SECURITY POLICY

Title:	**SP**
Management Policy Number:	**SS01/01/17**
Compiled by:	**Chief Security Officer**
Approved by:	

Contents page

Foreword by the Vice-Chancellor

Lupane State University is committed to the security of its staff, students and visitors through the establishment of reasonable practices that support a secure teaching, learning, working and living environment. This document therefore, serves as a statement about the institution's commitment to security and explains how the institution intends to protect its community and its assets by illuminating the objective of Security Section, personal security, security of buildings and property among other things. The main objective of this document is to provide a security framework that minimises the University's exposure to all levels of security risk where personal and property security are potentially compromised.

In order for Lupane State University to be secure it is, therefore, incumbent upon its community to ensure that this policy is adhered to.

Professor Pardon K. Kuipa

Vice-Chancellor

Definition of Terms

University - refers to Lupane State University

University Community - refers to Lupane State University employees, students, visitors and contractors.

University Property - refers to any property owned by the University or any property that is used for University business. It includes moveable and immovable objects as well as land.

Visitor - refers to a person who is not a member of staff or student who has been lawfully granted access to the University premises.

Contractor - refers to a person who is not a member of staff or student who lawfully provides labour or performs a service within the University.

Restricted Area- refers to any area of the University which unauthorised people are not allowed to enter and is only accessible to authorised person.

1. Purpose

The purpose of this policy is to define procedures and responsibilities for maintaining security of Lupane State University and protecting the University's property and assets under University employees' control.

2. Application

This policy covers the role and responsibilities of Lupane State University Security Section as well as physical security in relation to the University community and University property and assets. The policy does not cover security of property and assets that are not owned or controlled by Lupane State University.

3. Scope

This policy determines the roles and responsibilities and the requirements for the following:

i. Security Section
ii. Personal security
iii. Security of Perimeter Boundary and Buildings
iv. Security of Property
v. Identification of staff, students and visitors
vi. Control of keys
vii. Incident Reporting
viii. Monitoring and evaluation of Security Policy
ix. Review of Security Policy

4. University Security Section

Lupane State University employs its own security staff who enforce law and order on all University premises and work closely with the external security agencies. The Section has the primary responsibility for crime prevention, law enforcement, parking control, emergency preparedness, response and security at special events.

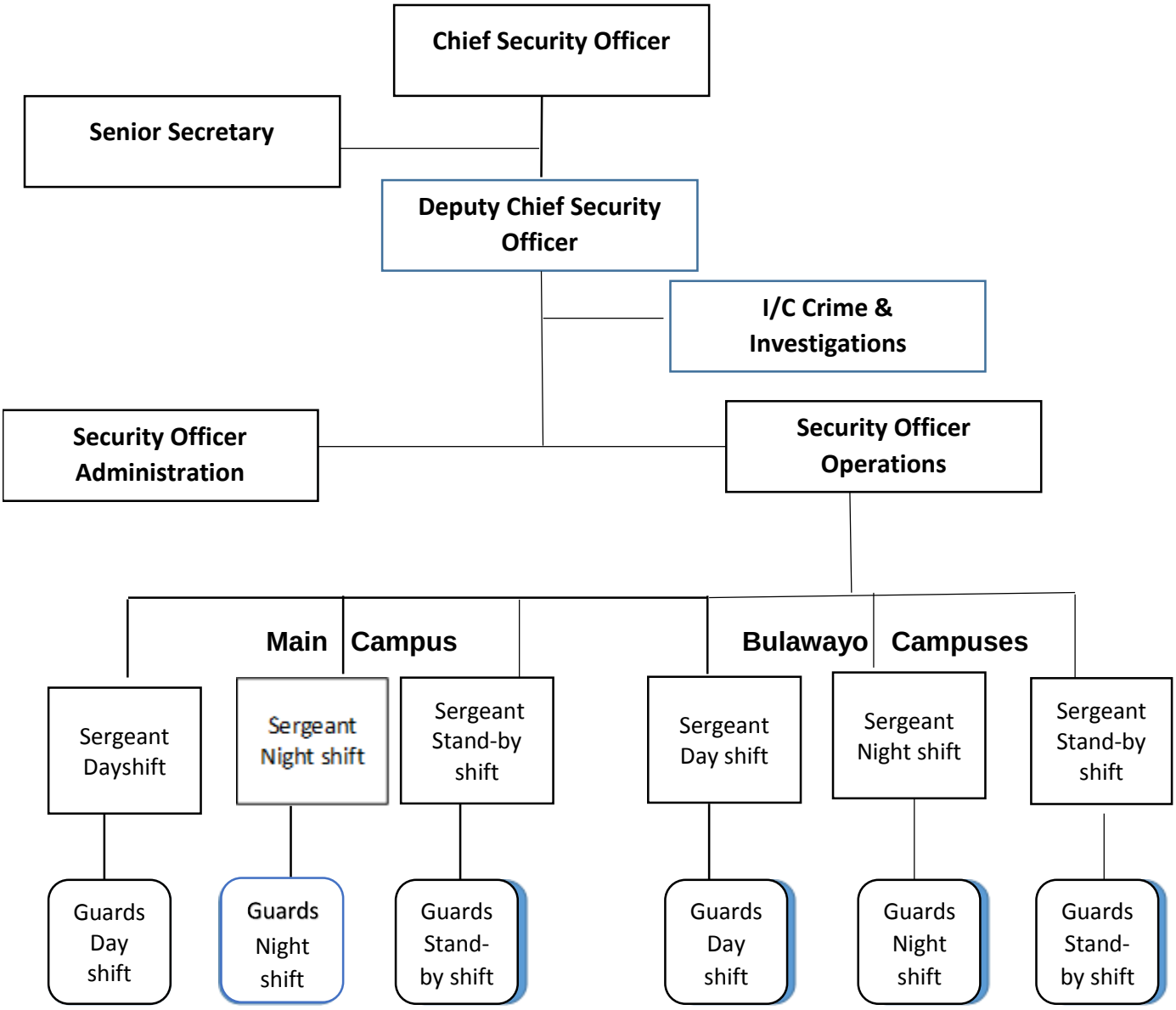
4.1 Purpose of Security Section

The purpose of the Lupane State University Security Section (Campus Security) is to protect facilities and personnel and support learning and teaching activities at the University.

4.2 Objective of Security Section

The main objective of the Section is to contribute to the achievement of the University's stated mission. This is through its commitment to the development and retention of a safe and secure working environment to enable academic life to thrive.

4.3 Security Section Structure



NB: Number of guards shall be determined by the nature of premises to be guarded.

4.4 Authority of Security Staff

Although members of the Security Section do not have police powers to arrest offenders they are however empowered by the Part V, sections 27, 29 and 30 of the Criminal Procedure and Evidence Act [Chapter 9:07] to arrest any person for certain offences committed within University premises.

Once an arrest has been made the offender shall, without any unnecessary delay, be handed over to the Chief Security Officer or any other senior member of the Security Section present.

The Chief Security Officer shall, depending on the nature of misconduct or offence, direct that the offender be either:

a. Reported to relevant University authorities.
b. Handed over to the nearest police post or station for further action.

In terms item of 2 of the Lupane State University Management Policy Number SS03/02/16 (Investigation Procedure Manual) the Security Section also has authority to investigate any incidents that occur within University premises.

4.5 Responsibilities of Security Section

The Security Section has the responsibility of developing a positive security atmosphere within the University community and to encourage a culture where this responsibility is accepted by all and the actions of those who breach security are not tolerated.

In this regard the Section shall:

4.5.1 Enforce the University security policy.
4.5.2 Protect University community and property through patrols, the use of electronic security systems and the provision of crime prevention and crime reduction awareness campaigns.
4.5.3 Deter and detect crime.
4.5.4 Employ strategies that are aimed at reducing the fear of crime.

4.5.5 Respond quickly to calls of security nature and report crimes or incidents.

4.5.6 Investigate security incidents or breaches in a fair, objective and professional manner.

4.5.7 Address security issues which impede or disrupt the operation of the academic process.

4.5.8 Develop and maintain partnerships with external security agencies and any other relevant stakeholders.

4.6 Security as a Shared Responsibility

A safe and secure environment depends on cooperation and assistance from every member of Lupane State University staff and all students.

5. Personal Security

Whilst the Security Section takes all reasonable measures to ensure safety and security the University community, staff and students shall take reasonable steps to protect themselves and their own personal belongings whilst on University property.

The Security Section shall regularly provide information to assist staff and students in protecting themselves and personal belongings.

Members of staff and students are therefore advised to read security notices and updates.

Staff and students shall discharge their security responsibilities to the best of their abilities.

6. Security of Perimeter Boundary and Buildings

The Security Section is responsible for securing the perimeter boundary of the University. It is also responsible for defining and implementing adequate security for all buildings within the University.

The Security Section shall develop and monitor the Access Control Procedures for University premises. (See Appendix A for Access Control).

At satellite campuses or premises, the respective Dean, Director, Chairperson or the most senior person at such campus or location, is responsible for securing all buildings under his/her jurisdiction.

Access to University premises shall be granted on the basis of identified need for members of the University community.

Security staff shall prevent unauthorised access to buildings and premises they are guarding in line with the relevant security procedures.

Building occupants shall prevent unauthorised access to buildings and offices under their control in line with the relevant security and access control procedures.

7. Security of Property

To prevent unathurised use, removal or damage of University property and assets building and office occupants are responsible for securing all University property under their control. Such property includes, but not limited to, furniture, records, tools, materials and vehicles.

Any person wishing to remove University property from University premises must have necessary authority and complete the Property Removal Form. (See Appendix C for Property Removal Form).

8. Identification of Staff, Students and Visitors

For identification purposes and accessing University facilities and residence halls staff and students are required to wear a lanyard with a current University identification (ID) card at all times.

Staff and students should be prepared to show their ID card when requested by security personnel or any member of University staff.

Visitors and contractors shall obtain temporary identification tags from relevant reception area upon entry to University premises. They shall display the tags at all times when they are within University premises and return them upon leaving.

9. Control of Keys

Issuing of keys for use by University staff and students shall be controlled to minimise the risk of unauthorised access into buildings.

All keys shall be managed in accordance with the Key Management Policy. (See Appendix B for Key Management Policy).

All electronic access systems that provide access to University buildings or offices shall be managed in accordance with the access control procedures.

10. Incident Reporting

All incidents of a security nature must be reported to the Security Office. This can be done either by direct contact with the office or through security staff located at various University sites.

All reports shall be recorded in the appropriate security books. To ensure easy follow-up of a report a reference number shall be given to the person making it.

11. Monitoring and Evaluation

Responsibility for monitoring and evaluation of the Security Policy lies with the University's management.

12. Custody of the policy

The Chief Security Officer is the custodian of this policy.

13. Review of Policy

This policy shall be reviewed every three years and as and when the need arises.

Appendix A

Access Control Procedures

Definition of Terms

For the purposes of these Procedures the following definitions apply:

Access - refers to permission, liberty or ability to enter, approach, or pass through Lupane State University premises and or facilities.

Access Card - refers to a specialised ID card that is programmed for use with an electronic locking system.

Authorized User - refers to any individual who has been issued a key, access card, or biometric Access to a University Facility.

Biometric Reader- refers to an electronic device used to determine a person's identity by detecting and matching the person's physical features, such as fingerprints or the eyes, to a database.

Designated Authority - refers to the person in each Faculty, Department, Centre of Excellence, building or site who has been designated to authorise and maintain access control measures for University premises and facilities within their respective areas of jurisdiction.

Disaster Management Plan - refers to systematic procedures that clearly detail courses of action aimed at mitigating events that could compromise Lupane State University's ability to function.

Electronic Access Control - refers to an electronic locking system that is activated by an access card or Biometric Reader.

Emergency Management Response Team - refers to a designated group responsible for the coordination and management of emergencies at Lupane State University.

Key - refers to a key, access card or code that operates the exterior door locks for a building.

University Property or Facilities - refers to all locations and spaces owned and/or leased by Lupane State University for the purposes of carrying out University activities.

1. Purpose

The purpose of these Procedures is to outline the process for authorising, monitoring and controlling the access to all Lupane State University premises and facilities.

2. Scope

These Procedures apply to all University staff, students and visitors.

3. General

3.1 Access to University premises and facilities will only be provided with the appropriate authorisation.

3.2 Unauthorised access to any University premises and facilities is strictly prohibited and may lead to prosecution.

3.3 Individuals are prohibited from unauthorised possession, duplication, disabling, programming or by-passing of locks and/or electronic access control systems to University premises and facilities.

4. Responsibilities and Accountabilities

4.1 The Chief Security Officer (CSO) is responsible for access control measures for all University premises and facilities. The CSO shall advise and make recommendations to Faculties, Departments, Centres of Excellence and all premises regarding the development and maintenance of access control measures for their respective premises.

4.2 The Director, Physical Planning, Works and Estates (P P W & E), is responsible for administering, controlling, production, distribution and return of keys.

4.3 The Director P P W & E is the only person authorised to approve the installation, management and maintenance of locks and electronic access control systems for all University premises and facilities.

4.4 All requests for keys must have the approval of the Director, P P W & E prior to being issued.

4.5 The Head of each Faculty, Department or Centre of Excellence will appoint a Designated Authority for their respective areas. This person will act in

consultation with the Director P P W & E and in accordance with University Access Control Procedures requirements.

4.6 In the event of an emergency, safety and protection of life will take precedence. In such circumstances authority for access control to all University premises and facilities will be transferred to the University Emergency Management Response Team (EMRT) or the individual in charge of the EMRT, as set out in the University's Disaster Management Plan (DMP).

5. **Keys**

5.1 Only one key will be issued to the authorised user for a specific lock or electronic access control system.

5.2 Once a key is issued to the authorised user, it is not transferable and may not be duplicated.

5.3 The authorised user is responsible for the security of the key issued to him/her.

5.4 Access cards or codes will be issued to authorised users for doors where an electronic access control is installed.

5.5 All keys issued for University premises and facilities remain the property of the University and must be surrendered upon request by relevant authority or returned when no longer needed.

6. Lost keys or access cards

6.1 Individuals possessing keys to University premises and facilities are responsible for such keys.

6.2 If an individual loses a key or it is stolen, the individual must report this immediately to his/her Head of Department/Section.

6.3 A replacement key may be issued after completion of the Key Request Form (Appendix B-1).

Appendix B

Key Management Policy

Definition of terms

Key - refers to any device used to grant or deny access. For this Procedure the word “key” shall refer to electronic and mechanical devices including burglar alarm access codes.

Key Control - refers to any method or procedure which limits unauthorised acquisition of a key and/or controls distribution of authorised keys. It also refers to a systematic organisation of keys and key records.

Key Control Authority (KCA) - refers to an individual or a group having the responsibility and jurisdiction for creating, enforcing and administering all key control procedures.

Multiple Key holder - refers to an individual authorised to be issued bulk keys.

1. Purpose

The purpose of this Key Management Policy is to help protect life, property and enhance security of Lupane State University.

It serves as the framework by which all keys will be managed, issued, duplicated, stored, controlled, returned, replaced and accounted for.

This policy shall apply to all keys for offices, equipment, lecture rooms, storerooms, gates, vehicles, safes or any facility owned, operated or controlled by Lupane State University.

This policy seeks to establish authority on key control, a recorded chain of possession of all keys and key issuance authority.

2. Control of keys

2.1 The University shall appoint a Key Control Authority (KCA) to implement, execute and enforce key control procedures

2.2 All keys shall be stored in a secured locked cabinet.

2.3 All keys shall remain the property of Lupane State University. Keys shall be issued only to individuals who have a legitimate and official requirement for them.

2.4 Those issued with keys shall only use their keys to access their assigned areas and should lock doors whenever they leave.

2.5 Those issued with keys must ensure that keys are safeguarded at all times

2.6 Keys that are no longer required for authorized purposes shall be returned to the KCA.

2.7 No person shall knowingly receive, borrow or possess any key for any offices, equipment, lecture rooms, storerooms, gates, vehicles, safes or any facility owned, operated or controlled by the University without receiving permission from a person duly authorized to give permission to possess such key.

2.8 No person shall knowingly alter, duplicate or copy any key without receiving permission from the KCA.

2.9 Key holders shall not loan any keys issued to them.

2.10 Key holders shall not use their key(s) to grant access to non-authorised individuals.

2.11 Lost keys shall be reported immediately to the KCA.

2.12 It shall be the University policy that when keys are lost or stolen, to change immediately any lock accessed by the lost keys.

2.13 Only a University-approved locksmith shall be permitted to cut keys.

2.14 Installation of locks and locking systems or devises shall only be performed by University approved locksmith or technician.

2.15 Any employee who violates this policy may be subject to disciplinary action.

Appendix B-1

Lupane State University

Building Communities through Knowledge

Key Replacement Request Form

Key holder's name:	**EC Number:**
Department/Section:	**Title:**
Extension:	
Key Requested: *Please provide specific room or office for which key is requested.*	
Justification for issuance of key	
Issue of key authorised by	
The key noted above has been issued to the key holder by	

Key holder signature _____ **Date** _____

Distribution

Copy Head of Department/Section ☐

Copy Security Office ☐

Copy Department of Physical Planning, Works and Estates ☐

Appendix C

LUPANE STATE UNIVERSITY

APPLICATION FOR REMOVAL OF UNIVERSITY EQUIPMENT
(Complete 3 back to back copies)

1. **FACULTY**----------
   (Where applicable)
2. **DEPARTMENT**---------- ----------**OFFICE NUMBER** ----------

3. **FULL NAMES OF APPLICANT**----------
4. **EMPLOYEE STAFF NUMBER** ----------
5. **APPLICANT'S TELEPHONE NUMBER** ----------

SIGNATURE----------

6. **LIST OF EQUIPMENT TO BE MOVED**

ITEM NAME	QUANTITY	MAKE / TYPE / MODEL	SERIAL/ ASSET NUMBER	ITEMS SEEN AND DECLARE OUT *Security check point (Tick)*

Attach appendix where applicable

7. **PLACE WHERE EQUIPMENT IS TO BE MOVED TO, *(PUT PHYSICAL ADDRESS)***

   ----

8. **REASON** ----------

9. **DATE OF MOVEMENT** / / **TIME OUT** :

10. **DATE OF RETURN *(ON OR BEFORE)*** / / **TIME IN** :

11 Security detail checking items out at exit point (gate) ----------
(Print name in full)

Date / / **Time** **Hrs**

12 EQUIPMENT RETURNED BY ---------- ----------

12.1 Actual date of equipment returned / /

12.2 Comment on state of Equipment, Working / Not Working

12.3 Other----------

/ /

NB: The following Signatories must sign in that order. ICTS Director for all Computer Equipment and Asset Register for all Assets. No Equipment will be allowed out without the Security Signature (Para 17)

---

13. CHAIRPERSON / HEAD OF DEPARTMENT
Approved / Not Approved

Signature----------Date / /
(Official Stamp)

14. DEAN OF FACULTY ***(Where applicable)***
Approved / Not Approved

Signature----------Date / /
(Official Stamp)

15. BURSAR (ASSET REGISTER)

Signature---------- Date / /
(Official Stamp)

16. DIRECTOR OF ICTS

Signature---------- Date / /
(Official Stamp)

17. CHIEF SECURITY OFFICER

Signature---------- Date / /

(Official Stamp)

DISTRIBUTION

1. Copy Chairperson or Head of Department ☐

1. Copy Chief Security Officer ☐

1. Copy Assets/ICTS ☐

Approved: _____ Date: _____