INFORMATION AND KNOWLEDGE BASE

SECURITY

- Chapter 9 -

Page

9. Security

"If you want to know what a man is like look at the way he treats his inferiors and not his equals" -Sirius Black, a character from Harry Potter written by JK Rowling

- Chapter 9 -

SECURITY

9.1 Introduction

The security of residents, visitors and employees is a critical aspect of the governing body. Residents and their loved ones expect to be safe and for their assets to be protected. It would be wise for the governing body to allocate the necessary time and resources to this function and appoint a governor to this portfolio. Residents expect security to be cost effective, less visible, and intrusive but effective. It is therefore important to plan well before implementation of systems or the upgrading thereof.

9.2 Policy

The governing body should understand and define its responsibility with regards to security, set the boundaries for its responsibility and communicate the policy and its commitment to the community. The policy forms the basis for providing the services that are necessary to achieve the commitment as set out in the document.

9.3 Master Plan

A master plan with an end vision is the best way to tackle the security challenge. It could be very costly to amend a system realizing later that a better option or options existed. Speaking to service providers as to where the industry is heading, attending security conferences, and visiting other governing bodies is highly recommended in the process of producing a well-thought-through, financially affordable, long-term security plan.

9.4 Commitment and Focus

The governing body must ensure that the security function operates at the standard as envisaged in the policy document. The way to ensure this is for management to report comprehensively to the governing body on all critical matters relating to its security on a pre-established format and monthly.

The issues and areas to be overseen by the governing body are *inter alia*:

- The governing body policy on security of the governing body.
- The master plan for security, upgrades, and expansions.
- Security procedures that are equitable, consistent and do not discriminate against any person.

- Indemnities from residents, staff, and visitors.
- Standard operating procedures that cover all security related aspects in detail.
- Security staff, supervisors, and managers training.
- Insurance cover on possible claims and damages because of the actions or non-actions of security personnel.
- Compliance to all the *PSIRA* security labour regulations. Wages, working hours, bonus payments, long service awards, etc.
- Non-adherence to operating instructions and the resultant disciplinary actions.
- Daily, weekly, and monthly checks compliance.
- Security equipment A risk analysis and mitigation plan. This analysis and plan must be reviewed at least every three years and preferably with the input of a knowledgeable person who is up to date with the latest trends in the security industry and who is able to poke holes in the existing security procedures and equipment and devices.
- maintenance, replacements, and upgrades. Services and replacements as per the maintenance plan.
- Incident reporting by categories of severity and the corrective action. Critical incidents must be discussed to ensure remedial steps.
- Security function audits every three years and a plan to address shortcomings.
- Investigate the latest technology and decide if and how this can improve the governing body's security function.
- Approval of all equipment replacement, additions, extensions, and upgrades.
- Service level agreements with service providers. Tender procedures, contracts, monitoring, etc. See paragraph 9.5 below.
- Access control of residents, domestic workers, gardeners, contractors, club members etc
- Armed response and back-up.
- New appointments.
- Insourcing vs outsourcing justifications.
- Security forums in the area and participation therein.
- Background testing policy – staff, contractors and/or tenants.

9.5 Perimeter Control

9.5.1 Introduction

Perimeter control refers to the fences, walls and any other structures surrounding the property and ensuring that prospective intruders remain outside. The perimeter safety can be enhanced with devil's fork, barbed wire, electrified fencing, natural barriers, and a close circuit television

(CCTV) system. People, vehicle, dog, and horse patrols around the property at night must be considered.

9.5.2 Standard Operating Procedures (SOP) for Perimeter Control Function

The standard operating procedures should at least cover the following areas:

- Site and emergency information.
- Job specification of personnel.
- Equipment and personal wares list.
- Perimeter lighting plan and reporting.
- Vehicle-use rules and instructions.
- Perimeter fence plan.
- Perimeter fence daily, weekly, and monthly checks.
- Guard clocking patrol procedures.
- Control room duties including monitoring the CCTV and all the procedures that need to be followed in the control room and reacting to alarms.
- Service and maintenance schedules of all perimeters and perimeter safeguarding equipment.
- The reporting and handling of incidents (occurrence book to be used) where the perimeter is being interfered with as well as any suspicious activities detected.
- The reaction procedures to be followed for alarm detection on electrical fences and the CCTV system.
- Supplier service level agreement monitoring procedures and reporting.
- Security back-up from a response service provider.
- Lightning protection of all cameras, lights, control hardware etc.
- The certificate of compliance (COC) for the electric fence.
- Patrol routes, clocking and procedures to be followed.
- Power back-ups for electricity outages.
- Night control procedures and reporting.
- Incident reporting procedures.
- Incident follow-up procedures by management and governing body. All incidents must be properly analysed, and preventative procedures implemented to prevent a re-occurrence of similar incidents.
- Serious incident investigation at a high level and the related procedures.

9.5.3 Equipment Management

A service contract (service level agreement) with a reliable service provider must be in place for

the systems and equipment in use. Actual performance against the agreement must be monitored.

An equipment replacement and maintenance programme should be drawn up. This schedule can give a good indication of the risk of failure of a particular piece of equipment, the impact of such a failure and the lead time required to replace the item. Critical items should be held in stock to reduce downtime.

Lightning protection poles and ancillary support equipment must be in place and checked for their effectiveness on a yearly basis.

Critical areas and equipment must have a warning system when the equipment is out of order.

9.6 Access Control

9.6.1 Introduction

Access control is defined as rules and procedures that ensure only authorized entry to the governing body's property. This applies to access by residents, employees, domestic workers and gardeners, club members, contractors, all visitors, deliveries, and emergency vehicles.

9.6.2 Standard Operating Procedures for Access Control Function

The standard operating procedures for the access control function should cover at least the following areas:

- Site and emergency information.
- Job specifications of all personnel.
- Detailed duties of the security officer, supervisors, and guards.
- Conduct rules for staff.
- Equipment and personal wares (bullet proof jackets, helmets, etc.), list of personnel.
- Emergency procedures when systems are down.
- Security back-up from a response service provider.
- Power back-ups for electricity outages.
- Control procedures when access system is down.
- Daily, weekly, and monthly security checks to be performed by security officer and their supervisors.
- Residents, gardeners, and domestic worker registration procedures.

- Access control instructions for residents, gardeners and domestic workers, and deliveries. This will include after-hours access procedures as well.
- Access control of visitors including admission procedures by residents. This includes modern visitor applications developed by specialised service providers.
- Access control procedures for contractors to the site.
- Access control procedures for deliveries to the facilities or residents' homes.
- Access control procedures for emergency vehicles and staff.
- Access control procedures for property practitioners.
- Access instructions for other businesses within the premises like golfers, a country club, restaurants, and others.
- Supplier service level agreement monitoring procedures and reporting.
- Background vetting of new tenants, domestic workers, and gardeners.
- Disclaimer to protect the governing body against possible security related claims.
- Occurrence procedures and following of reported incidents whether manual or electronic.
- Blacklisted vehicle monitoring.
- Searching procedures and intervals of cars, bags etc.
- Training of staff.

9.6.3 Equipment Management

It is important that the keypad systems, biometric systems, boom gates, gates and any other equipment that is used in the access control to the premises are correctly maintained. A service contract (service level agreement) must be in place and emergency equipment must be on standby when needed.

An equipment replacement and maintenance programme must be established. This schedule can give a good indication of the risk of failure of a particular piece of equipment, the impact of such a failure and the lead time required to replace the item. Critical items should be held in stock to reduce downtime.

Critical areas and equipment must have a warning system when the equipment is out of order.

9.7 Security in General

9.7.1 Introduction

Security personnel can be either insourced or outsourced, but either way the governing body must ensure that personnel can be relied upon to offer an excellent security service to residents.

9.7.2 Standard Operating Procedures for Security Personnel in General

Areas related to the management of personnel must be covered in standard operating procedures and are as follows. (Also see the chapter on *Human Resources Management*, chapter 7 of this document.):

- The recruitment, appointment, and termination of staff.
- *Private Security Industry Regulations Authority (PSIRA)* registration and membership fees.
- Employment contracts, working conditions, confidentiality agreements.
- Disciplinary code and procedures.
- Payroll, staff duty roster, templates, and payroll related matters.
- Incident reporting and the follow up of any incidents.
- Leave procedures and staff replacements.
- Incentives, penalties, and employee of the month awards.
- Attendance registers or clocking in systems.
- Job specifications, critical performance areas and duties for the various positions.
- Performance evaluation.
- Criminal background vetting.
- Hygiene-related issues around the work area.
- Specific OHSACT.
- Dress code and uniforms.
- Telephone etiquette.
- Radio rules and etiquette.
- Public relations and communication etiquette with residents and visitors.
- Insurance cover on possible negative actions of security staff.
- Resident rules and regulations and how they should be monitored by security.
- Lighting and lighting reports.
- Resident panic button systems.
- Contractors' rules while on site and the monitoring thereof.
- Training of staff.
- Enforcement of general rules of the governing body.

9.8 Other Security Matters

9.8.1 Lighting

Good visibility at all critical perimeter and access points is essential and the governing body will do well to inspect all areas regularly and upgrade the lights to ensure good visibility at night of

the areas that have a higher entry risk.

9.8.2 Safety of Residents

The policy document discussed in the introductory paragraph sets the limit of the governing body's responsibility and the security services provided by the governing body. Additional services may be provided to add to the security of residents such as panic buttons, alarm systems, cell phone applications that alert the guards in emergencies and house visits in instances where owners are absent. Residents should be regularly reminded of their duty and responsibility as far as their own security is concerned.

9.8.3 Private Security Services

The governing body must provide the rules and procedures that apply where residents are allowed to make use of private security companies and their related alarm systems.

Guidelines for appointing a security service provider:

- Size of the service provider. You do not need one-man shows.
- References to be checked thoroughly with one visit to the site.
- *Private Security Industry Regulatory Authority* (PSIRA) registration is necessary.
- *Occupation Health and Safety Act (OHSACT)* compliance must be negotiated.
- Compliance to the *Compensation for Occupational Injuries and Diseases Act* (COIDA) and a letter of good standing is important.
- The service level agreement (SLA) that is signed with the supplier must incorporate *inter alia*:
  - Use the standard agreement supplied by service provider as a starting point.
  - Probation period to be included.
  - Services provided must explain use of staff and equipment, and explain how general maintenance, fence maintenance and CCTV maintenance is going to be done.
- Cost of services and increase clause.
- Prices of equipment that will be replaced.
- Period of the agreement.
- The facility's own SOP on security as explained in this chapter to be included.
- Service levels to be agreed on.
- Access to the facility by the service provider.

9.8.4 Indemnities

Indemnifying the governing body against possible damage claims must be incorporated into the

founding document, member registration form, the website and email correspondence.

9.8.5 Audit of Security Function

The security function should be checked and evaluated at least every three years. An independent consultant should test the perimeter, the access controls, and all other aspects of the governing body's security function. Improvements to the current systems and replacement of old technologies with new developments should be part of the assessment in the report. The governing body should oversee plans for the implementation of the recommendations and allocate the necessary funds for the upgrades. Undercover operations must be considered as this will allow detailed knowledge of what is going on in the function.

9.8.6 Local and Regional Forums

The governing body's involvement in security forums to discuss security matters in the area should be encouraged. It is beneficial to cooperate with and to contribute towards these forums.

9.8 Communications

Keeping residents informed on critical security incidents and related issues are a must. Informed residents are contented residents. The governing body should also enlighten residents of security improvement plans, progress on projects approved and from time to time some general safety precaution reminders.

9.8 Information Security

The safe keeping of information, back-ups and limiting access to the security systems is a must.

9.9 Other Possibilities

Other effective security improvement measures should be considered continuously. Drones, moving cameras, body cameras and body recordings are only a few examples of the possibilities.