**[company name]**

**CCTV POLICY STATEMENT v3.0**

**xxx 2016**

Contents

[1 Owner 2](#_Toc463098183)

[2 The CCTV system 3](#_Toc463098184)

[2.1 System components 3](#_Toc463098185)

[2.2 CCTV camera locations 3](#_Toc463098186)

[2.3 Signage 3](#_Toc463098187)

[2.4 Effectiveness 3](#_Toc463098188)

[3 Purpose of the system 3](#_Toc463098189)

[3.1 Introduction 3](#_Toc463098190)

[3.2 Covert recording 4](#_Toc463098191)

[4 Legal context for the CCTV system 5](#_Toc463098192)

[5 The Security Control Room 6](#_Toc463098193)

[5.1 Monitoring 6](#_Toc463098194)

[5.2 Access 6](#_Toc463098195)

[5.3 Procedures manual 6](#_Toc463098196)

[5.4 Compliance with the POPI Act 6](#_Toc463098197)

[5.5 Staff 6](#_Toc463098198)

[5.6 Recording 6](#_Toc463098199)

[6 Access to images 7](#_Toc463098200)

[6.1 Access to images by third parties 7](#_Toc463098201)

[6.2 Contractual relationship with Operator 7](#_Toc463098202)

[6.3 Access to images by a subject 7](#_Toc463098203)

[7 Request to prevent processing 8](#_Toc463098204)

[8 Complaints and requests 8](#_Toc463098205)

[9 Monitoring of the system 8](#_Toc463098206)

[10 Appendix 1 8](#_Toc463098207)

[11 Appendix 2 8](#_Toc463098208)

[12 Appendix 3 9](#_Toc463098209)

[13 Appendix 4 10](#_Toc463098210)

[14 Sources 10](#_Toc463098211)

# Owner

The Owner of the CCTV system on behalf of [company name] is xxx.

The Owner can be contacted at email address: xxxx.

The Owner has the following responsibilities:

* Ensure that the use of CCTV systems is implemented in accordance with this policy
* Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes
* Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy
* Ensure that the CCTV monitoring is consistent with the highest standards and protections
* Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy
* Maintain a record of access (e.g. an access log) to or the release of images or any material recorded or stored in the system
* Approve the location of temporary cameras to be used during special events that have particular security requirements and ensure their withdrawal following such events.
* Give consideration to both staff and customer feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment
* Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the business and be mindful that no such infringement is likely to take place
* Ensure that adequate signage at appropriate and prominent locations is displayed as detailed above
* Ensure that monitoring images are stored in a secure place with access by authorised personnel only
* Ensure that images recorded on tapes/DVDs/digital recordings are stored for a period not longer than xxx days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil) or other bona fide use as approved by the Information Officer
* Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics
* Ensure that camera control is not infringing an individual’s reasonable expectation of privacy in public areas
* Ensure that where South African Police Service request to set up mobile video equipment for criminal investigations, legal advice has been obtained and such activities have the approval of the Information Officer
* Ensure that staff operating the CCTV system have been adequately trained in the application and use of this policy

# The CCTV system

## System components

* Fixed position cameras
* Pan Tilt and Zoom cameras
* Monitors
* Multiplexers
* Digital recorders
* Control room
* Documentation
* Public information signs

## CCTV camera locations

CCTV cameras will be located at relevant points on the premises of [company name], including but not limited to:

* X
* X
* X
* X

No camera will be hidden from view.

## Signage

Signs will be prominently placed at relevant points on the [company name] premises to inform staff, visitors, customers and members of the public that a CCTV system is in use. Also see Appendix 4.

## Effectiveness

Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

# Purpose of the system

## Introduction

The system has been installed by [company name] with the primary purpose of reducing the threat of crime generally, protecting [company name]’s premises and helping to ensure the safety of all [company name]’s staff, customers and visitors consistent with respect for the individuals' privacy. These purposes will be achieved by monitoring the system to:

* Deter those having criminal intent
* Assist in the prevention and detection of crime
* Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order
* Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff and assist in providing evidence to managers and/or to a member of staff against whom disciplinary or other action is, or is threatened to be taken.
* To provide management information relating to employee compliance with contracts of employment

SAIDSA observation categories. Observation categories are defined as follows:

* Monitoring and Control – to oversee a large area or wide field of view;
* Detection – to be alerted to the presence of activity in the field of view;
* Observation – to be able to observe characteristics within a moderately sized field of view;
* Recognition – to be able to identify a known person or object within the field of view;
* Identification – to be able to clearly identify an unfamiliar individual or object within the field of view.

Source: SAIDSA By Law 9 [www.saidsa.co.za](http://www.saidsa.co.za)

In specific applications, such as schools, a more detailed review of purposes might be required, yielding the following list as example purposes:

* To prevent or respond to Bullying
* To prevent or respond to Truancy
* To prevent or respond to Smoking
* Other disciplinary infringements
* To monitor Staff behaviour
* To monitor Visitor behaviour
* To monitor Security
* Crime investigation
* To monitor Personal safety
* Dispute resolution
* Protecting staff and students from outside threats
* Theft prevention and prosecution

The system will not be used:

* To provide recorded images for the world-wide-web.
* For any automated decision taking

## Covert recording

Covert cameras may be used under the following circumstances on the written authorisation or request of xxx and where it has been assessed by xxx

* That informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording; and
* That there is reasonable cause to suspect that unauthorised or illegal activity is taking place or is about to take place.

Any such covert processing will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected unauthorised activity.

The decision to adopt covert recording will be fully documented and will set out how the decision to use covert recording was reached and by whom.

# Legal context for the CCTV system

[company name] is committed to compliance with the Protection of Personal Information Act, No. 4 2013 (POPI Act). As such, this policy addresses the following specific requirements of the POPI Act:

* Condition 1: Accountability. The Owner is accountable for lawful processing of personal information in the use of the CCTV system
* Condition 2: Lawfulness of processing and Minimality. The Owner will ensure these conditions are met
* Condition 2: Consent. The use of the CCTV system is in accordance with of section 11(f), “legitimate interests of the responsible party”. Specifically these interests are:
  + x
  + X
  + X
  + X
* Condition 3: Specific purpose. As detailed under Condition 2 the specific purposes are:
  + x
  + X
  + X
  + X
* Condition 3: Retention of records. CCTV images will be retained for a period adequate to fulfil the purposes specified. This will normally be for a period of xxx (also see section 5.6 below). After this period the CCTV images will be electronically deleted.
* Condition 4: Further processing limitation. CCTV images captured by the system may be further process in accordance with section 15 (3) (c) (iii), conduct of proceedings in any court. This may also require the retention period be increased for this further processing purpose.
* Condition 6: Openness. Data subjects have the right to request access to the CCTV images using the [company name] request process. See also section 6.2 below.
* Condition 6: Notification to data subject. Signage will be implemented to comply with section 18 of the POPI Act. See also section 2.3 above.
* Condition 7: Security safeguards. The Owner will ensure compliance with sections 19 to 22 of the POPI Act. Also see clauses 5 and 6 below for examples of specific measures.
* Condition 8: Data subject participation. The [company name] data subject access request process will be used.

The Owner will ensure that in all other respects [company name] will comply with the requirements of the POPI Act through an annual review of the CCTV system with the [company name] Information Officer (see section 9 below).

# The Security Control Room

## Monitoring

Images captured by the system will be monitored and recorded in the Security Control Room, "the control room", twenty-four hours a day throughout the whole year. Monitors are not visible from outside the control room.

## Access

No unauthorised access to the Control Room will be permitted at any time. Access will be strictly limited to the duty controllers, authorised members of senior management, police officers and any other person with statutory powers of entry. A list of those members of senior management authorised to access the Control Room is given at Appendix 2.

## Procedures manual

Details of the administrative procedures which apply to the Control Room will be set out in a Procedures Manual, a copy of which is available for inspection by prior arrangement, stating the reasons for the request.

## Compliance with the POPI Act

Images of identifiable living individuals are subject to the provisions of the Protection of Personal Information (POPI) Act, 2013; the Control Room Supervisor is responsible for ensuring day to day compliance with the Act. All recordings will be handled in strict accordance with this policy and the procedures set out in the Procedures Manual.

## Staff

All staff working in the Security Control Room will be made aware of the sensitivity of handling CCTV images and recordings. The Control Room Supervisor will ensure that all staff are fully briefed and trained in respect of the functions, operational and administrative, arising from the use of CCTV.

Training in the requirements of the POPI Act, 2013 will be given to all those required to work in the Security Control Room by xxx.

Staff access to the system will be limited through appropriate use of secure logon and access procedures.

## Recording

Digital recordings are made using digital video recorders operating in time lapse mode. Incidents may be recorded in real time.

Images will normally be retained for xxx days from the date of recording, and then automatically over written and the log updated accordingly. Once a hard drive has reached the end of its use it will be erased prior to disposal and the log will be updated accordingly.

All hard drives and recorders shall remain the property of [company name]until disposal and destruction.

# Access to images

All access to images will be recorded in the Access Log as specified in the Procedures Manual.

Access to images will be restricted to those staff who need to have access in accordance with the purposes of the system. A list of such staff is given at Appendix 2.

## Access to images by third parties

Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and is limited to the following authorities:

* Law enforcement agencies where images recorded would assist in a criminal enquiry and/or the prevention of terrorism and disorder
* Prosecution agencies
* Relevant legal representatives
* The media where the assistance of the general public is required in the identification of a victim of crime or the identification of a perpetrator of a crime
* People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings.
* Emergency services in connection with the investigation of an accident.

## Contractual relationship with Operator

Where [company name] makes use of a service provider (e.g. a security company operating the system or the provider of the CCTV systems components), known in the POPI Act as an Operator, the Owner will ensure that there is a valid POPI Act-compliant contract in place with the Operator.

## Access to images by a subject

CCTV digital images, if they show a recognisable person, are personal data and are covered by the POPI Act. Anyone who believes that they have been filmed by CCTV is entitled to ask for a copy of the data, subject to exemptions contained in the Act. They do not have the right of instant access.

A person whose image has been recorded and retained and who wishes access to the data must apply in writing to xxx. Subject Access Request Forms are obtainable from xxx, between the hours of 0900 and 1200 and 1400 to 1700 Monday to Friday, except when [company name]is officially closed.

xxx will then arrange for a copy of the data to be made and given to the applicant. The applicant must not ask another member of staff to show them the data, or ask anyone else for a copy of the data. All communications must go through xxx. A response will be provided promptly and in any event within xxx days of receiving the required fee and information.

The POPI Act gives the Information Officer the right to refuse a request for a copy of the data particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

If it is decided that a data subject access request is to be refused, the reasons will be fully documented and the data subject informed in writing, stating the reasons.

# Request to prevent processing

An individual has the right to request a prevention of processing where this is likely to cause substantial and unwarranted damage or distress to that or another individual.

All such requests should be addressed in the first instance to xxx, who will provide a written response within xxx days of receiving the request setting out their decision on the request. A copy of the request and response will be retained.

# Complaints and requests

It is recognised that members of [company name]and others may have concerns or complaints about the operation of the system. Any complaint should be addressed in the first instant to xxx.

The contact point for members of [company name]or members of the public wishing to enquire about the system will be xxx which will be available during the hours of 0900 and 1200 and 1400 to 1700 Monday to Friday except when [company name] is officially closed.

Upon request enquirers will be provided with:

* A summary of this statement of policy
* A subject access request form if required or requested

# Monitoring of the system

The effectiveness of the system and all documented procedures will be kept under review and a report periodically made to the [company name] Executive Committee. This will happen at least once per calendar year.

# Appendix 1

**Authorised access to the Security Control Room.**

Other than Security Control room personnel the following have authorised access to the Security Control Room:

Xxxx

xxxx

# Appendix 2

**Access to recordings**

Those authorised access to recordings in order to achieve the purposes of the system (list of names)

Xxxx

Xxxx

# Appendix 3

**Checklist for the [company name] CCTV system**

|  |  |
| --- | --- |
| Checklist item | Status |
| 1. There is a named individual who is responsible for the operation of the system. |  |
| 1. The problem we are trying to address has been clearly defined and installing cameras is the best solution. This decision should be reviewed on a regular basis. |  |
| 1. A system has been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required. |  |
| 1. Cameras have been sited so that they provide clear images. |  |
| 1. Cameras have been positioned to avoid capturing the images of persons not visiting the premises. |  |
| 1. There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s). |  |
| 1. Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them. |  |
| 1. The recorded images will only be retained long enough for any incident to come to light (eg for a theft to be noticed) and the incident to be investigated. |  |
| 1. Except for law enforcement bodies, images will not be provided to third parties. |  |
| 1. The potential impact on individuals’ privacy has been identified and taken into account in the use of the system. |  |
| 1. The organisation knows how to respond to individuals making requests for copies of their own images. If unsure the controller knows to seek advice from the Information Commissioner as soon as such a request is made. |  |
| 1. Regular checks are carried out to ensure that the system is working properly and produces high quality images |  |

# Appendix 4

**Sample wording for notification signs**

In line with the POPI Act, notification (condition 6) should be given when collecting image or sound of individuals. Wording used in signage should be appropriate to the purposes defined in the CCTV policy. The purpose or purposes (condition 3 of the Act) should be made clear in the privacy notice on the organisation’s web site. A source of further information such as the relevant full privacy notice or policy should be provided. Note: A QR code generator can be found at <http://www.qr-code-generator.com/>

Size: be an appropriate size depending on context. For example, whether they are viewed by pedestrians or car drivers.

Placement: entrances to premises and in other appropriate places as reminders, especially where they might not be expected to be in operation. Be clearly visible and readable;

Sample signage wording:

Michalsons suggested the following notification wording in 2008 ([www.michalsons.co.za](http://www.michalsons.co.za)) but this is probably excessive for most signage purposes (rather include in your privacy notice or policy document):

*“CCTV Monitoring: In order to protect your personal safety when on our premises; and investigate, detect or prevent crime and to apprehend or prosecute offenders, we reserve the right to: inspect your person or property when entering our premises; refuse you entry in our discretion; and monitor and record activities that are in plain view on our premises using closed circuit television (CCTV) cameras. By entering our property, you acknowledge that you are aware that we may monitor your activities and consent to us disclosing CCTV footage to authorised persons.”*

# Sources

Acknowledgement is provided to the three sources used in developing this document for use in South Africa in supporting compliance with the POPI Act:

* Data Protection in Schools, 2015. Available from <http://www.dataprotectionschools.ie/en/Data-Protection-Guidelines/CCTV/Use-of-CCTV-Systems-in-Schools/>
* Government of South Africa, 2013. Protection of Personal Information Act, No. 4 2013. Available from [www.justice.gov.za](http://www.justice.gov.za)
* Information Commissioner’s Office, 2015. In the picture: A data protection code of practice for surveillance cameras and personal information. Available from [www.ico.org.uk](http://www.ico.org.uk)
* Michalsons [www.michalsons.co.za](http://www.michalsons.co.za)
* SAIDSA [www.saidsa.co.za](http://www.saidsa.co.za)
* University College London, 2010. CCTV policy statement. Available from [www.ucl.ac.uk](http://www.ucl.ac.uk)