SOUTH AFRICAN INTRUDER DETECTION SERVICES ASSOCIATION

BY-LAW NO. 9

Requirements for the installation of a CCTV System

September 2015

PREAMBLE

The purpose of this By-Law is to determine a minimum technical requirement for CCTV surveillance systems that will ensure the appropriate/sufficient quality images under different physical and environmental circumstances around residential and commercial sites for monitoring, detection, recognition and identification with the purpose of deterrence of potential perpetrators and the generation of video footage that will support investigations and successful prosecutions.

The compilation of this By-Law involved consultation between members of SAIDSA; experts in the field of CCTV, including amongst other accredited installers, retailers and manufacturers of CCTV equipment and other relevant sectors where required. Many local and world standards were referenced and included to assist in the compilation and application of this By-Law.

These minimum requirements for CCTV surveillance can be categorised as follows, and are dealt with separately under each heading:

-

1. Operational Requirement Analysis (OR)
2. Functional requirements
3. System management
4. Installation guidelines

Definitions

For the purpose of this By-Law, the following definitions apply:

CCTV System: System consisting of camera equipment, storage, monitoring and associated equipment for transmission and controlling purposes.
Surveillance: Observation or inspection of persons or premises for security purposes.
Operation Requirement (OR): A statement of needs based on a thorough and systematic assessment of the problems to be solved and the hoped for solutions.

1. **Operational Requirement Analysis (OR)**
The Operational Requirement analysis is a critical requirement when designing, testing and the operational effectiveness of the CCTV system.

The OR document clearly states:

1.1. **What problems need to be solved** – the user needs to assist in selection of observation purposes for each camera. These categories are to suggest appropriate image size to aim towards, so as to fulfill the specific observation requirement. The speed of target movement in the observation frame must be considered, as this affects frame rate of the events being observed. If the imagery is to be recorded, playback observation may be affected by compression technologies.

1.1.1 These observation categories are defined as follows:

1.1.1.1 **Monitoring and Control** – to oversee a large area or wide field of view;

1.1.1.2 **Detection** – to be alerted to the presence of activity in the field of view;

1.1.1.3 **Observation** – to be able to observe characteristics within a moderately sized field of view;

1.1.1.4 **Recognition** – to be able to identify a known person or object within the field of view;

1.1.1.5 **Identification** – to be able to clearly identify an unfamiliar individual or object within the field of view.

1.2 **Operational issues** – will suggest:

1.2.1 who will monitor the CCTV system;
1.2.2 when and where the CCTV system shall be monitored from;
1.2.3 how the events observed or generated will be handled.

The selections taken here will impact heavily on many of the system and management requirements of the CCTV system. A robust operating procedure is imperative for establishing integrity of evidence and dealing with legal challenges in court.

1.3 System requirements

1.3.1 What alert function must the system produce on event detected/triggered, i.e. audible, display, record, log, etc

1.3.2 Display of images, i.e. screen sizes, number of images per display, remote viewing, etc

1.3.3 Recording, i.e. storage media, retention periods, image quality, frame rates, compression technologies, metadata embedded into image, etc

1.3.4 Archiving & Exporting of data for permanent record, i.e. export/archive procedure, media & software needed to view images.

1.4 Management issues.

1.4.1 Constraints, i.e. licensing, regulations, public consultations, etc;

1.4.2 Legal issues, i.e. laws pertaining to Data Protection, Privacy, handling of data for evidentiary proceedings, etc;

1.4.3 Maintenance, i.e. of system equipment, warranties, upgrades, etc;

1.4.4 Resources, i.e. personnel to run system, service contracts, consumables, training costs, etc.

2 Functional requirements

2.1 Image Capture

All images that are captured shall have sufficient detail and accuracy to enable the user to extract sufficient information as defined in the operational requirement. This may include but is not limited to resolution, colour, size of displayed image and frame rate.

2.2 Image Handling

2.2.1 Presentation

The displayed image shall be the same as in the original image source. Any object masks, timestamps, camera names or camera numbers produced by the system shall not obscure the required image. This does not include privacy masks.

The following information shall be stated in the manufacturer's documentation with regard to presentation of images:

2.2.1.1 Monitoring device (e.g. Monitors, TV monitor, mobile devices, projector)
2.2.1.2 Maximum number of images displayed
2.2.1.3 Resolution
2.2.1.4 Frame rate
2.2.1.5 Response time

2.2.2 Storage

Where recording functions or storage are available in the system the following shall apply and must be stated in the manufacturer's documentation:

2.2.2.1 Any live display shall not influence the storing of video images
2.2.2.2 The system shall be able to be configured in such a way that the maximum storage time can be set.
2.2.2.3 The CCTV system shall be capable of automatically deleting images once they have been stored for the set period of time.

2.2.3 Image data backup / archiving

If storage or recording functions are available in the CCTV system, the following requirements apply:

2.2.3.1 It shall be possible to extract and preserve the image data for evidential or other purpose. A means of playing back the extracted image data shall be available without compromising the ability of the system to continue to function as designed.

2.2.3.2 If digital data is transferred to a secondary storage medium, then it shall be an identical copy of the original data and shall be called ´exact copy´.

2.2.3.3 A documented procedure should be written and followed, specific to each operational need requirement.

3. System management

3.1 Operation

User instructions shall be self-explanatory. Alarm situations shall be identifiable and accessible immediately with consistent documentation of the event.

3.2 Activity and information management

3.2.1.1 The system must be capable of distinguishing between user requested and event-driven data. Alarm data shall always be given priority over events.
3.2.1.2 The CCTV system shall be capable of indicating an alarm visually and audibly.
3.2.1.3 The CCTV system shall offer a means of alarm acknowledgement.

3**.2.2** For systems of security grades 3 and 4, on an alarm the CCTV system shall be able to display alarm information which should include:

3.2.2.1 alarm origin;
3.2.2.2 alarm type;
3.2.2.3 alarm time and date.

3.3 System Logs

The system must be capable of,

3.3.1 Maintaining accurate and complete system logs for a period of time defined in the Operational Requirement;
3.3.2 Presenting log data in a chronological order;
3.3.3 Preventing unauthorized editing or deletion of system logs;
3.3.4 Maintaining a log, that should contain each individual operator's activity.

3.4 System security

CCTV system security consists of system integrity and data integrity.

3.4.1 System integrity includes physical security of all system components and control of unauthorised access to the CCTV system. CCTV systems of security grades 2, 3 and 4 shall be capable of backup and restoral of all system data.
3.4.2 Data integrity refers to the prevention of unintentional changes to the CCTV system data.

3.5 System Integrity

3.5.1 Detection of failures

CCTV systems with a user interface, which is normally manned by an operator (either remote or local), alarm conditions from the specified components shall cause an alert. The failure shall be notified at any time that a new user logs in or the system restarts.

The information to be presented shall include:

4.5.1.1 Time and date;
4.5.1.2 Origin and type of failure.
Where the system provides for the facility to prioritize messages, then the priority level shall also be indicated.

3.5.2 Monitoring of power supply

The CCTV system shall be capable of,

3.5.2.1 Shutdown without loss of stored data;
3.5.2.2 Resuming normal operation after a power loss.

3.5.3 Monitoring of system functions and components

For security grades 3 and 4, the CCTV system shall manage device failure by indicating any failure of the essential functions.

3.5.4 Tamper protection and detection

3.5.4.1 The CCTV system shall be protected against tampering.
3.5.4.2 Where a tamper condition is detected, a tamper alarm must be generated and logged separately to an alarm condition or failure.

3.5.5 Protection against unauthorized access

3.5.5.1 **Access levels**

For each security grade of a CCTV system, there shall be several user authority access levels. These access levels govern privileges to the functions of the CCTV system.

3.5.5.1.1 **Level 1** - Any person - This level has no restriction on access.

3.5.5.1.2 **Level 2** - Any user - This level affects system operation, without configuration changes. Access may include password, key or code.

3.5.5.1.3 **Level 3** - System administrators -This level affects system configuration. Access may include password, key or code.

3.5.5.1.4 **Level 4** - Service personnel or manufacturer - Access to system design changes and maintenance. Access may include password, key or code

3.5.6 Authorisation

A CCTV system that implements user level authorisation shall be capable of,

3.5.6.1 Passwords of users shall be hidden, never be stored or displayed in an alpha or numerical format.

3.5.6.2 A password change by the user shall always require a valid user login.

3.5.6.3 Providing a method for data access to system logs and system setup according to the valid authorisation level granted to the user.

3.6 Image and data integrity

3.6.1 Data identification

3.6.1.1 The CCTV system shall provide methods to identify data in accordance with the applicable security grades.

3.6.1.2 The CCTV system shall always maintain the original data labels when data is exported.

3.6.2 Data authentication

In order to verify the integrity of images and data, grades 3 and 4 systems shall provide a method (e.g. watermarking, checksums, fingerprinting) to validate image and Metadata.

The validation method shall be applied to the recording and shall advise the user of the following:

3.6.2.1 Changes or alterations to images.

3.6.2.2 Images removed from a sequence;

3.6.2.3 Images added to a sequence;

3.6.2.4 Changes or alterations to data labels.

3.6.3 Data protection

CCTV systems of security grade 4, shall provide a method to,

3.6.3.1 prevent unauthorized viewing of the images and data;

3.6.3.2 Protect the confidentiality of copied and exported data.

3.7 Documentation

Documentation relating to a CCTV system shall be sufficient to,

3.7.1 Install;
3.7.2 Commission into operation;
3.7.3 Operate and maintain;
3.7.4 Procedures that need to be followed.
3.7.5 System specifications and block diagrams, including specification of configuration, shall be documented.

4. Installation Guidelines

4.1 Scene and illumination

4.1.1 The existing lighting should be evaluated for the level, direction and spectral content. Optimal light sources are those which have a spectrum that best matches the camera imaging device response. If additional lighting is required, the number, type, siting and power of the light sources should be determined taking the following parameters into consideration:
4.1.2 The new or additional light source selected should give acceptable pictures under all likely working conditions.
4.1.3 Illumination over the scene being surveyed should be as even as possible avoiding any area of very low light illumination. The ratio of maximum to minimum illumination within the covered area of any scene should ideally be 4: 1 or better.
4.1.4 Where possible lights should be mounted so that they do not impair the camera picture quality. The preferred position for the light is above the camera. The camera should not view the scene through intense beams of light.
4.1.5 Particular attention should be paid to the direction of illumination. The aim is to produce a maximum of contrast for intruder detection. An object can only be detected it its brightness is different to that of its background.
4.1.6 Prior to commencing work all relevant Safety Requirements should be considered. These will vary with the nature of the premises and may involve special installation equipment when working in hazardous areas.
4.1.7 Electric installation methods should comply with current national and site regulations and the installation should be carried out by technicians who are qualified to the appropriate level.

4.2 Cable installation

4.2.1 All cables to be of a type and size appropriate to the application and should take account of transmission rate, electrical interference and voltage drop.
4.2.2 Cable routes should be planned to provide the shortest practical distance between the equipment locations. Consideration should be given to the possibilities of future expansion of the system and any likely changes to the site.
4.2.3 When selecting cables consideration should be given to possible voltage drop and signal loss. Environmental, safety and security aspects should be taken into consideration and cables should be marked with the appropriate ratings.
4.2.4 When fiber optic cables are used, loss figures should allow for a minimum of three cable repairs during the life of the system. Bending radius should be within the manufacturer's specification.

4.2.5 Overhead cable runs should be avoided wherever possible. If this is not possible, the clearance height should allow for stretching of the support wire and fixings should comply to the current standard.

4.2.6 Where cables are installed in underground ducts, a draw wire should be left in the duct for maintenance purposes.

4.2.7 Protection should be provided for cables which are subject to mechanical damage or deliberate interference.

4.2.8 Cable wiring to camera equipment with pan and tilt units should remain sufficiently flexible over the full environmental temperature range.

4.2.9 Precautions should be taken during cable installation to ensure that moisture cannot penetrate; this is especially important, when using air spaced coax cables.

4.3 Hardware mounting

4.3.1 Fixings should be in accordance with the manufacturer's instructions. Environmental conditions may influence the choice of fixings.

4.3.2 Earthing should take into consideration the possibility of lightning strikes and electrical interference. On winch down and pivot types of masts, earth continuity must allow for the mechanical joints.

4.3.3 Camera and lens mounting arrangement should allow for the separation of video signal earth and housing and local safety earth.

4.3.4 All fixing positions should allow for mechanical stability, future access and safe working.

4.3.5 Planning considerations and architectural requirements should be taken into account.

4.3.6 Brackets and towers should be selected to support the maximum weight of the equipment and to provide sufficient rigidity for the camera equipment and other devices. As a general rule, the narrower the angle of view, the more rigid are the mounting requirements.

4.3.7 The rigidity of camera equipment fixings and the possibility of shock and vibration should also be taken into account.

4.3.8 Camera towers should preferably be of the winch down or pivot type and be positioned to provide safe access for service.

4.3.9 No equipment should be mounted near overhead high voltage cables.

4.3.10 All anti tamper devices should be employed where it is required.

4.3.11 Mounting equipment sighting should not compromise the overall security of the site.

4.3.12 Moving cameras should have sufficient clearance from adjacent objects.

The Following referenced standards and documents will assist in the application of this Bylaw:

EN 50132-1	**European Standard: Alarm systems** - CCTV surveillance systems for use in security application - March 2010
BSIA	**Planning, design, installation and operation of CCTV Surveillance Systems** - Code of Practice & associated Guidance - Feb 2014, Issue 3
SABS-0222-5-2:1999	**CCTV Installation Guidelines**
SANS 10222-5-1-2:2007	**Electrical security installations** - CCTV installations – CCTV surveillance systems for use in security applications: System design requirements
SANS 10222-5-1-1:2007	**Electrical security installations** - CCTV installations – CCTV surveillance systems for use in security applications: Operational requirements
SANS 10222-5-1-3:2007	**Electrical security installations** - CCTV installations – CCTV surveillance systems for use in security applications: Installation, planning and implementation requirements
SANS 10222-5-1-4:2003	**Electrical security installations** - CCTV installations – CCTV surveillance systems for use in security applications: Testing, commissioning and hand-over requirements
SANS 10222-5-1-5:2003	**Electrical security installations** - CCTV installations – CCTV surveillance systems for use in security applications: Maintenance requirements