Security Information Manual

st martini gardens

74 QUEEN VICTORIA ST., CAPE TOWN 8001, TEL: +27 (0) 21 424 7529, WWW.STMARTINIGARDENS.CO.ZA

1. Purpose of this manual

The trustees of St Martini Gardens are aware of the need to protect the privacy of its members, residents, visitors, employees, service providers and the general public in line with the South African constitution and the Protection of Personal Information Act 2013 (POPIA), and to allow access to this information in terms of the Promotion of Access to Information Act 2000 (PAIA).

This manual describes the way that the SMG Body Corporate (represented by the trustees) will meet its obligations in terms of this legislation to manage and protect the personal information held on-site, by the Building and Security Managers by:

- Stating desired behaviour that recognises privacy as a human right.
- Developing and implementing processes and internal controls for the processing of personal information.

- This manual is aligned with, and subordinate to the SMG Privacy Policy and the SMG PAIA Manual.

Table of Contents

2. System overview

The Body Corporate (consisting of all owners) of St Martini Gardens desires to protect the physical safety and security of the scheme's residents and owners and their property and has authorised the trustees and Building Managers to take steps to support this.

This includes the development, installation and operation of a security system with the following components:

2.1. A **service agreement with Trident Security Services** to provide on-site security services in line with the SMG Security Procedures Manual (which forms the Scope of Work).

2.2. **A closed-circuit television (CCTV) system** with video monitoring and recording capabilities in order to deter, detect and respond appropriately to any criminal or other undesirable behaviour on the SMG common property and in its immediate surroundings.
Audio recording is also enabled in the security cubicles.

2.3. **A tag-based Access Control System** that permits owners, residents, and agents and employees authorised by owners or Building Management to enter and exit the premises freely.

2.4. **An Occurrence Book** that is completed by the security officers on duty to record significant events on site. Supporting incident reports are added when necessary.

2.5. **Whatsapp messages** exchanged between residents and others, and the security officers.

2.6. **Access registers** that are completed by short-term residents; residents without access tags; unaccompanied visitors; and contractors.

2.7. **A wireless intercom system** that enables security officers to call a resident when a visitor arrives. It can also be used for security to make short calls to non-resident trustees and others.

The components of the security system include the collection, processing and use of personal information. This information is considered confidential, and will be accessed, used, safeguarded, released and destroyed in line with the procedures in this manual.

Confidentiality/ privacy agreements are in place between SMG and Trident Security Services and other service providers who have or may have access to confidential and/ or personal information, to ensure that such information will not at any time, during or after termination of their services at SMG, be used, disclosed or removed except as necessary to perform their duties.

The CCTV system, Access Control system and Access Registers include **personal information about persons under 18.**

3. CCTV system

3.1. Purpose

3.1.1. The CCTV system is designed to provide records to deter, detect and respond appropriately to criminal or other undesirable behaviour on the SMG common property and in its immediate surroundings.

3.2. System description

3.2.1. The system consists of network of seven digital video recorders (DVRs) which are located in secure cabinets throughout the complex. Each is connected to a number of cameras (over 100 in total), and to a system management PC via the SMG ethernet network.

3.2.2. The information on each DVR is encrypted and can only be accessed directly with a user id and admin password (which are held by the SMG Security Manager). In the event of theft of a DVR, the data is not accessible.

3.2.3. The system is supported by ES Solutions when necessary.

3.3. Information quality

3.3.1. Cameras have been selected and positioned in order to capture useful images. However, there is no expectation that all of the activities on and around the site are covered, or that all persons involved can be identified.

3.3.2. The accuracy of the date/ time settings on the DVRs are checked periodically.

3.3.3. The DVRs and cameras are powered from the SMG rooftop solar system which has substantial battery capacity and is supported by mains electrical power.

3.3.4. In the unlikely event of total power failure video surveillance and recording from the affected cameras, or all cameras connected to the affected DVR will cease until power is restored. When power is restored surveillance and recording re-starts automatically. No existing data should be lost.

3.4. Privacy and security

3.4.1. Notices are posted at all entrances of the building indicating that the premises are monitored by CCTV.

3.4.2. The system is designed in line with the following privacy principles:

- Residents have some expectation of privacy in the residential corridors, their connecting stairwells and lift interiors, where security risks are low. Therefore the CCTV images from these areas will be recorded but will not be routinely monitored.
- Residents have no expectation of privacy in the ground floor entrance foyers and lift lobbies, the parking garages, the exterior pathways and the garden, where security risks are higher. Therefore the CCTV images from these areas will be routinely monitored by the on-site security officers, and recorded.
- The public has no expectation of privacy in the street immediately outside St Martini Gardens, and therefore the CCTV images of the external perimeter of the site and the street will be routinely monitored by the on-site security officers, and recorded.
- Employees of the Body Corporate and its subcontractors have no expectation of privacy while performing their duties.

3.4.3. Recordings on the whole CCTV system can only be accessed from the system management PC in the boardroom in B block.
The boardroom is kept locked when unattended, and the PC is protected by a userid and password.

3.4.4. The keys to the boardroom and the userid and password for the PC are held by Building Management and the trustee responsible for security matters.

3.4.5. No data is transmitted outside the network.

3.5. Retention and destruction of information

3.5.1. Storage space on the hard drives is limited. Recordings are automatically overwritten, usually after two to three weeks.

4. Access control system

4.1. Purpose

4.1.1. The tag-based Access Control System permits owners, residents, and agents and employees authorised by owners or Building Management to enter and exit the premises freely.

4.2. System description

4.2.1. The system consists of tag readers at the pedestrian entry/ exit points to SMG, a monitor in each security cubicle, a system controller, and a system management PC.

The components of the Access control system are connected on a separate closed ethernet network: no data is transmitted outside this network.

4.2.2. The tag holder's data (consisting of name, photograph, flat number and contact details) is linked to the tag number and appropriate access permissions, and this is stored on the system controller.

4.2.3. Monitors in each security cubicle display the name, flat number and photograph of the most recent users of any of the entry or exit points on a scrolling display. This enables the security officers on duty to identify the use of a tag by an unauthorised third party.

4.2.4. Tag-holder data is captured, queried and maintained via the system management PC by the SMG Security Manager or, in his absence, the Building Manager or a designated trustee.

4.2.5. The system is supported by Quantum Fire and Access when necessary.

4.3. Information quality

4.3.1. The information in the system is not intended to be a complete record of persons entering and exiting the premises, as it is only used by pedestrians, and not separately by each member of a group who enter or exit together.

4.3.2. All elements of the system are powered from the SMG rooftop solar system which has substantial battery capacity and is supported by mains electrical power.

4.3.3. Tag-holder reports are extracted twice a year in order for Building Management to "audit" and remove expired and redundant tags from the system.

4.4. Privacy and security

4.4.1. Residents have some expectation of privacy when entering or leaving the premises, therefore the monitors in the security cubicles are angled so that they cannot be seen by others outside the cubicle.

4.4.2. The system database can only be accessed from the system management PC which is in a locked office.
The office is kept locked when unattended, and the PC is protected by a userid and password.

4.4.3. The keys to the office and the userid and password for the PC are held by Building Management and the trustee responsible for security matters.

4.4.4. Transaction data can be extracted from the system via built-in reports, but this is not done routinely.

4.5. Retention and destruction of information

4.5.1. When a tag-holder moves out or a change of owner takes place, the personal information relating to the tag-holder is delinked from the assigned tag and flagged for deletion when database maintenance is done (usually every 2nd month).

4.5.2. Unless required for ongoing investigations, tag transaction data is deleted after two months.

5. Occurrence Book and supporting incident reports

5.1. Purpose

5.1.1. The Occurrence Books (OBs) and supporting incident reports are completed in order to record significant events on site as observed by the security officers.

5.2. Description

5.2.1. Occurrence books currently in use are kept in the A and B block security cubicles. They may only be removed for inspection by the security service provider's management, the SMG Building management and/ or the trustee responsible for security matters for a short period, as necessary in order to manage the physical safety and security of SMG's residents and owners and their property.

5.2.2. Incident reports are completed when required and handed to the Security Manager or Building manager as soon as practical.

5.3. Information quality

5.3.1. The information in the OBs and incident reports is handwritten by the security officials on site. While the officers are aware of the need for accuracy, especially in regard to correct identification of persons involved, errors may occur.

5.4. Privacy and security

5.4.1. Occurrence books currently in use are kept in the A and B block security cubicles, under the control of the officer(s) on duty.
The B block security cubicle is never left unattended; the A block cubicle is locked when unattended.

5.4.2. Completed Occurrence Books and Incident Reports are filed in a locked cabinet in a locked store-room under the control of Building Management.

5.5. Retention and destruction of information

5.5.1. Unless required for ongoing investigations, Occurrence Books and Incident Reports are shredded after five years.

6. Whatsapp messages

6.1. Purpose

6.1.1. Whatsapp messages are sent by residents and others to the security officers to inform them of incidents. The security officers respond, for confirmation or to request further information.

6.2. Description

6.2.1. Whatsapp messages are sent and received on the smartphone held by the senior security officer in the B block security cubicle.
This phone may only be removed for inspection by the security service provider's management, the SMG Building management and/ or the trustee responsible for security matters for a short period, as necessary in order to manage the physical safety and security of SMG's residents and owners and their property.

6.3. Information quality

6.3.1. The Whatsapp messages are sent by residents and others, and responded to by the security officials on site.
While the security officers are aware of the need for accuracy, especially in regard to correct identification of persons involved, errors may occur.

6.4. Privacy and security

6.4.1. The smartphone is kept in the B block security cubicles, under the control of the officer(s) on duty. This security cubicle is never left unattended.

6.5. Retention and destruction of information

6.5.1. Unless required for ongoing investigations, Whatsapp messages are deleted after 1 week.

7. Access registers

7.1. Purpose

7.1.1. Access registers are completed by short-term residents; residents without access tags; unaccompanied visitors; and contractors in order to maintain the physical safety and security of the scheme's residents and owners and their property, and to provide information to support compliance with the SMG Conduct Rules, especially in terms of overcrowding and disturbances.

7.2. Description

7.2.1. There are three Access Registers, one for Contractors, one for Visitors (and residents without tags) and one for Short-stay residents. They all include space for names, contact numbers, destination and other personal information.

7.2.2. The Access Registers currently in use are kept in the A and B block security cubicles. As soon as a page is completed, it is removed from the file and given to the Security Manager or (out of hours) put under his office door.

7.3. Information quality

7.3.1. The information on the registers is handwritten by the resident/ visitor/ contractor. The accuracy of the information provided cannot be relied on.

7.4. Privacy and security

7.4.1. The completed forms are kept in a ring binder in a locked cupboard in a locked store-room under the control of the Building Manager.

7.5. Retention and destruction of information

7.5.1. Access Registers are shredded after five years.

8. Wireless intercom system

8.1. Purpose

8.1.1. The wireless intercom system enables security officers to call a resident when a visitor arrives. It can also be used for security to make short calls to non-resident trustees and others.

8.2. Description

8.2.1. The wireless intercom system is GSM-based. There is one unit in each security cubicle (A and B blocks).

8.2.2. The systems are programmed with names, phone numbers and access codes: the security officer uses a printed list to look up and use the access code for a resident in order to call him/ her.

8.2.3. The SMG data for the system is stored on a password-protected server belonging to the system supplier (Accentronix). It is updated by the Building Manager when required, by logging on to the server with a userid and password.

8.2.4. The system is supported by Sirens Electronics when necessary.

8.3. Information quality

8.3.1. The information in the Intercom system is provided voluntarily by residents and others (including trustees and service providers) by way of a resident information form or otherwise e.g. verbally or by e-mail.
The data subjects are entitled to check and amend their own information at any time.

8.4. Privacy and security

8.4.1. The printouts from the system given to security officers consist of names, flat numbers and access codes only – they do not include the residents' phone numbers.

8.5. Retention and destruction of information

8.5.1. The records are deleted when the resident moves out, or on the request of the data subject.

9. Internal investigations using security system information

9.1. The following incidents are the most likely to give rise to a need to access and process security system information:

9.1.1. An incident giving rise to a charge laid with the SAPS. The case number must be provided to substantiate this.

9.1.2. An incident that has caused loss or injury to an owner, resident, visitor, or the Body Corporate but which appears to be accidental, or where it is not considered appropriate for the matter to be reported to the SAPS.

9.1.3. A material breach of the Body Corporate's Conduct Rules where the alleged offender cannot otherwise be identified.

9.1.4. Alleged misconduct of a worker employed by the Body Corporate or one of its subcontractors.

9.1.5. Any other incident or alleged incident which, in the opinion of the trustee body, warrants investigation by this means.

9.1.6. An approved request for information in terms of PAIA.

9.2. An investigation may be requested by any person who is affected by an incident described above.

9.2.1. Where possible, the time and place of the incident must be specified so that only the relevant information/ recordings of specific locations and time periods are searched.

9.2.2. Any complaints requiring investigation of CCTV recordings must be received timeously, before the material is overwritten.

9.2.3. Any complaints requiring investigation of Access control system recordings must be received timeously, before the material is deleted.

9.3. The first part of the investigation form (Appendix A) must be completed by or on behalf of the requestor, including the purpose of the investigation, and submitted to Building Management or the trustees.

9.4. If satisfied that the investigation is justified in terms of the circumstances listed above and stated purpose, and it is considered that such an investigation will be productive, the investigation may be approved by a trustee or one of the Building Management staff who is not the requestor.

9.5. Special care must be taken when the investigation involves a person under 18.

9.6. When the investigation is approved, the relevant information may be searched for and inspected by one or more member of the Building Management staff and/ or trustee (who may be the requestor or the approver).

9.6.1. The details of the information searched (including specific cameras and periods for CCTV recordings) must be recorded on the investigation form.

9.6.2. If information is found that meets the stated purpose, an extract from the records will be copied and secured.

9.6.3. This extract must only include a minimum of information required to provide evidence of the (alleged) incident.

9.6.4. Special care must be taken if the information found relates to a person under 18.

9.6.5. The copied information will be secured under control of the Security Manager or Building Manager.

9.6.6. Any other copy of the information made must be recorded on the log form.

9.7. If no useful information is found, this must be recorded on the log form.

10. Releasing written information about an incident

10.1. A written report of the (alleged) incident may be prepared. This should only include a minimum of information required to serve the purpose of the investigation.

10.2. The written report may be released:

10.2.1. To the requestor, where no person other than the requestor is identified in the report, or where all persons identified in the report give their consent.

10.2.2. To the respective member where the incident involves alleged misconduct of a resident of or visitor to their section.

10.2.3. With the consent of the Information Officer, to the respective employer where the incident involves alleged misconduct of a worker employed by the Body Corporate or one of its subcontractors.

11. Releasing a copy of a record

11.1. Copies of records made should only include a minimum of information required to serve the purpose of the investigation.

11.2. Special care must be taken when the record includes personal information about a person under 18.

11.3. A copy of a record may be released to the requestor, where no person other than the requestor is included in the record, or where all persons identified in the record give their consent.

11.4. A copy of a record may be released, with the consent of the Information Officer, in the following circumstances:

11.4.1. To the SAPS, where a case has been logged and the case number provided, or in response to a subpoena, or otherwise as required by law.

11.4.2. To the respective member where the incident involves alleged misconduct of a resident of or visitor to their section.

11.4.3. To the respective employer where the incident involves alleged misconduct of a worker employed by the Body Corporate or one of its subcontractors.

Copies of record(s) will be provided on media provided by the requestor, or at a reasonable fee.

11.5. A copy of a record may be provided to any other person in terms of an approved PAIA application, on payment of the specific fees.

12. Deleting a copy of a record

12.1. Copies of records made in the course of investigations by the Body Corporate will be destroyed after 180 days, unless otherwise requested in writing for a valid purpose, in which case they will be destroyed as soon as the purpose is achieved.

13. Auditing the process

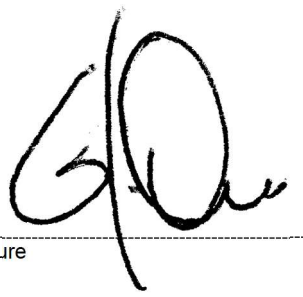
Compliance with the process will be included in the Information Officer's periodic Privacy Review, and a summary of his findings will be included in the annual Trustee Report to members.

14. Investigation log form (Appendix A)

Attached

15. Approval

Glyn Fogell
Information Officer



Signature

18 November 2024

Date

Glossary of acronyms

BC	Body Corporate
CCTV	Closed Circuit Television
CSOS	Community Schemes Ombud Service Act 2011
OHS [Act]	Occupational Health and Safety Act 1993
PAIA	Promotion of Access to Information Act 2000
POPIA	Protection of Personal Information Act 2013
SMG	St Martini Gardens
STSMA	Sectional Titles Schemes Management Act 2011

Revision History

November 2024	pp 2&6 – Removal of references to COVID Compliance p 2 - Amend service provider name pp 3&4- Add reference to rooftop solar power system p 4 – Amend retention period pp 5&6 – Amend storage location

St Martini Gardens investigation log Number:

Request for investigations using security system information			
Requestor name			
Address			
Phone number		e-mail address	
Details of alleged incident (include date, time and place)			
Purpose of investigation			
Signature		Date	
Approving the investigation of security records			
Name		Position	
Signature		Date	
Locating, viewing and copying security records			
Name		Position	
Information (date/ time, cameras)			
Details of extract(s) copied			
Location of copies			
Releasing information from security records			
Written report prepared by		Date	
Released to		Date	
Records copied by		Date	
Released to		Date	
Deleting a secured copy of security records			
Deleted by		Date