

Martin Towers

Video Surveillance Policy



Introduction

The purpose of the *Video Surveillance* policy is to define the policy towards the intended use of the video surveillance system and subsequent access to Video Data recorded within Martin Towers. The *Video Surveillance* policy has been developed in concert with the [Australian Privacy Act 1988](#) and the [South Australian Surveillance Devices Act 2016](#).

The *Video Surveillance* policy is in force for Community Corporation No. 23362 Inc. and addressed the apartment complex situated at 4 – 8 Charles Street, Adelaide South Australia.

We recognise the importance of protecting the privacy of information collected depicting our residents and visitors to our apartment complex, in particular information that is capable of identifying an individual ("personal information"). This *Video Surveillance* policy governs the manner in which your personal information, obtained through admittance to the apartment complex, will be dealt with. This *Video Surveillance* policy may be reviewed from time to time and you will be informed of material changes. A copy of the *Video Surveillance* policy will be available from the web site (www.223NorthTce.info).

Definitions

1. **Authorised Maintainer** is the installing company (i.e., *SA Electronics*)
2. **Caretaker** is the person appointed as the primary caretaker to Martin Towers
3. **Committee Members** are the elected members of the Martin Towers Management Committee
4. **Communications Room** is the room that houses the video monitor and video recording equipment
5. **Corporation Manager** is the Body Corporate Manager of Martin Towers
6. **Incident** is an occurrence that it would be reasonably expected to result in harm to the environment, equipment or a person.
7. **Management Committee** are the elected Martin Towers Management Committee
8. **Other persons** are members of the public who are not Owners or Residents
9. **Owners** are owners of apartments within Martin Towers
10. **Police Officer** refers to officers of the SA Police force or Commonwealth Police force
11. **Presiding Officer** is the person appointed as Presiding Officer of Martin Towers Management Committee
12. **Residents** are people who occupy apartments within Martin Towers
13. **Security Manager** is the member of the Martin Towers Management Committee tasked with leading the building security sub-team
14. **Video Data** is the individual or integrated video imagery and/or video metadata

Purpose

The purpose of the *Video Surveillance* policy is to ensure that the use of the recorded Video Data, from the Martin Towers, Closed Circuit Television (CCTV) system is only used for the investigation of Incidents, for reasons to support the maintenance of the CCTV system and for no other purpose. Individual's access to Video Data will only be allowed as described below.

Martin Towers

Video Surveillance Policy



The purpose of the CCTV system is to record video and associated metadata only for the purposes of providing a video record of potential nefarious events.

Collection of Personal Information

Personal information is collected when individuals enter and perambulate within the apartment complex. It is our intention that this policy will protect your personal information from being dealt with in any way that is inconsistent with applicable privacy laws in Australia.

Use of Personal Information

Personal information that residents and visitors provide by entering the apartment complex is used only for the purpose for maintaining security of persons and common property or for such other secondary purposes that are related to the primary purpose, unless we disclose other uses in this Video Data Privacy Policy. Copies of video data, that may contain personal information, may be stored in secure archives for record-keeping and back-up purposes only.

Disclosure

Disclosure of video data is necessary to achieve the purpose for which it was collected, personal information may be disclosed in situations where we have reason to believe that doing so is necessary to identify, contact or bring legal action against anyone damaging, injuring, or interfering (intentionally or unintentionally) with our rights or property, residents, lawful visitors, or anyone else who could be harmed by such activities. Also, we may disclose personal information when we believe in good faith that the law requires disclosure.

Security

We strive to ensure the security, integrity and privacy of personal information collected and we review and update our security measures in light of current technologies. Unfortunately, no video data collection technology can be guaranteed to be totally secure. However, we will endeavour to take all reasonable steps to protect the personal information collected by the video cameras. We endeavour to make our best efforts to ensure the security on our video systems and video data collected.

In addition, our employees and the contractors who provide services related to our video cameras are obliged to respect the confidentiality of any personal information held by us. However, we will not be held responsible for events arising from unauthorised access to your personal information.

Martin Towers

Video Surveillance Policy



Access to Information

We will endeavour to take all reasonable steps to keep secure any information which we hold about you. In addition, our employees and the contractors who provide services related to our video systems and video data are obliged to respect the confidentiality of any personal information held by us.

Specifically, those persons who will normally have access (including remote access) to the video data will consist of the apartment complex Caretaker and our Presiding Officer or their delegate, who at their discretion may make video data recordings for purposes consistent with this policy. The Caretaker and/or the Presiding Officer may at their respective discretions allow video data recording to be displayed to relevant employees of our corporation manager and/or to members of the police force and/or members of our Management Committee. This video data recording may also be displayed to professionals acting on our behalf and to members of the courts in Australia or as required by law.

Destruction of Information

Duplication of video data to media must subsequently be either properly disposed of by destruction of the media or by delivery of the media to the police. Similarly, any failed video system component that has been used to store video data must be appropriately destroyed to mitigate against the likelihood that this data could be subsequently recovered.

Problems or Questions

If we become aware of any ongoing concerns or problems with the collection of video data, we will take these issues seriously and work to address these concerns. If you have any further queries relating to our Video Data Privacy Policy, or you have a problem or complaint, please contact us through any member of the management committee.

Notice to the Public

Notices shall be provided warning the public as to the presence of the CCTV system.

CCTV Recordings

The following areas will be supported by video surveillance:

- Gym area
- Mail room
- North Tower foyer
- Plaza area
- Pool area

Martin Towers

Video Surveillance Policy



- South Tower ground floor covering lift entry
- South Tower lift
- Sub-basement car park

Video recording will be motion activated and saved on a continuous loop. Older Video Data will be automatically over-written.

CCTV System Access

The following individuals will have access to the Video Data, for the purpose stipulated:

- **Authorised Maintainer** access to the live video and to recorded Video Data for the purpose of system maintenance only
- **Caretaker** will have access to the live video and to recorded video, requiring user login, for the purpose of investigating potential incidents
- **Security Manager** will have access to live video for the purpose of confirming that the CCTV system is operational but will not be offered a user login
- **Police Officer** will have access to recorded Video Data, typically in the form of removable media, for the purpose of searching for events of interest (i.e., incidents)

The activities that are sanctioned under the *Video Surveillance* policy, are identified below:

1. The **Authorised Maintainer** will have a valid administrator login.
2. The **Caretaker** will have a valid user login.
3. The **Corporation Manager** has the authority to engage the Authorised Maintainer to provide remedial and preventive maintenance to the CCTV system. The **Corporation Manager** will invoice the **Resident** who requested the video to be given to a **Police Officer** for the amount covering the cost of production and the cost of the removable media required to store the Video Data. If the Corporation Manager or the Management Committee has requested the Video Data, then the cost will be borne by the corporation.
4. The **Caretaker** will confirm on a regular basis that the CCTV system is operational. The **Caretaker** has the authority to escort **Police Officers** into the Communication Room, present video of potential interest associated with an Incident and if so requested, to copy the applicable Video Data to removable media for offline access by the **Police Officer**. The **Caretaker** must create a record of any Video Data recorded to removable media.
5. Jointly (i.e., the request must come from both individual), the **Presiding Officer** and the **Security Manager** are authorised to request the **Caretaker** to make copies of Video Data pertaining to an Incident onto removable media. This request must be addressed to the **Management Committee** on or before the next Management Committee meeting. The **Caretaker** will have the responsibility to hold the removable media securely from unauthorised access.
6. The **Security Manager** will periodically confirm that the that the CCTV system is operational.
7. Person or organisations, other than those identified above, will not be permitted to view live or recorded Video Data without the approval of both the **Presiding Officer** and the **Security**

Martin Towers

Video Surveillance Policy



Manager or their delegates, in the case where one or both are unable to provide this authority. There must be a valid reason for the viewing of Video Data for the Video Data to be accessed. Typically, this will involve the occurrence of prior damage or threat to property or person, or theft of property. Copies of Video Data can only be made upon request from a **Police Officer** and only be given to the **Police Officer**.

Revision History

<i>Issue Number</i>	<i>Date</i>	<i>Author</i>	<i>Extent of Change</i>
8	20 Jun 2020	P Relf	Substantial update, reviewed by Con Karykis