CYTOLUX
SECURITY

METHODOLOGY

CONTENTS

1. INTRODUCTION

Cytolux Security is pleased to submit its proposal for the Provision of security services. The objective of this proposal is to show case our understanding of your requirements and how Cytolux Security is well placed to offer a solution efficiently and cost effectively. We understand the importance placed by our clients on the selection of their security service provider, who can. Demonstrate a capacity for managing a high-quality, cost-effective project delivery with adequate experience in this field.

We believe our approach and credentials will clearly demonstrate key points of differentiation for Cytolux Security to deliver this service. Our deep industry knowledge and roll out experience positions Cytolux Security to confidently deliver the desired results to our clients. We plan to use a team which brings a blend of generation experience with security roll out expertise to ensure complete satisfaction. Our proposed solution will help you to attain:

- Financial and operational procedure streamlining & effectiveness.
- Real time access to information and analytics to ensure efficient, transparent decision making at the highest levels.

We look forward to work with you on this exciting project. In responding to your tender, we feel there are three key factors that differentiate Cytolux Security from the many Security Companies in the market: Cytolux Security

- Our Collaborative Business Style
- Our People and Approach
- Our Energy

Cytolux Security Operations and Test Plan starts from the premise that, notwithstanding every entity's right to safety and security, the integral attribute of existence inadvertently precipitates incidents of duality, in that these are always either pleasant or painful. The challenge therefore, is to align ingenuity, resources and personnel to best contend with these unforeseeable but conceivable safety compromising scenarios in good times and in bad times.

Our value offering, therefore is a function of an effectively synthesized, analyzed risk evaluation and optimal disbursement of resources to arrest and manage crisis eventualities in a manner that ensures unruffled business continuity. This Black Paper is therefore forever transmigrating as the boundaries of best practice and delivery excellence recede. Our clients and personnel are our most cherished and esteemed originators of this document.

2. MANAGEMENT TEAM

We have the most dynamic management team in the security industry. The team is composed of younger as well as more matured individuals. The experience in the team is broad, from individuals who have provided close protection services for the presidency to law and financial experts. We are a group of Black Professionals, dedicated to growing and developing our skills even further in the security industry. Our management team is comprised of the following critical individuals:

- Chairperson
- Operations Director
- Operations Manager

The mission of the Management Team is:

- To develop a comprehensive, dynamic, crisis management plan.
- To identify, assign and supervise personnel responsible for implementing crisis operations.
- To arrange for necessary materials and support that the plan anticipates will be needed.
- To evaluate actions needed to address unanticipated consequences of the crisis.

Our risk management is based on a "business continuity planning" model. We assess and plan potential risks in the various segments of a business unit, categorized as strategic operational compliance related. The Primary function of this model is based on:

- Reduction of operational loss
- Early detection of unlawful activities
- Reduced exposure of future risks
- Expose inadequate or foiled internal processes, people and systems
- Probability of harm being realized and the severity of the consequences.

3. INTELLIGENCE

Intelligence functions—before, during, and after an event—are critical for security. We rely on local and state intelligence resources. The State Security Agency may also assist with intelligence on dangerous persons who have threatened public officials.

INCIDENT PLANNING

We do more planning prior to accepting and executing a brief to enable ourselves to be better prepared in addressing future incidents and managing other crises. Our motto in this regard is: *Prior Planning Prevents Poor Performance*.*

Our plan therefore, includes a detailed list of standard preparations that are made before accepting and executing a brief. We also itemize specific steps to be taken in anticipation of a crisis. All our plans, Crisis preparations, Emergency activities and Security response measures are focused on three fundamental goals:

- Protecting the viability of facilities and Assets.
- Enabling uninterrupted operational continuity and where interruptions have been unavoidable, quick operational recovery.
- Providing the best support and conditions for employee functional excellence

We run your program 3 months in advance to ensure that we are aware of all guests and plan for all associated risks.

RELATIONSHIPS

As part of our relationships to ensure proper service delivery, we create and maintain relationships with the following stakeholders for a much more effective crime prevention system:

1. **SAPS:** We develop this relationship with all the local police stations around our sites to ensure that we keep up to date with current trends in the area. This information is used to draw up action plans. For instance, if a particular car is currently being stolen in the area, we can use the information to prepare our sites adequately against that particular theft. We do this around all sites.

2. **Home Affairs departments:** The departments are key in identifying individuals that pose a threat to our sites; these can be visitors themselves or learning more about associates of the risk threats.

This is done to ensure that we have full profile of all guests and their risk profiles in order to secure the sites better.

FORENSIC

Our company is committed to providing forensic services to help feed better management decision making with security related operations. Services included are:

- Business services (e.g. screening of employees)
- Business (e.g. profiling and vendor due diligence)

Forensic investigations into alleged fraud, corruption and theft, for the purposes of:

- Disciplinary proceedings
- Criminal and/or civil litigation
- Fraud awareness training
- General fraud and anti-corruption consulting
- Fraud prevention programmers
- Organizational fraud and anti-corruption awareness surveys
- Ethics Hotline Reporting Services asset tracing

VERIFICATIONS

We have specials services on offer relating to the confirmation of information relating to employees. Our service offering covers the following:

1. Employee Credit checks

2. Employee qualification checks

3. Vetting of visitors, risk and data gathering

4. STANDARD OPERATIONAL PROCEDURES TO BE FOLLOWED BY ALL SITES

OPERATIONAL RISK ANALYSIS

Our security officers are well trained to be able to deter and instill discipline at all entry points, to record sequence of events in the manner that they took place, report non- compliance by employees of the company and those that they are in cohesion with externally.

EMPLOYMENT PRACTICES AND WORKPLACE SAFETY

Occupational Health and Safety is a cross- disciplinary area concerned with protecting the safety and welfare of people engaged in work or employment. The promotion and maintenance of the highest degree of physical, mental and social well- being of workers in all occupations, the protection of workers in their employment from risks resulting from factors averse to health, the adaptation of work to officers and of each officer to his/her job.

These areas are very critical in order to achieve ultimate operational efficiency; our company is committed to abiding and enforcing the various disciplines. Empowered and healthy officers can and are capable of performing their duties to their utmost best.

WORKABILITY

Our company is committed to providing unwavering service throughout the contract term. Our Security Service is in accordance with acceptable standards of the trade industry. Non- conformity has no room in our company and such employees are not welcome to participate in our company structures.

OFFICER REPLACEMENT PROCEDURE:

Should an Employee be requested to vacate site due to non-conformance witnessed by client or its representative, such employee's services shall be terminated. At any point the client's testimony shall be construed as true and correct. The replacement officer will then be posted simultaneously to ensure un-interrupted service on site.

FACILITY SECURITY:

Our Crisis Management Plan achieves the following:

- Identify critical sites that require security and determine the degree of Safety required
- Ensure that all security and key operations personnel who will need to get to the facility have company identification and appropriate authorizations
- Detail the steps to be taken to secure critical sites, gates and equipment's against identified and envisaged threats
- Itemize and stock the supplies and equipment's (including back-up equipment’s) that will be needed to secure the facility before and during the crisis and to assist in operations meant

to assist recovery from the crisis

LOGISTICS

Cytolux Security will also ensure that personnel that remain on- site are safe, and that equipment's and communication capabilities are adequate. Our pre comprehensive pre-logistical planning preparations assist us and our employees and our contractors to swiftly and effectively undertake post crisis recovery operations.

COMMUNICATIONS

Reliable communications are important in ensuring completion of pre-crisis preparations, addressing emergencies and coordinating and conducting response operations. It is helpful, under the circumstances to make the assumption that cell phone networks will become overloaded, providing our employees and us with little or no service. Without electricity, computer-to-computer email will not be available.

Cytolux Security Operations has planned for these eventualities by making use of a generator back up system and ensuring that its employees and contractors are versed on communications expectations and procedures.

Portable Radios

Key personnel are equipped with digital hand-held Radios. We always ensure that an adequate stock of batteries is stocked. We have further established a Digital Base Station to receive reports and to respond to callouts or emergencies.

Cellphones

Having multiple cell phone providers increases the odds that one will be operational during and after a crisis. A sole source provider is likely not to be sufficient, especially if that provider is completely out of service in that area. Contact information and procedures In addition to planning for and acquiring communications devices, we have established a method and procedure of contacting our Security Executives, key personnel employees and contractors.

Periodical updating of personnel contact information

Immediately prior to an anticipated or known event, all executives and employees are requested to review and to update their personal contact information.

Preparation of paper copies of updated personnel rosters and contact information prior to each crisis event

In the eventuality of not electronically being able in an emergency to access personnel information, keeping an updated copy of personnel contact details will assist the situation.

We are further considering the usage of a "Hotline" concept where employees can call in and report their status.

In this arrangement, selected Senior Management may also call in or email the hotline to request the status on certain employees or business units.

Key Contacts

We update and distribute a list containing the relevant contact information for key corporate, governmental, community and Utilities officials.

5. STANDARD OPERATION PROCEDURES

Serviceable hand-held radios are provided at all times to enable efficient reporting and dual communication by all authorized personnel. No personal or private communication will be utilized by our officers whilst on duty as this will hamper the officer's concentration in being vigilant for the intruders.

First and Second Level supervisors make daily contact with the site representative in order to verify and handle mutual complaints or mishaps or concerns regarding the rendering of service. Hourly updates are also made with the main control room to enable corresponding OB numbers in respect of incidents and the smooth running of the site. No security Officer is allowed to do duty longer than the regulated 12 hours.

Lost and/or articles found at the site for which ownership cannot be immediately established, will be recorded in the occurrence book and handed over to the main control Centre, wherein should the owner be identified, then such items shall be handed over. No deliveries by any person shall be received by our officers, unless prior arrangement has been made with the site supervisor or management of the company and such arrangement recorded in the Occurrence Book.

SECURITY OFFICERS (GUARDS) OPERATIONS CONDUCT

1. All security personnel will report for duty, in full uniform, at least 10 (ten) minutes prior to shift commencement.

2. All officers will report on and off duty in the 'Occurrence Book'.

3. The shift supervisor will carry out an informal/formal parade and ensure the following are adhered to:

    a. All officers are in full uniform, tidy and neatly dressed;
    b. No civilian clothing is worn with the uniform; and
    c. Officers are not under the influence of alcohol and/or smell of alcohol.

4. Under no circumstances will an officer use alcohol, illegal substances and/or habit forming drugs.

5. Officers will not smoke in the presence of senior management, visitors and/or customers.
6. No friends, family and/or visitors will be entertained on the client's premises.
7. Always be friendly and polite to customers, visitors and employees.
8. All registers, books and documents will be kept clean, neat and updated per regularly per arrangements.
9. At no time will any officer interfere with machinery and/or enter restricted areas without express permission of the client.
10. Do not damage, abuse or mishandle the client's property.
11. Avoid forming close relationships with the client's employees.
12. Under no circumstances will an officer borrow money from or lend money to any of the client's employees.
13. Sleeping on duty is a dismissible offence; under no circumstances must an officer sleep on duty
14. Occupants of vehicles entering and/or leaving the premises will be saluted.
15. Ensure your hands are always clean, especially before touching anything belonging to a visitor.
16. Do not desert your post prior to being properly relieved by another uniformed officer.
17. Careful considerations must be given to any sign of un-authorized entry into the premises and stationed vehicles.
18. Vehicles parked at the premises must be inspected frequently at regular intervals
19. Patrols must not be done in the same sequence, time and route must always be rotated.
20. During patrols the Security Officer should ensure that:

    a. All outside doors to the building are closed,
    b. If there are any windows open, special attention should be given to these areas,
    c. All vehicle doors are locked, windows are properly closed, boots are locked and that the spare wheels are not missing where fitted underneath the vehicle

21. at the designated search point area:

    a. All vehicles leaving the premises must be stopped and the Security Officer must search the vehicle and ensure that the drivers of each vehicle are in possession of the vehicle keys,
    b. Ensure that no person wanders between the vehicles.

22. At the reception areas the Security Officer must ensure that:

    a. All visitors entering the premises must complete the visitors register,

b. Assist VIP's (as communicated in advance) to access the premises during visits,

23. He/ she records events in an occurrence register and informs the Security Manager as well as the of such incidents
24. He/ she keeps a register of all personnel/ vehicles who visit the offices during their shifts after normal working hours

We 'the company' are not averse to amendments of agreed working guidelines, provided all stakeholders are informed timeously about the amendments, unless agreed to in principle in cases of emergency and that same be placed in writing in due course. ALL said protecting our Client's interest, reputation and assets takes precedence, and can only be achieved by having motivated and empowered officers at the various sites.

SECURITY OFFICERS DUTIES

ACCESS CONTROL:

- **Entry Points**

Visitors will be asked as to whom they are visiting. As soon as it has been established that the visitor has come to see a specific person and that the person in question does work at 'The Company', the visitor will be requested to sign in on 'The Visitors' register. An access card will then be issued to the visitor. The card will only work on preloaded authorized entry points. The visitor must then be directed to the Reception of the person he/ she intends to see. Our access control system will then issue a warning if the visitor does not report to their destination within a set period of time, usually 15 minutes, at that point and a search party we begin. Should a visitor arrive after hours, the person he/ she intend to see must be contacted to meet the visitor at the Main Gate, unless prior arrangements have been made and such arrangements are recorded in the Occurrence Book.

All visitors will go through the metal detectors and parcels and luggage passed through our x-ray machines for dangerous or unwanted goods. The visitors are then monitored with the CCTV as they walk through the premises to their destinations, and they need to check in with their access cards to alert guards that they have arrived at their zones.

Pre-loaded vehicles will pass through automatically when the number recognition identifies them. They will still need to go through the metal detectors and x-ray machines.

Contractors performing work on the premises must sign in the Visitor Control Register being allowed access to the premises. Long term contractors, are preloaded on to the system and granted access zones of where the work should be performed. These access cards will work only during the time zones authorized by the client. Before work commences, the contractor has to sign a Contractors Commitment Form, which should be availed by the officer. ID cards of employees have to be checked daily. Employees not in possession of ID cards must be recorded in the applicable register. They will be issued with a temporary access card.

All vehicles entering and leaving the premises must be searched thoroughly. Dedicated lanes will be issued for staff and pre-registered visitors and contractors. Another lane will be reserved for visitors. In the morning during congested traffic, more lanes will be used for entering and in the afternoon, more will be used for exiting to ensure limited congestion at entry points.

Check all delivery and/ or dispatch documentation against the goods being delivered and/ or removed to/ from premises.

When 'The Company' vehicle leaves the premises, the following details must be recorded in 'The Transport Register':

a. Drivers Name
b. Vehicle Registration Number
c. Kilometer Reading
d. Destination
e. Time Out/ In

Firearm holders must be requested to leave their firearms in the firearm safe provided by the company, and retain the sub key to the respective locker.

FULL knowledge and understanding of these operating procedures is essential. Security Officers must at all times remain alert and suspicious of any 'Company' goods/ property leaving the premises.

All access control is electronic. Our Occurrence books are also electronic and all reports are available to the client at any given moment.

- **Egress/Exit**

1. Upon exit, all visitors and staff to present access cards
2. All visitors will be required to return tags
3. Long term contractors will also be required to return access cards
4. Visitors will be searched. Laptops checked against registering upon entering.
5. Any unauthorized removal of assets will be reported and suspects apprehended.
6. Around half an hour prior to normal operating hours ending, a report of all visitors still on the premises will be run. Security will then proceed to those check points to inform them that all access is about to be terminated. The person being visited will then have to approve any extension of time so the control room can place an exception on those cards.

PATROLS

1. Patrols are normally implemented when a specific area/ premises has to be protected, which is different from Access Control guard duty. Officers on patrol duty are constantly on the move, which makes it difficult for potential intruders to establish the exact locations of Security Officers.

2. General rules before patrolling commences:

   a. The Officer has to be rested and in good physical health.
   b. The Officer must be adequately dressed to with stand extreme weather conditions.
   c. Striking (noteworthy) and/ or noisy objects that could forewarn would be intruders should be minimized/ avoided.
   d. Should the circumstances of the area to be patrolled be unknown to the Officer, he/she should be briefed/ informed of the following:

      - Possible hiding places
      - Unsafe conditions
      - Lighting Conditions
      - Vulnerable areas encompassing expensive items, movable electrical systems, vehicles, tooling etc.
      - Conditions of doors, windows and fences
      - The shift leader/ supervisor must ensure that all new Officers familiarize themselves with all the above captioned.

3. Observations on Patrol

   I. Acute observation regarding items that have been removed and/ or moved to alternate positions is absolutely crucial whilst on patrol.

   II. Careful attention should be given to any signs of unauthorized

   Entry into any building and/ or adjacent thereto.

   III. Should any breach be detected, 'The Control Room' should be informed immediately and an accurate report made in the Occurrence Book, furthermore the 'Head Procurement' of the company to be notified accordingly within 30 (thirty) minutes of detection/ occurrence.

   iv. Any report made in the 'Occurrence Book' should include the below captioned information:

      - Detailed description of the incident
      - Patrol reports must be made in the following instances:
      - Broken doors, windows and locks

- Breach of the perimeter fence

v. Employees found in unauthorized areas

vi. Suspected stolen property recovered

vii. Damage to/ interference with Company property

viii. Faulty/ abnormal lighting systems

ix. Unsafe acts/ conditions

x. Interference with/ disregard of 'Standard Operating Procedures'

xi. Power failures (exact times to be recorded)

4. Patrol Routes

Patrol routes must be altered as often as possible to obviate any potential would be intruder to note the exact number of patrols per shift, the timing thereof and/ or starting and end routes.

KEY MANAGEMENT

1. All doors across all sites will be marked and numbered.
2. In each building a key safe will be installed.
3. The keys will be placed and properly marked to the relevant door within the building.
4. Security control room with key holders for the safe keys.
5. Each morning, patrolling guards will unlock all common area doors of the buildings they are allocated and will lock these doors after normal operating hours in the evening.
6. Should staff require access earlier or later than normal, they will arrange this with the security supervisor on duty who will then assist upon staff member being properly identified.
7. All other doors will operate with an access card system and access will be available 24 hours provided your access card permits you entry into those points.
8. Security supervisors will have unrestricted access; however, their movements and actions will be monitored by the 24-hour CCTV operation.
9. If a key is lost,

a. Security will unlock the door, provided that the person has been properly identified to have access to the area.
b. The door lock will be replaced and marked. Staff member will be issued with a new key.

GENERAL VISITORS

Visitors must not be permitted to wander around in The Company without being accompanied by the company employee/officer. Should a visitor be found wandering on his/ her own, he/she must be taken to the control room and the person been visited being requested to attend to their visitor, failing which permission to access premises may be revoked under notification to the 'Head of Company'. We will be able to monitor all visitors as our access control system will be able to determine where visitors are going and if they have arrived.

DELIVERIES

- The officers at the gate will accompany all deliveries to the mail room. Prior to this:
- All parcels to pass through x-ray machine
- Dogs to be used to check the parcels if they contain any threats
- Full details of driver delivering parcel and positive ID to be confirmed and obtained
- Drivers will then be escorted to exit point
- A manned body will always be available to escort delivery vehicles.

SECURITY OFFICER MONITORING

The security, officer are monitored in several ways.

1. Upon arrival, all officers clock in their shifts on a bio-metric device in the control room, they also clock out when leaving. This allows us to verify which officers are absent from work and afford us the time to obtain a replacement officer if required.

2. The guards are issued with a patrolling system. The system informs them when it is time to do a patrol and where to patrol. Should an officer not comply, it will alert the control room who can then take immediate action.

3. Our Occurrence book is electronic and our control room has access to it off site. Therefore, incidents are monitored as they occur on site and a remedy can be done on the spot.

ELECTRONIC DASHBOARD

Due to our electronic systems, we are able to report on our sites effortlessly. The client can request a report on a specific date and time and we are able to comply with the request immediately.

Due to the fact that some items are system generated, the client is afforded the opportunity to see any non-compliance by us. For instance, if a guard does not report to a clocking point, the system will generate a report that has that item on it. Client can then raise all points relating to such.

CCTV

Our operation of the CCTV technology operates on three levels.

1. The site itself has a control center for the operation of the equipment and monitoring.

2. All sites report into the Mankweng office and monitoring can also occur on that level.

3. The Mankweng control room is also linked to our control room on sites.

As a result, the CCTV is monitored by three individuals simultaneously. This means that:

1. The probability of picking up problems is increased.

2. Full visibility of site functions.
3. Our control room in addition to each site has the ability to retrieve any incidents that may have occurred due to the technology being used.

PROHIBITED ITEMS

The following it ems are not allowed into The Company premises:

- Firearms
- Traditional Weapons
- Drugs
- Alcohol
- Any other items not permissible into the company per management's instructions

All visitors are to be asked whether they would like to declare any such items/ in possession thereof, and be requested to leave the said items in the Security Office for safekeeping. An OB entry must be made and the items/ goods returned when the visitor leaves the premises. Should a visitor refuse to leave any of the mentioned/ restricted items, he/ she must be requested to wait at the Security Office and the matter reported to the Senior Officer on duty. All staff and visitors will pass through walk-through metal detectors and their luggage through x-ray machines to identify possible risks. Should we pick any unwanted items, they will be escorted to a nearby space and hand searched thoroughly.

PREVENTATIVE MAINTENANCE (SECURITY PLAN)

Our equipment comes with a maintenance and warranty plan across the three-year period.

1. Each month, a random sample of devices is tested for issues.

2. Cameras are cleaned and serviced monthly.

3. Testing of emergency procedures and system.

We are proactive in our approach to servicing equipment and detecting possible issues.

DELIVERIES

The officers at the gate will accompany all deliveries to the mail room. Prior to this:

- All parcels to pass through x-ray machine
- Dogs to be used to check the parcels if they contain any threats
- Full details of driver delivering parcel and positive ID to be confirmed and obtained
- Drivers will then be escorted to exit point
- A manned body will always be available to escort delivery vehicles.

6. OPERATIONS WORK PLAN

OPERATIONS MANAGER DUTIES:

- Draft site instructions in collaboration with client requirements,
- Liaise with the Security Manager
- Oversee all operations and adherence to site instructions,
- Training of officers according to site specifications,
- Liaise and establish a strong working relationship with client, and
- Attend to quarterly meetings and/or if there's decisions to be made.

SITE MANAGER

- Co-ordinate, manage and ensure officers are familiar with site instructions,
- Responsible for on job training and refresher training,
- Attend weekly and emergency meetings and liaise with the Security Manager
- Attend to duties of being the first contact officer with client representative,
- Responsible for weekly and monthly reports,
- Attend to site visits during weekends and public holidays
- Attend monthly meetings

SITE SUPERVISOR

- Ensure that officers adhere to site instructions given by site manager,
- Ensure that the company image is maintained,
- Ensure that patrols, access control and general monitoring process is done per site specifications,
- Ensure that the equipment is in good working order,
- Ensure systematic report of incidents is properly transcribed on the occurrence book,

- Ensure that the joint operations control room is updated hourly concerning the site.

SUPERVISION

The company is committed to ensuring that our mobile supervision team, who will also take it amongst themselves to interact with the designated client's representative, will supervise all our security officers. Not only is it the commitment to supervise our security officers, it is the company's core principle to uphold service level agreements in all our dealings. In this regard on job training will further play a critical role in maintaining the acceptable standards whilst adhering to agreed service level agreements.

In order to create, sustain and uphold the present working environment, it is our company's intention to retain and give priority to those deserving employees currently on board with the competitor. However, this does necessarily imply the non-performers will be retained. The experience and previous training of those retained will be passed and amalgamated with our current training

7. SITE PROCEDURE MANUAL

MAIN ENTRANCE ACCESS CONTROL

1. Treat all clients and visitors with respect and in a friendly manner. Example: “Good day Sir/Madam. How can we assist you? Do you have anything to declare? (Fire arms, laptops). Have a nice day and keep well”
2. We do not allow drunk and disorderly persons to have access onto the premises.
3. Access control and searching is done and conducted at all times on all vehicles entering and leaving the premises. All samples are assessed by security at the main gate and directed to the visitor’s pavilion for immediate referrals/assistance (such samples must be directed by pavilion staff to the relevant labs immediately).
4. Security ensures that all registers and relevant documents are completed in full when visitors enter and leave the premises and that all information is recorded on the documents.

SHORT POSTINGS / ABSENCE OF OFFICERS

1. There are normally no short postings except in cases where officers are absent without informing management in time and officers that are sick.
2. In case of absence and illness of officers or other emergencies officers who are on their off days are called to cover the shift.
3. If the shift cannot be covered Cytolux Security supervisors and controllers will assist to cover the site.

EMERGENCY SITUATIONS

1. The security controller will call the emergency services in case of an emergency. (SAPS, Ambulance and Fire Brigade)

2. At an emergency situation no visitors will be allowed to enter the premises through the access gates.

3. In case of an emergency in the premises, security will ensure that the emergency services have quick access to the premises.

4. A security officer will escort the emergency services to the scene.

5. Officers posted in the buildings will assist with evacuation of employees and visitors from the buildings.

6. All paraplegic access gates inside the buildings will be opened by security.

7. Security officers will also assist the evacuation officers in the buildings with safety procedures to see that no one is using the lifts and assist with employees and visitors evacuating the buildings at the stairs and emergency exits.

8. Clear communication channels must be kept on the radio whilst the situation is taken care off.

9. Full OB entries will be made before, during and after the emergency situation.

HIGH PROFILE DIGNITARY VISITS

1. Security will be informed by the client of any visits by High profile dignitaries.

2. High profile dignitaries visit the client.

3. They will have access to the premises as quick as possible and secured parking will be arranged in advance for them.

4. In case of a Minister's visit, body guards will come and sweep the area of visit in advance.

5. Security officers will be placed at strategic areas to assist the safe guarding of the high-profile dignitary.

6. Additional security officers will be arranged on request of the client if necessary.

INCIDENTS: THEFT

1. The client will be informed in case of theft.

2. This will be followed up with communication with Cytolux Security management and the controller.

3. The SAPS will be informed of the theft on the premises. They will take statements and open a case.

4. A preliminary incident report will be done and send to the client and Cytolux Security

management.

5. A full investigation of the theft will be done by Cytolux Security (Statements, photos etc.)

6. A final incident report will be sent to the client by Cytolux Security

8. CONCLUSION

Information is needed at all levels of an entity in order to identify, assess and to respond to risk and also to run the entity and to achieve objectives. For our company to conduct an effective operation, we will capture and use historical data in conjunction with the current one. Historical data will allow us to tract actual performance against targets, plans and expectations. This will data can also provide insights correlations and trends and to forecast on future performance. Historical data can also provide early warnings of potential events or threats that warrant management attention.

Our management team will keep the client's authority up to date on performance, developments, risks and functioning of risk management and other relevant events and issues. We have proof that the more relevant effective communication, the successful client authority will be carrying out its oversight responsibilities. Our communication method raises awareness about the importance and relevance of effective risk management. We also ensure that our personnel communicate risk-based information across all sections.