health and safety of the University community through planning, organising, and directing Student and Staff Health Services operations and activities; ensure that related activities comply with established standards, requirements, laws, codes, regulations, policies, and procedures; implement, evaluate and develop standardised procedures and clinical protocols; and plan, organise, promote and direct health education functions and activities to enhance health awareness and public safety.

9.1.9 Director of Security

The Director of Security is the Head of the Security Unit and has responsibility for: the management and implementation of the security policy and procedures; monitoring these policies and procedures to ensure their continued effectiveness; delivery of an efficient and effective

security service to the University; management and training of security staff; investigation of serious crime or confidential breaches in security; provision of expert and impartial advice to the University management; emergency management and liaison with the police and other security agencies, other emergency services and local authorities where relevant; risk management, analysis and implementation of security solutions; provision of security hardware including keys, locks, safes, access control, CCTV, intruder alarm installations; and maintenance of good order on campus.

9.1.10 Head of Fire Services Unit

The Head of the Fire Services Unit's main mission is to protect life and property. This means planning, developing, implementing, and monitoring a fire safety plan that addresses specific fire and life safety systems. He/she is also in charge of training and supervising personnel needed to carry out the overall mission and each element of a fire safety plan. He is also to advise on fire issues relating to building structure and fabric, services, alterations, and maintenance; advising on fire safety requirements for new buildings, coordinating and monitoring the University's program of fire risk assessments. He is also to liaise with the Federal/State/Local Fire Services/Authorities involved in fire safety, advising on fire issues relating to the day-to-day activities of the University community.

9.1.11 The Mayors

The Mayors in the staff quarters shall work with the relevant units/officers to ensure the safety of occupants, buildings, properties.

9.1.12 Security Officers

Security Officers have responsibility for the promotion of crime prevention and access control; patrolling all areas on campus; maintaining good order on campus, the provision of a safe environment; providing security support to the university community and visitors.

9.1.13 Special Marshal

The Unilorin Special Marshal Unit is a voluntary arm of the Federal Road Safety Corps that operates to monitor road users by ensuring that orderliness and relevant traffic laws and regulations on the roads are maintained. They assist staff, students and visitors navigate the campus smoothly, especially during periods of high traffic as seen during occasions, such as inaugural lectures and convocation ceremonies.

9.1.14 Heads of Department/Unit and Heads of Professional Services Sections

The Provost, Dean, Director, and Heads of Departments/Units are vital in promoting security and safety within their units. The responsibilities will vary according to the location of the department

or section and the nature of its activity, but several general responsibilities can be identified. The Heads of Units may wish to delegate responsibility for routine tasks to a nominated individual in their unit. Still, the overall responsibility for security matters shall remain with the head of the unit.

The general responsibilities held by all Heads of units are to:

i. ensure that all members of staff and students in their department or section understand and exercise their security responsibilities, including the display of identification cards (ID) where appropriate whilst on campus and having due regard to University property, in particular, the security of equipment and personal and institutional data and information;

ii. liaise with the University Security Committee and Director of Security or his nominee on any security matter and attend security coordination meetings if required;

iii. undertake a security risk analysis of their unit and operations, and in liaison with the security unit, act to remove or reduce as far as possible any security risks;

iv. control access to their unit by taking responsibility for the issue of keys and by authorising staff to have 'out of hours' access only as necessary;

v. ensure that their departmental/section staff return to the department/section their University ID and any issued keys on their last day of work;

vi. notify the Head of the Security Unit or their nominee of any potential security risk, who will then advise on any additional security or protection and investigate any related crime or incident; and

vi. ensure that all staff, including all those with a contract of work, research staff, visiting lecturers, and anyone employed as a tutor, supervisor, or lecturer on an ad hoc basis, are familiar with, and follow the procedures linked from, the University Security Policy, paying particular attention to those issues which are relevant to the activities of relevance to the department/section/individual.

10.0 Campus Security

The Security Unit maintains policies for the identification of students, staff, and visitors. All employees and students are required to display identification cards on their upper body while on duty. Identification cards are to be displayed picture-side out.

i. Students and employees are issued identification cards. These ID cards are required to access some facilities and buildings on campus buildings. The identification card is to be worn on the upper torso where it can be easily seen.

ii. Staff, students, and visitors must respect the parking lot access principle which varies from unit to unit.

iii. Closed-circuit television monitors are in place in relevant places on campus and allow viewing of the interior and exterior of all buildings, parking lots, and hostels on campus.

iv. Hotlines and Emergency Phone lines are located at every nook and cranny of the University.

11.0 Access control

11.1 Control and Use of the University of Ilorin Identity Cards

i. The University provides photographic identification cards to identify the cardholder.

ii. The University Management oversees the University's official and authorised identification card system. No other parties are permitted to create, alter, or replicate the authorised identification card system.

iii. All University identification cards remain the property of the University and shall not be duplicated, traded, or provided to anyone other than the person it is issued.

iv. Students can apply for their identification cards through the Student Affairs Unit. University Staff can apply for identification cards through the Directorate of Academic Support Services.

v. All staff and students are required to always carry their ID Cards with them.

vi. Members of the University Community shall present their University identification cards upon reasonable request from the Security Unit or any authorised individual, without refusal or unreasonable delay.

vii. Should a member of the University Community misuse or inappropriately use their ID card in a manner inconsistent with their role or responsibilities, this may result in the immediate deactivation of the card and its associated privileges.

viii. The visitors and ad hoc contractors will be issued a visitor's pass at the point of entry and are expected to wear these passes throughout their stay or visit to the University.

ix. The staff member responsible for the visitor/contractor should ensure they submit the visitors' pass when signing out upon leaving the campus.

x. Contractors who will be on-site for more than a week will generally be issued a peculiar University identity card to allow them access to the building they are working in. Arrangements for these cards are to be made by the Director of Works.

11.2 Security in the office

All staff are expected to be aware of, and familiar with, all procedures that ensure a safe and secure environment for personnel, equipment, documentation, and information in their office areas. General Awareness:

i. University ID cards should be worn by students and staff at all times on university campuses.

ii. Staff should have the University Security and Fire Units Hotlines for reporting incidents on their phones and readily available should they require any assistance.

iii. Staff working 'out of hours 'should ensure they follow 'out of hours' procedures and contact the Director of Security through their Heads of Units if they need assistance. At the end of each working day, staff should ensure that:

a. valuables and confidential documents (laptops, sensitive data, personnel files, etc.) are locked away with keys secured in key cabinets or taken home;

b. any departmental keys that have been issued during the day have been returned and any losses reported immediately;

c. a 'clear desk policy' is maintained where it is possible to ensure confidential and personal data and documentation are locked out of sight;

d. all non-essential electrical appliances are switched off/unplugged;

e. doors and windows are closed and locked as appropriate; and

f. curtains and blinds are closed, with any items on windowsills that hinder closure removed, and lights turned off.

11.3 Key and lock management

The Porter Unit controls the issue and use of all locks and keys in offices and hostels while the Estate Unit controls keys and locks to the staff residential accommodation. No other make of lock or key should be installed on the University campuses without the authority of Porter, Estate, and the Security Units as the case may be. Operator keys or sub-master keys may be issued to departments or sections for local use and be issued to individual staff. All digilocks installed on University campuses must be fitted with a master key override to allow the Security Unit the ability to enter the room in an emergency. All digilock installations must be requested via the Porter Unit. The department/section should keep a record of all keys issued locally and ensure that staff return keys when they leave offices daily or when permanently leaving the University employment. The Porter Unit will also monitor the keys issued. 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 the Security and Porter Units. The Porter Unit has the facility to access student accommodation located on the University campus. Any student keys or cards that have been lost should be reported to the Hall porter or supervisor.

All keys belong to the University and are not exclusive. The Porter Unit carries out duties over 24 hours, 365 days per year, and requires the availability of keys for ease of access to all areas by the Fire Service or the Security Unit, especially in emergencies. In exceptional circumstances, certain restrictions may apply to sensitive areas, but agreement should be achieved between interested parties regarding access in any emergency. The following principles must be adhered to in the management of keys and locks:

i. All losses of keys/cards must be reported immediately to the Security and Porter Units;

ii. Persons leaving the University or transferring to another department or section are to return their keys directly to their departmental or section office; they should not pass keys directly to their replacement as these need to be audited for security purposes;

iii. Replacement keys will only be issued after an investigation of the loss; the cost of replacement will be charged to the department/section or individual concerned;

iv. 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 department or section concerned; if loss of master or sub-master keys is suspected to have arisen through negligent action by a member of staff, student, or contractor, then an investigation under the appropriate disciplinary procedure or code of conduct should be undertaken. Further disciplinary action may be taken if appropriate, following the completion of the investigation.

11.4. Vehicle Tallies

Based on standard practice, access to the University Main Campus should be appropriately controlled. This is achieved by registering and issuing tallies to all vehicles entering the University. Similarly, all security operatives at the University access points should adhere to the standard Access Control procedures.

12.0 Reporting Incidents

It is the responsibility of all students, staff, visitors, and members of the public to report all activity, suspected or real, of a security/safety nature. Incident reporting is crucial to the identification of patterns of criminal activity and the analysis of risk. It also helps to identify security issues relating to data loss and unlawful access to digital materials. It permits investigation and recommendations to be made to prevent any recurrence. Comprehensive reporting of incidents provides an accurate picture of the level of crime throughout the University of Ilorin campuses and thus ensures that adequate resources are provided to combat that crime. Success in the investigation of any issue is greatly

enhanced by fast, efficient, and detailed reporting. The following principles should be adhered to at all times when reporting incidents:

i. All incidents of security/safety nature and emergencies on the university campuses should be reported promptly to the appropriate university officials such as the Director of Security or any campus security personnel and Head of Departments/Units. Reports can be made in person, by phone, or through the university's online reporting system, and can be submitted anonymously if desired. The Security Team shall always treat any reports seriously and respond accordingly. Departments or individuals responsible for an activity that may impact on the security of the campus, or the halls of residence must also report this to the Security Team.

ii. The university will investigate all reports promptly and thoroughly, taking appropriate actions to address safety and security concerns and prevent future incidents.

iii. Victims of all crimes are advised to first inform the University Security Unit or the Head of Department or unit. For students residing in campus hostels, however, the first report can be made to the Hall Masters/Mistresses or directly to the Students Affairs Unit. On no account must any crime be escalated to the Federal Security Agencies without consulting the Security Unit.

iv. The university will as much as possible respect the wishes of victims of suspected crimes who do not want them to be referred to the security for investigation; the Security Agencies should only be contacted if the victim-survivor gives their consent to do so, as the victim-survivor must be empowered to choose the reporting options that feel right to them; as a matter of fact, staff should not go against the individual's wishes and report the incident to the Security Agencies without their consent; Security Agencies should be informed without the consent of the victims only in cases where there is an immediate and serious risk to the safety of others; in these cases, the University reserves the right to report suspected criminal offenses committed by staff, students, or visitors to the Security Agencies, in line with the relevant disciplinary procedures or by any Data Sharing Agreement;

v. For no reason must there be the involvement of Security Agencies on University campuses without prior approval of the Vice-Chancellor, who shall direct the Director of Security on how to ensure effective management of the actions required on campuses. The operations of the Security Agencies on any of the University campuses will be undertaken in line with specific agreed protocols;

vi. Criminal offenses committed by the students will be reported to the Police by the Director of Security, in line with General Students Regulations; and

vii. Where appropriate, in addition to any of the Federal Security Agencies' involvement in alleged criminal offences by staff and students, the University will refer security incidents that may constitute breaches of its own Codes of Conduct for possible consideration under the relevant

disciplinary procedure.

13.0 Criminal investigations

All crimes on university campuses shall be investigated appropriately to punish offenders, prevent recurrence, and aid crime prevention. The Security Division as delegated shall carry out internal investigations of security-related incidents, producing written reports for University Management where necessary and providing follow-up crime prevention advice.

14.0 Reporting Incidents

It is the responsibility of all students, staff, visitors, and members of the public to report all activity, suspected or real, of a security/safety nature. Incident reporting is crucial to the identification of patterns of criminal activity and the analysis of risk. It also helps to identify security issues relating to data loss and unlawful access to digital materials. It permits investigation and recommendations to be made to prevent any recurrence. Success in the investigation of any issue is greatly enhanced by fast, efficient, and detailed reporting. The following principles should be adhered to at all times when reporting incidents:

i. All incidents of security/safety nature and emergencies on the University campuses should be reported promptly to the appropriate university officials such as the Director of Security or any campus security personnel and Head of Departments/Units. Reports can be made in person, by phone, or through the university's online reporting system, and can be submitted anonymously if desired. The Security Team shall always treat any reports seriously and respond accordingly. Departments or individuals responsible for an activity that may impact on the security of the campus, or the halls of residence must also report this to the Security Team.

ii. The university shall investigate all reports promptly and thoroughly, taking appropriate actions to address safety and security concerns and prevent future incidents.

iii. Victims of all crimes are advised to first inform the University Security Unit or the Head of Department or unit. For students residing in campus hostels, however, the first report can be made to the Hall Masters/Mistresses or directly to the Students Affairs Unit. On no account must any crime be escalated to the Federal Security Agencies without consulting the Security Division.

iv. The university will as much as possible respect the wishes of victims of suspected crimes who do not want them to be referred to the security for investigation; the Security Agencies should only be contacted if the victim-survivor gives their consent to do so, as the victim-survivor must be empowered to choose the reporting options that feel right to them; as a matter of fact, staff should not go against the individual's wishes and report the incident to the Security Agencies without their consent; Security Agencies should be informed without the consent of the victims only in cases where there is an immediate and serious risk to the safety of others; in these cases, the

University reserves the right to report suspected criminal offenses committed by staff, students, or visitors to the Security Agencies, in line with the relevant disciplinary procedures or by any Data Sharing Agreement;

v. For no reason must there be involvement of Federal Security Agencies on University campuses without prior approval of the Vice-Chancellor, who shall direct the Director of Security on how to ensure effective management of the actions required on campuses. The operations of the Security Agencies on any of the University campuses will be undertaken in line with specific agreed protocols;

vi. Criminal offenses committed by the students, staff and visitors shall be reported to the appropriate Federal Security Agency by the Director of Security, in line with extant rules and regulations; and

vii. Where appropriate, in addition to any of the Federal Security Agencies' involvement in alleged criminal offences by staff and students, the University will refer security incidents that may constitute breaches of its own Codes of Conduct for possible consideration under the relevant disciplinary procedure.

15.0 Anti-Social Vices

The Security Division's database on security targets and identified anti-social elements within the campus shall be regularly updated. In this regard, a healthy security liaison must be maintained with Federal Security Agencies to facilitate security enforcement when and where necessary.

16.0 Vehicle Parking Management

16.1 Visitor Parking

Visitors' Parking space is available but limited. It is the responsibility of the member of staff to make necessary arrangements and inform their visitor. Vehicles and their contents are left on University property at the owners' risk. The University accepts no responsibility for theft or damage to vehicles on its premises.

16.2 Enforcement

Drivers of vehicles parked in breach of the Parking Policy are liable to receive penalty notice.

16.3 Motorcycle Parking

Anyone leaving a motorcycle or scooter on university premises must leave it safely and securely locked.

The University cannot accept any liability for vehicles, motorcycles scooters, or bicycles or their

contents when parked or left on university premises.

17.0 Emergency Response

These include responses for normal activities (such as door opening, and escorts), urgent activities (such as requests for assistance and stand-by, reports of theft, and other crimes), and emergency responses (such as immediate student or staff danger, fire alarms, disasters, and similar activities).

General procedures for these types of events guide security or University staff. Security Services and designated staff are trained to recognize, and respond to, specific emergencies as defined in these plans. The plans also provide processes to inform leadership, and as needed, implementation of campus-wide emergency activity (e.g., campus-wide communication/notification) and/or implementing the emergency operations plans.

Any incident involving students, visitors, personnel, or property should be reported to the Security office. A Security Officer will take all information regarding the incident and record it on the Security Incident Report. The Director of Security shall present a summary of all incidents, corrective actions, as well as trends in crime and location to the University Security Committee. The Committee, after thorough analysis, shall present its recommendations to the Vice-Chancellor.

18.0 Asset protection, equipment, data, and documentation

The safekeeping of all University property will help to ensure that equipment is available for use at all times. It is the responsibility of all staff and students to take reasonable measures in protecting the University's property, as well as their personal property, from theft or damage. Staff members have a special responsibility to take appropriate measures to ensure that equipment directly under their control is kept safe and secure. Members of staff are expected to seek advice from the Security Team.

19.0 Management of lost property

i. Management of the lost property is the responsibility of the University Security Unit.

ii. Unattended property that appears to be abandoned or left unattended in the University buildings or grounds may be treated as lost property.

iii. Individuals who have lost their property may visit the Security Unit to determine whether their item has been turned in.

iv. Individuals whose property is lost or missing may file a report with the University Security Division within 24hours after becoming aware so that they can be contacted if their item is found and turned

in.

v. After a reasonable time, if the property found has not been claimed, all items shall be handed over to the relevant Security Agencies.

20.0 Security Liaison

This involves maintaining a good relationship with all Federal Security Agencies (FSA). The University Collaborators in this regard include but not limited:

- The Nigerian Police Force (NPF)

- Department of State Services (DSS)

- Nigeria Security and Civil Defense Corps (NSCDC)

- Federal Road Safety Corps (FRSC)

- Federal Fire Service (FFS)

- Nigeria Drug Law Enforcement Agencies (NDLEA)

21.0 Flow of Intelligence

There must be a free flow of intelligence from both the State Security Agencies and the Campus security formations. Security Liaison with the Federal Security Agencies also facilitates the following:

- Prompt Security support when needed;

- Prosecution of apprehended Criminals on any of the University campuses;

- Quick resolution of clashes between stakeholders on campus and host communities; and

- Provision of security awareness workshops and seminars for campus security operatives.

22.0 Invitation of Federal Security Agencies

Invitation of Federal Security Agencies to mitigate any crisis on campus can only be authorised by the Vice-Chancellor on the advice of the Campus Security Committee or the Director of Security, as the case may be.

23.0 Mitigation Efforts by Federal Security Agencies

Federal Security Agencies are not expected to use live ammunition on campus to mitigate crises. A total breakdown of law and order in the University shall be handled professionally in line with the best practices. Invitations by Federal Security Agencies to students or staff of the University to assist in an ongoing investigation shall go through the office of the Director of Security. In this regard, after appropriate clearance from the Vice-Chancellor, the Director of Security shall provide adequate assistance for the Federal Security Agents where necessary.

24.0 Holding Facility

The Security Division maintains a Holding facility, where suspects are kept in accordance with the law while a case is under Preliminary Investigation. The suspect may then be transferred to relevant Federal security agencies for further investigation and possible prosecution.

25.0 Campus Closure

i. The University may be required to either partially or completely close one or more of its facilities, in response to an emerging or current crisis.

ii. The University Security Unit may implement restrictions to University staff, Students and other stakeholders refusing entry and limiting electronic access (swipe) to the University facilities, as determined by the designated authority.

iii. In the event of a crisis on the University Campus, the designated authority shall implement, through the University Security Division, an emergency lockdown of specific areas, an entire campus, or all University-controlled facilities.

26.0 Confidential waste

Confidential waste collection and disposal is in place at the University. The sacks must be filled following the prescription by the University Environmental Services Unit. It is the responsibility of the department/section requesting disposal to ensure confidential material is secured at all times until collected.

27.0 Health Safety and Environment (HSE)

27.1 Objective of HSE

Health, Safety, and Environment deals with occupational health and safety rules and regulations. This includes environmental protection from natural hazards.

Objectives of HSE include:

● Prevention of all incidents and accidents that can result from abnormal operating conditions;

and

- Reduction of adverse effects that may result from normal operating conditions.

27.2 Safety Culture

A Safety Culture is created when the University sees the value of a safe work environment. To this end, the promotion of a Strong Safety Culture shall be sustained in the University environment. This safety culture includes:

- Perception of safety as a core value;

- Strong Leadership;

- Establishment and enforcement of high standards of expectations and performance;

- The involvement of all staff and students;

- Effective communication and commonly understood and agreed-upon goals;

- Good organisational learning and responsiveness to change; and

- Provision of timely responses to safety issues and concerns.

27.3 Safety Signs

Safety signs give general instructions and suggestions about safety measures. The University shall ensure that appropriate safety signs are mounted at designated places.

28.0 Handling Bomb and Suspect Material

Any member of staff or student who receives a suspicious package should not open the package, but immediately call the Security Division, who will also liaise with the Bomb Disposal Unit of the Nigeria Police Force. Members of staff, students, and visitors are encouraged to report any suspicious items such as bags left unattended to security. Security will respond to all calls and take appropriate action.

29.0 Collaboration with Relevant Stakeholders

The University of Ilorin shall collaborate with relevant security agencies and institutions to enhance sustainable security on the campus. It will do this by:

i.   synergising with relevant conventional security outfits and sister institutions to improve campus security and share inter-campus security experiences;

ii.   collaborating with the leadership of the host communities to improve campus security and

improve town-and-gown relationships;

iii.   paying regular visits, dialogue, and consultations with the University's immediate neighbours to improve campus security;

iv.   having regular joint campus sub-sector security committee meetings, and

v.   joining inter-university campus security associations and relevant online platforms.

30.0 Policy Review

This policy shall be reviewed periodically to ensure it:

i. remains fit for purpose and accuracy;

ii. reflects changes in technologies.

iii. is aligned with industry's best practices; and

iv. supports continued regulatory, contractual, and legal compliance.

31.0 Policy Violations

This policy shall be applicable to all persons who operate or are within the territories or any of the campuses or facilities belonging to this University. Violators of this policy shall be made to face the appropriate disciplinary actions in line with the extant University regulations.