

PHYSICAL SECURITY RISK ASSESSMENT

Analysis Report



SUNRISE GUESTHOUSE

42 Acacia Avenue, Rosebank, Johannesburg

ASSESSMENT DATE	30 March 2022
-----------------	---------------

PRESENTED BY	Mfanafuthi Solutions Pty Ltd
--------------	------------------------------

ADDRESS	947 Texas Crescent Cosmo City Ext O
---------	-------------------------------------

PREPARED BY	Glen M D Mhone
-------------	----------------

Table of Contents

- 1. Introduction**
- 2. Project Scope & Background**
 - Purpose
 - Approach/Legislative Scope
 - Disclaimer
- 3. Checklist Compliance Summary**
 - Compliance Overview
 - Flagged Items
- 4. Security Risk Assessment**
 - Risk Summary
 - Community Assessment (Threats / Support)
 - Perimeter Fencing
 - Access Control
 - Buildings
 - Perimeter Lighting
 - Firefighting
 - Brief OHS
 - Security Systems (CCTV/Motion sensors/Alarms etc.)
 - Various Areas of Concern
- 5. Strategic Deployment Recommendations and Plans**
- 6. Conclusion**
- 7. References**

Introduction

Mfanafuthi Solutions Pty Ltd greatly appreciates the opportunity to submit a Security Risk Assessment and Deployment plan for Sunrise Guesthouse conducted on 30 March 2022 by our Risk & Investigations Teams led by Glen M D Mhone and Tebogo Phelephe. The Risk Analysis was focused on the expert security services and deployment strategies to be provided for the protection of Sunrise Guesthouse as well as Total Control of all Health & Safety matters throughout the perimeter.

Project Scope & Background

Purpose

The purpose of the Risk Assessment and Analysis is to:

- Ascertain the level of the physical risk and the weaknesses that exist around the perimeter fence, the premises as well as infrastructure within and around the cemeteries.
- To identify risks and threats to the perimeter wall and access control gates.
- To evaluate the security measures installed at the premises and to make further recommendations for possible improvements.
- To assist in the implementation of these recommendations wherever possible.

This survey includes the comprehensive observations of all applicable Risk Management disciplines and includes the relevant recommendations that indicate what action needs to be taken to remove or bring situations mentioned under control. It is however, seen as the client's prerogative to determine all that may be practical to apply.

Risk is defined as an exposure to the chance of any hazardous or criminal circumstances "A source of, or exposure to danger, injury or loss".

Approach/ Legislative Scope

The approach we adopted maybe summarized as follows:

- An assessment of the physical infrastructure and security systems surrounding the entire premises and a full review of the operational strategies currently implemented by the security service provider.
- Assessing whether adequate policies and procedures exist with regards to the provision of security services and whether there is clearly defined responsibilities and accountability.
- Drafting of a risk report detailing all the requisite control recommendations required to ensure that all key and material weaknesses identified are addressed.
- Implementing recommendations with the assistance and agreement of Sunrise Guesthouse.

The level and quality of the security services proposed are in accordance with the set standards required by the Private Security Industrial Regulatory Authority (PSIRA). We will take all possible steps to ensure the legislative compliance of the Security Officers Act 92 of 1987, these steps include, inter alia, the following:

- The protection of Sunrise Guesthouse as well as the protection of the said property, infrastructure, assets, perimeter fence, adjacent buildings and vehicles against theft, robberies, trespassing, terrorism, fire, espionage, vandalism, sabotage with appropriate access management and control measure clearly defined.
- The protection and safety of Sunrise Guesthouse Visitors against injuries, violence, robberies, theft of personal property, death including other offences referred to in Schedule 1 of the Criminal Procedure Act of 1977, (Act 51 of 1977).

Disclaimer

Any action taken by the recipient of this report or by his/her representatives based upon this security assessment does not guarantee or warrant in any way whatsoever that the assessed location/s, facility, its users or visitors may or may not be rendered safer, invulnerable or in any fashion impervious to successful penetration, attack or other acts which could cause property damage and/or personal injury to the facility or its patrons. By accepting this security assessment report, and or avoiding to take any action based on its written or verbal content Sunrise Guesthouse hereby agrees to **RELEASE, WAIVE, DISCHARGE, HOLD HARMLESS and NOT SUE** Mfanafuthi Solutions Pty Ltd, any of its partners, associates, officers and or employees, for any and all loss, harm, liability or damage caused as a consequence of the security assessment, release of the written report, pictures and assessors opinions including any loss arising from a claim of negligence. Further, by accepting this report, Sunrise Guesthouse agrees to **INDEMNIFY** Mfanafuthi Solutions Pty Ltd, its partners, associates, its agents, officers and employees from any loss, harm, liability, lawsuits, damages or costs including court costs and attorney fees.

Checklist Compliance Summary

COMPLIANCE OVERVIEW

A structured checklist audit was conducted across **7** of **9** assessed areas, covering **55** inspection items. Overall compliance stands at **60%** (30 of 50 applicable items passed), with 5 items marked not applicable. **2** areas were not audited via checklist.

Compliance % is calculated from Yes and No responses only; items marked N/A are excluded from the score.

AREA	YES,	NO	N/A	COMPLIANCE
Social & Environmental Threats and/or Support	6	5	3	55%
Access Control	4	4	0	50%
Perimeter fencing or walling	3	5	2	38%
Buildings - Infrastructure	4	1	0	80%
Lighting Systems	5	0	0	100%
Technical Security Systems (CCTV, PIDS, Guard Patrol, Alarms.)	7	5	0	58%
Fire Protection	1	0	0	100%
OHS Assessment	Not Audited			—
Various Areas of concern	Not Audited			—

FLAGGED ITEMS

SOCIAL & ENVIRONMENTAL THREATS AND/OR SUPPORT

1. Is there any available footage of the incident?
2. Are there contingency plans in place for natural disasters or other large-scale community events that could impact security?
3. Are there existing partnerships or collaborative agreements with other local security companies to share resources and intelligence on security threats?
4. Is the facility located in a statistically high-risk area for specific threats (e.g., theft, vandalism, violent crime, terrorism)?
5. Are there informal settlements or areas of dense, unregulated housing near the facility?

ACCESS CONTROL

1. Is there a documented procedure for access control?
2. Are search procedures for packages and vehicles being followed?
3. Are Security Officers deployed for access control during the dayshift? If yes, indicate the total number deployed.
4. Is the current deployment sufficient to cover access control, patrols, incident response, monitoring of surveillance systems, and other essential security functions?

PERIMETER FENCING OR WALLING

1. Are perimeter doors, gates, and docks secured and in good working condition?
2. Are all perimeter fences and barriers made of materials that prevent easy tampering or breaching?
3. Are there detection systems (e.g., motion sensors or pressure-sensitive devices) along the perimeter to alert security of unauthorized activity?
4. Are there measures in place to deter or detect attempts to climb, cut, or bypass perimeter security?
5. Is the perimeter regularly surveyed for environmental changes (e.g., fallen trees, erosion) that could compromise security?

BUILDINGS - INFRASTRUCTURE

1. Are there existing building access systems, such as card readers and biometric scanners, if yes are they regularly tested and updated for security and how frequently?

TECHNICAL SECURITY SYSTEMS (CCTV, PIDS, GUARD PATROL, ALARMS.)

1. Are surveillance cameras installed with adequate coverage?
2. Is there a backup power system to keep surveillance and alarm systems operational during power failures?
3. Are there policies and procedures for handling and reviewing video footage in case of an incident or investigation?
4. Is there a designated clocking point for security personnel to check in and out at the start and end of their shifts?
5. Are there backup systems or protocols in place if a clocking point fails (e.g., malfunctioning equipment)?

C O N F I D E N T I A L



Security Risk Assessment

RISK SUMMARY

This assessment identified **27** vulnerabilities across **9** assessed areas. 2 critical, 8 high, 7 medium, 2 low, and 8 requiring severity classification. The highest concentration of risk was identified in **Access Control**. Immediate remediation is required for 2 critical vulnerabilities identified.

SEVERITY DISTRIBUTION



RISK BY AREA (C = CRITICAL H = HIGH M = MEDIUM L = LOW U = UNRATED)

AREA	C	H	M	L	U
Social & Environmental Thr..	1	.	3	1	.
Access Control	1	3	1	.	.
Perimeter fencing or walling	.	4	.	.	.
Buildings - Infrastructure	.	1	2	.	.
Lighting Systems	.	.	1	.	.
Technical Security Systems	.	.	.	1	1
Fire Protection	.	.	.	.	3
OHS Assessment	.	.	.	.	2
Various Areas of concern	.	.	.	.	2

Social & Environmental Threats and/or Support

AUDIT

#	INSPECTION ELEMENT	YES	NO	N/A	COMMENT
1	Are there neighborhood or building-related risks that could increase security threats?	✓			
2	Is there an established relationship with local law enforcement to facilitate rapid response in case of a security breach?	✓			
3	Is the any available footage of the incident?		✓		

#	INSPECTION ELEMENT	YES	NO	N/A	COMMENT
4	Are there community-based initiatives, such as neighborhood watch programs, that collaborate with your security efforts?	✓			
5	Are there contingency plans in place for natural disasters or other large-scale community events that could impact security?		✓		
6	Are there any socio-economic or political factors in the local community that might increase the likelihood of security threats (e.g., protests, high unemployment, or civil unrest)?	✓			
7	Are there existing partnerships or collaborative agreements with other local security companies to share resources and intelligence on security threats?		✓		
8	Are there available crime statistics that indicate a higher-than-average risk in the surrounding area (e.g., increased burglary, violent crime, vandalism)?	✓			
9	Is the facility located in a statistically high-risk area for specific threats (e.g., theft, vandalism, violent crime, terrorism)?		✓		
10	Does the facility regularly review crime statistics and adjust security measures based on emerging threats or trends?	✓			
11	Are there informal settlements or areas of dense, unregulated housing near the facility?		✓		
12	Are informal settlements involved in any criminal activities that could potentially spill over into the facility's security perimeter (e.g., gangs, illegal activities)?			✓	
13	Are there specific security measures in place to monitor or control access points that could be impacted by informal settlements (e.g., increased foot traffic, unauthorized entry)?			✓	
14	Are there proactive security measures in place to prevent crime spillover from neighboring facilities or surrounding areas, such as increased perimeter patrols and surveillance?			✓	

Security Vulnerability Assessment

1. Inadequate Crime Support.

The site is situated far from law enforcement agencies.

2. High-Risk Area.

Informal settlement identified in close proximity to the site.

3. High-Risk Area.

The site is situated in a High-Risk area.

4. Lack of Community Policing.

There are no community policing forums in the area.

5. Inadequate emergency support.

The site is situated in a remote area and is far from healthcare facilities.

VULNERABILITIES

1. Law enforcement agencies L

Law enforcement agencies e.g. SAPS are the most crucial support system to any site and the distance between the site and the nearest police station has a direct impact on the response time & any meaningful effect on the likelihood of delaying, denying, deterring, or catching/apprehending offenders.

2. Increase in crime states M

Current crime stats have increased on scrap metal theft and the close proximity of an informal settlement with scrap metal traders is a direct threat to the site. The site's infrastructure and assets are at the risk of sabotage, vandalism, and theft.

3. Infrastructure C

Infrastructure, assets, perimeter fencing, adjacent buildings and vehicles are subject to the risk of potential theft, trespassing, vandalism, and sabotage. Visitors and tenants are subject to the risk of potential injuries, violence, robberies, theft of personal property, and death.

4. potential risk of an increase in crime M

There is the potential risk of an increase in crime in communities which includes illegal drugs, gang violence, muggings, and burglaries.

5. difficulty in seeking help M

If an incident were to occur while working in a remote area, employees may have great difficulty in seeking help and getting the emergency response they need. This may potentially exacerbate injuries, the medical condition they are in, or may ultimately result in potential death.

RECOMMENDATIONS

1. The current security service provider must formally engage other stakeholders located in close proximity to the site to understand crime trends in the area. If possible, all stakeholders involved may form relationships that ensure a collaborative approach to fighting crime within the community.
2. Intensified patrols around the site to deter metal traders from sabotaging, vandalizing or stealing site infrastructure.
3. Intensified patrols around the site to deter metal traders from sabotaging, vandalizing or stealing site infrastructure.
4. The current security service provider must formally engage other stakeholders located in close proximity to the site to understand crime trends in the area. If possible, all stakeholders involved may form relationships that ensure a collaborative approach to fighting crime within the community.
5. Management should supply small first aid kits and advise staff to carry the kits with them at all times. These can be used to treat minor injuries and potentially buy time till emergency services arrive.

Access Control



AUDIT

#	INSPECTION ELEMENT	YES	NO	N/A	COMMENT
1	Is facility access controlled with restricted entry points?	✓			
2	Is there a documented procedure for access control?		✓		
3	Are visitors and contractors properly screened, signed in and out, and required to present identification?	✓			
4	Are search procedures for packages and vehicles being followed?		✓		
5	Is there a list of approved contractors/vendors, and is it regularly updated?	✓			
6	Are Security Officers deployed for access control during the dayshift? If yes, indicate the total number deployed.		✓		

#	INSPECTION ELEMENT	YES	NO	N/A	COMMENT
7	Does the facility operate 24/7? If yes, are Security Officers deployed for access control during the nightshift? Indicate the total number deployed if applicable.	✓			
8	Is the current deployment sufficient to cover access control, patrols, incident response, monitoring of surveillance systems, and other essential security functions?		✓		

Security Vulnerability Assessment

1. Access Control & Management Compromised.

Entry and point left open and unmonitored.

2. Compromised Locking System.

Padlocks and chains have succumbed to rust.

3. Insufficient personnel posting.

There is Insufficient security personnel at access entry and exit points to regulate and manage access control.

4. Deficient Gate.

Access control gate cannot be secured due to physical damage/ wear and tear.

5. Deficient Access control.

Access control procedures and protocols are not being observed. Security personnel are not identifying visitors on entry

VULNERABILITIES

1. Access control and management is compromised M

Access control and management is compromised and rendered purposeless when there are gates that are left unlocked and unmonitored as criminals can access the site from various points undetected.

2. can be easily breached H

Padlocks, gate latches, and chains that have succumbed to erosive elements causing them to rust can be easily breached.

3. potential risk of unauthorized access H

There is the potential risk of unauthorized access to regulated areas within the site with no identification of perpetrators being captured.

4. access control cannot be managed H

The gate cannot be secured therefore access control cannot be managed efficiently which may lead to the risk of intrusion.

5. unauthorized access to regulated areas C

There is the potential risk of unauthorized access to regulated areas within the site with no identification of perpetrators being captured.

RECOMMENDATIONS

1. The security service provider must ensure security officers are trained on proper access control procedures &/or protocol. Gates that are not in use should always be kept closed and locked.
2. All compromised locking systems must be repaired or replaced. Security management must conduct regular checks on padlocks and chains to ensure their structural integrity is not compromised.
3. Deployment of additional security personnel on all access points.
4. The security service provider must ensure security officers are trained on proper access control procedures &/or protocol. Gates that are not in use should always be kept closed and locked.
5. Management to deploy identity scanners at main access points to ensure the genuine capturing of identification and vehicle registration.

Perimeter fencing or walling



AUDIT

#	INSPECTION ELEMENT	YES	NO	N/A	COMMENT
1	Is there adequate perimeter protection, such as fencing, barricades, and landscaping?			✓	

#	INSPECTION ELEMENT	YES	NO	N/A	COMMENT
2	Are physical barriers used to restrict vehicle access to the building?			✓	
3	Are perimeter doors, gates, and docks secured and in good working condition?		✓		
4	Are regular patrols conducted along the perimeter to inspect for damage and security breaches?	✓			
5	Are guard dogs or other security measures utilized along the perimeter?	✓			
6	Are all perimeter fences and barriers made of materials that prevent easy tampering or breaching?		✓		
7	Are there detection systems (e.g., motion sensors or pressure-sensitive devices) along the perimeter to alert security of unauthorized activity?		✓		
8	Is there regular maintenance on fencing and physical barriers to ensure their integrity over time?	✓			
9	Are there measures in place to deter or detect attempts to climb, cut, or bypass perimeter security?		✓		
10	Is the perimeter regularly surveyed for environmental changes (e.g., fallen trees, erosion) that could compromise security?		✓		

Security Vulnerability Assessment

1. Deficient Perimeter Fencing.

There is no security fence top-guard e.g. razor wire, electrical fences, spikes, etc.

2. Deficient Perimeter Fencing.

The perimeter fence is compromised. Breaches were recorded along the fence.

3. Deficient perimeter Fencing.

Perimeter fencing is short and easily scalable.

4. Deficient perimeter fencing.

Perimeter fencing is insufficient to deter potential intrusions. it can easily be cut with pliers

VULNERABILITIES

1. Unauthorized access H

A perimeter fence that has no top-guard may easily be scalable presenting intruders with the opportunity of gaining access into the site by jumping over the fence.

2. Breaches H

Criminals can use open spaces or breaches in the fence to enter or exit the premises without being detected or identified.

3. Potential intrusion H

Potential intruders will attempt to climb over the fence to access the internal perimeter of the site.

4. intrusions, theft sabotage and vandalism of property. H

There is the potential risk of intrusions, theft sabotage and vandalism of property.

RECOMMENDATIONS

1. The Installation of circular razor fence/electrical fencing, spikes can delay, deter, or deny intruders from unlawfully accessing the internal perimeter of the site.
2. Management to repair/ close all gaps along the Perimeter to reduce opportunities for intrusion.
3. Management to replace the perimeter fence with a taller solid structure that may not be easy to scale over.
4. Management to replace existing perimeter fence with a more solid structure e.g. Brick Wall

Reference: A guide to security. Ch-6 pg. 68

Buildings - Infrastructure



AUDIT

#	INSPECTION ELEMENT	YES	NO	N/A	COMMENT
1	Are multiple layers of protection implemented to secure core assets and sensitive areas?	✓			
2	Are critical assets safeguarded and monitored with controlled access?	✓			
3	Is the reception/security desk positioned to monitor all entrances?	✓			
4	Are there existing building access systems, such as card readers and biometric scanners, if yes are they regularly tested and updated for security and how frequently?		✓		
5	Are there security officers positioned at high-traffic or vulnerable internal points to monitor movement within the building?	✓			

Security Vulnerability Assessment

1. Building Unsecure.

Building windows are not burglar proofed.

2. Building Unsecure.

Building doors are not burglar proofed.

3. Building Compromised.

The building is old and dilapidated.

VULNERABILITIES

1. probability of a successful break-in H

Buildings that have windows and doors that are not burglar-proofed increase the probability of a successful break-in as they present criminals with an opportunity to gain access into the internal perimeter of the building exposing assets to the risk of theft.

2. probability of a successful break-in M

Buildings that have windows and doors that are not burglar-proofed increase the probability of a successful break-in as they present criminals with an opportunity to gain access into the internal perimeter of the building exposing assets to the risk of theft.

3. potential mass damage to property and assets M

Buildings that have their integral structure compromised may collapse and they may be potential mass damage to property and assets. There is also the risk of injuries to visitors and tenants or potential loss of life.

RECOMMENDATIONS

1. Management must burglar-proof all windows and doors as an added security measure.
2. Management must burglar-proof all windows and doors as an added security measure.
3. Management must burglar-proof all windows and doors as an added security measure.

Lighting Systems



AUDIT

#	INSPECTION ELEMENT	YES	NO	N/A	COMMENT
1	Is perimeter lighting sufficient for security purposes?	✓			
2	Is the lighting adequate for effective surveillance camera operation?	✓			
3	Are lights monitored for malfunctions, and is there a quick response team to repair lighting issues?	✓			
4	Is lighting designed to minimize shadows or dark spots that could provide cover for criminal activity?	✓			
5	Is there an energy-efficient lighting strategy in place to maintain security without unnecessary energy waste?	✓			

Security Vulnerability Assessment

1. Insufficient Lighting.

The current lighting is insufficient to cover the building area effectively.

VULNERABILITIES

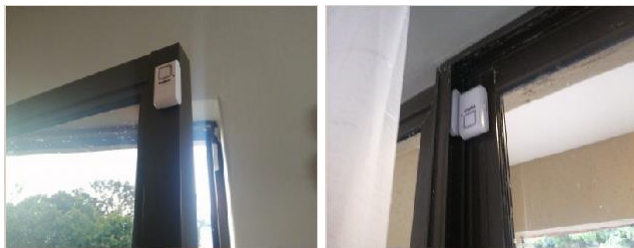
1. Hiding spots M

Insufficient lighting around buildings may create hiding spots for intruders.

RECOMMENDATIONS

- Additional lighting to be installed on building walls to ensure the building area is covered effectively

Technical Security Systems (CCTV, PIDS, Guard Patrol, Alarms.)



AUDIT

#	INSPECTION ELEMENT	YES	NO	N/A	COMMENT
1	Are surveillance cameras installed with adequate coverage?		✓		
2	Are perimeter alarms in place with sufficient coverage?	✓			
3	Are video surveillance records properly archived and easily accessible?	✓			
4	Are cameras and alarms regularly inspected and tested to ensure proper functionality?	✓			
5	Are video surveillance cameras monitored in real-time or only recorded for review later?	✓			
6	Are surveillance systems integrated with alarm systems for automated alerts in case of suspicious activity?	✓			

#	INSPECTION ELEMENT	YES	NO	N/A	COMMENT
7	Are the camera systems placed in strategic areas to monitor both the interior and exterior of the building effectively?	✓			
8	Is there a backup power system to keep surveillance and alarm systems operational during power failures?		✓		
9	Are there policies and procedures for handling and reviewing video footage in case of an incident or investigation?		✓		
10	Is there a designated clocking point for security personnel to check in and out at the start and end of their shifts?		✓		
11	Are clocking points regularly monitored to ensure compliance with scheduled patrols or shifts?	✓			
12	Are there backup systems or protocols in place if a clocking point fails (e.g., malfunctioning equipment)?		✓		

Security Vulnerability Assessment

1. Deficient Alarm Systems.

Inactive alarms identified on site

2. No CCTV System.

No CCTV cameras identified onsite.

VULNERABILITIES

1. potential mass damage to property and assets L

Inactive alarms are a security risk as they present criminals with an opportunity to access buildings' internal perimeters undetected. Security service provider will not be able to respond to incidents as they happen

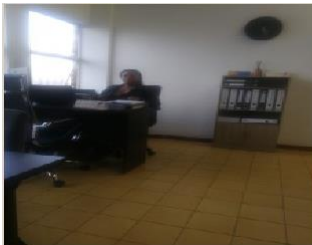
- The absence of CCTV cameras will not enable management to pick up visual illicit activities in unsupervised or physically monitored areas. Management may also be unable to conduct post-incident investigations of incidents that may happen on-site.

RECOMMENDATIONS

- Management to consider an assessment of all alarm systems with occasional testing to verify functionality. Alarm audio needs to be loud for officers on duty to respond.

2. Management to consider installing cameras to monitor activities on-site with a 24/hr. offsite monitoring strategy. This will enable CCTV Controllers to pick up any illicit activities taking place. An independent service provider should be contracted to monitor CCTV cameras on-site as this may:
 - Ensure there is no staff Intimidation.
 - Limit CCTV controller physical interaction with security personnel or staff members on-site hence eliminating the possibility of collusion.
 - Ensure cloud recording of events (all events are securely off-site in case the recorders are damaged or stolen).
 - Result in quick emergency activation in event of armed robberies. With on-site monitoring perpetrators may target the control room first to disable all communication cutting off the site from its support systems such as the police and response/reaction teams.

Fire Protection



AUDIT

#	INSPECTION ELEMENT	YES	NO	N/A	COMMENT
1	Are fire extinguishers easily visible and accessible within the facility?	✓			

Security Vulnerability Assessment

1. **No Firefighting Equipment.**
The site has no firefighting equipment sufficient to cover the site effectively from a fire outbreak.
2. **Compromised Firefighting Equipment.**
Firefighting equipment has not been serviced.
3. **Equipment Misuse.**
firefighting equipment is being used for other uses other than its intended use.

VULNERABILITIES

1. Potential mass damage to property if there is no equipment to contain a fire outbreak in its early stages.
2. Firefighting equipment may malfunction during a fire outbreak resulting in potential mass damage to property or injuries and potential loss of life.

3. Firefighting equipment misuse may result in the equipment malfunctioning in the event of a fire outbreak resulting in the risk of potential mass damage to property or injuries and/or potential loss of life.

RECOMMENDATIONS

1. Management must deploy firefighting equipment on-site to reduce the risk of massive damage to property and potential injuries or death of visitors, staff and contractors etc.
2. Management must ensure that firefighting equipment is serviced annually and all equipment has not been tampered with.
3. Management must ensure employees do not misuse the equipment and furthermore caution and educate employees on the disadvantages of misusing equipment.

OHS Assessment



Security Vulnerability Assessment

1. **Insufficient OHS Signage.**
No clearly visible and unobstructed assembly point identified.
2. **Locked Emergency Equipment.**
Locked first aid kit recorded on site.

VULNERABILITIES

1. The absence of a clearly marked visible assembly point may hinder the process of a proper headcount during a fire or an emergency as tenants or visitors to the site may not be familiar with its positioning.
2. Locked first aid kits in an emergency situation are as good as empty ones. Staff may lock the box to protect its contents from being stolen but this may result in complications during emergencies.

RECOMMENDATIONS

1. A clearly marked and unobstructed assembly point must be installed on-site and must be visible to all staff and visitors who enter the site.

2. Tamper seals may be used to secure first aid boxes as they are easily breakable and can show if the contents of the kit have been tampered with.

Various Areas of concern

Security Vulnerability Assessment

1. NIL

VULNERABILITIES

1. NIL

RECOMMENDATIONS

1. NIL

Strategic Deployment Recommendations and Plan

Deployment Plan

An effective physical security operational plan relies on a solid and impenetrable outer perimeter fence protection (First Line of Defense) as this allows for the deployment of available physical security officers strategically on ALL access and exit points to manage movement of assets and visitors in and out of the premises whilst recording all relevant details.

The deployment plan proposed in all areas requires urgent attention and the recommendations put forward aim to complement the current allocation of physical security. Further analysis is required to focus on training requirements of security teams at Sunrise Guesthouse as we did not evaluate their skills levels and their ability to respond high risk incidence, or their ability to conduct the day-to-day security operations in line with set procedures and protocols.

We also recommend the use of a tactical roving team in conjunction with other business security service providers in the area. This team's focus will be to respond to reported site incidents and alarm activations. This documented proposal can be made available and form part of the Site Operational Plan.

Mfanafuthi Solutions Pty Ltd further proposes the implementation of systems that will assist the physical guarding deployment which will include

- Perimeter Motion Sensor Beams, Electric Fence,
- After-Hours Motion Triggered Alarms,
- CCTV Camera systems with a motion sensor application at various high-risk areas to be monitored at an off-site Control room.

The security service delivery approach must also include the following;

- The induction of all new security personnel to Sunrise Guesthouse to ensure there are acquainted with their daily functions, duties and roles. The functions must be clearly defined and displayed in the Guardhouse wall where there are easily visible.
- Communication of a brand-new security processes and procedures to all internal security management, employees, tenants, subcontractors. It is also critical to communicate key security changes to community stakeholders, the police, surrounding security partners and the whole of local community.
- Introduction of phased security procedures, access control strategies, after-hours ops plans to the security team is a key pre- requisite.
- The proposal, initiation and implementing of a Community Policing Forum if non-existent.
- Health and Safety Training Initiatives and programs for all security personnel.
- Setting up joint patrol plans with neighboring security contractors.
- Communicating with visible signage all security procedures, trespassing laws and contravention penalties. These must be placed along the outer perimeters.
- Finally, assessment of the day-to-day operations of the guarding team.

These process recommendations may be reviewed at the discretion and request from Sunrise Guesthouse.

Recommended Deployment Posting

PROPOSED DAY SHIFT WEEKDAYS

DAY SHIFT DEPLOYMENT	
POST	GRADE
2× Reaction Officers with Vehicle	Grade B

PROPOSED NIGHT SHIFT WEEKDAYS/ WEEKENDS & PUBLIC HOLIDAYS

NIGHT SHIFT DEPLOYMENT	
POST	GRADE
1× Mobile Supervisor	Grade A+
1× Security Officer	Grade C

Conclusion

Mfanafuthi Solutions Pty Ltd appreciates the chance to be given an opportunity to provide such services as identified above. We would also appreciate the opportunity to strike a good working relationship with Sunrise Guesthouse. We would like to assure our client that our expert services would create an atmosphere of total safety and security.

The importance of security surveys and the identification of the risks which a company could be subjected to cannot be overemphasized. It may take considerable time to conduct a security survey; the end result can only be beneficial to the company and employees in the long run.

Such practice would have to be re-conducted after six months to confirm progress. Looking forward to continued communication in this regard.

SIGNED BY **Glen M D Mhone**

DATE 11 August 2026

References

1. Department of Defense United States of America - Unified Facilities Criteria (UFC) UFC 4-022-03, Security Gates and Fences, 1 October 2013