

Somerset East District

CCTV SYSTEMS

WITHIN

LICENSED PREMISES

OPERATIONAL REQUIREMENT

GUIDANCE



		Page No
1	Introduction	3
2	What is an Operational Requirement	3
3	Equipment	5
4	Cameras	5
5	Monitors	7
6	Recording of Images	7
7	Digital Recording Images	7
8	Image Quality	8
9	Image Retention	8
10	Time and Date Stamp	8
11	Image Integrity	8
12	Security of Equipment	8
13	Lighting	9
14	Signage	9
15	CCTV and the Data Protection Act	10
16	Installation	10
17	Commissioning	10
18	Training/Management System	11
19	Service/Maintenance Support	11
20	Checklist – Camera Locations	12
21	Checklist – CCTV Operational Requirement	13
22	Data Protection Act 1998 - Compliance Advice	14
23	CCTV Small User Checklist	15

1 Introduction

Closed Circuit Television, commonly referred to as CCTV, is a rapidly developing technology. A correctly designed, installed and maintained system can be an effective tool in the potential prevention and detection of crime.

This document is intended to provide a **minimum** performance specification for the installation of a CCTV system, or the upgrade of an existing system, within licensed premises. The primary objectives of installing a CCTV system within such an environment are –

- To seek to influence behaviour of patrons.
- To protect staff and property.
- Where necessary, to provide unequivocal evidence of an incident to assist subsequent prosecution.

An effectively installed and managed system will also help to prevent criminal and anti-social behaviour.

Proposed CCTV installations for licensed premises must comply with the requirements of this guidance. A suitably qualified company should be engaged to design and install the system to ensure compliance - NSI Gold or SSAIB Certified.

A system specification will be supplied to the Licensing Authority.

The following guidance seeks to assist the reader in the procurement process. It provides a checklist of criteria which are required for the specification of an effective CCTV system and is, in part, based upon advice published by the Police Scientific Development Branch (PSDB).

2 Operational Requirement Analysis

What is an Operational Requirement?

“A statement of needs based on a thorough and systematic assessment of the problems to be solved and the hoped for solutions”.

In its simplest form an Operational Requirement (O.R) makes the reader ask a series of simple questions -

- Why am I installing a CCTV system?
- What do I want it to do?
- Where should I install cameras?
- How should I record the images?

The Police Scientific Development Branch advise the use of the Operational Requirement checklist methodology for a number of reasons including –

- It is relevant to any size of system – Town Centre to Corner Shop.
- It is relevant to any type of system – Analogue or Digital.
- It is relevant at any stage in the system's life – from initial concept to upgrade.
- It identifies the role that the CCTV system will play in the overall security strategy for the premises.

When a client contracts an installer to design a CCTV system the installer will require certain information to enable them to create the specification for an effective system. It is unlikely that the client will have sufficient technological knowledge to specify which equipment is required.

The use of an Operational Requirement approach simplifies the process and reduces the opportunities for confusion, which may lead to a non-complaint installation.

The Operational Requirement should answer the following questions –

Who and/or where is to be observed?

- Customers, Patrons and staff.
- Internal/External use

What activities are of concern?

- Incidence of disorder.
- Assaults.
- Theft of property.
- Damage to property.
- Dealing of drugs.
- Drug abuse.
- Suspicious actions.

Why are the activities being observed?

- To monitor behaviour.
- To recognise and identify offenders.
- To produce physical evidence of incidents, which may subsequently be used in Court?

Picture Quality

The quality of images recorded is of paramount importance. They should therefore -

- Clearly show actions of persons involved in an incident.
- Provide supporting evidence of identity of offenders.
- Show an overall view of the scene.
- Be time and date stamped.
- A basic Operational Requirement covering these points should enable the installer to specify an appropriate system.

3 Equipment

In its simplest format a CCTV system comprises of one or more cameras, a multiplexer, a monitor, and a means of recording images. If poorly specified, each item has the potential to reduce the image quality. To enable accurate identification from recorded images, the Police Scientific Development Branch recommends that the system should produce an image quality at the monitor of 450 TVL (television lines)

4 Cameras

Image quality is measured against the Rotakin Standard. The Rotakin target was developed by the Police Scientific Development Branch as a means of auditing the efficiency of a CCTV system. It consists of a human silhouette target 1.8m in height. When the target fills the screen it is said to be 100%R.

There are four image standards -

Category	Person Screen Height	Image Quality
Identify	100%	Sufficient picture quality and detail to identify an individual beyond reasonable doubt Must pass HOSDB 'Faces' test
Recognise	50%	Viewers can say with a high degree of certainty whether or not an individual shown is the same as someone they have seen before. Same recording quality setting as that used for Identify
Observe	25%	Some characteristic details of the individual, such as distinctive clothing can be seen. Must be able to distinguish between individuals
Detect	10%	Sufficient image size and quality to enable an observer to detect whether an individual is present

The quantity and location of cameras will be site specific. They must meet the requirements identified within the Operational Requirement procedure in accordance with BS.EN.50132.7. The cameras wide dynamic range must be operational 24 hours at all light levels, not disabled at low light - full colour.

All external public access doors must be fitted with colour cameras which enable clear, unobstructed images of all persons entering/exiting the premises. Where practicable, these cameras should be mounted internally.

These cameras must be capable of producing PSDB Identification standard images (a minimum of 400 TVL resolution and **100%** Rotakin screen target height) and monitor.

The exterior of all entrance/exits will be covered by cameras to a radius of 4 metres of that door capable of providing PSDB recognition standard images (a minimum of 400TVL resolution at **50%** Rotakin screen height) at the monitor.

All internal cameras must be capable of producing PSDB Recognition standard images (a minimum of 400 TVL resolutions at **25%** Rotakin screen target height) at the monitor.

CCTV cameras are susceptible to interference and vandalism. Cameras should be fitted with robust anti-tamper housing to prevent such actions.

All cameras must be a minimum standard of 400 TVL. They must have back light compensation, direct drive or amplification capability, and a sensitivity of a minimum of 4 lux.

5 **Monitors**

A colour monitor must be provided with the system to view live or recorded images. The monitor must not be located where it can be viewed by unauthorised personnel.

The monitor must be capable of producing minimum of 400 TVL processed images. Images displayed on monitors must not be visible from outside the premises.

Certain premises may be advised to install a "comfort" monitor in the vicinity of the external public access doorways(s). This monitor should display images produced by the camera covering the said doorway. It **must not** display images produced by any other camera located within the premises. Patrons entering the premises will be made aware of the fact that their images are being recorded by a CCTV system, enhancing the systems potential deterrent value.

6 Recording of Images

As established during the Operational Requirement process one of the main reasons for installing a CCTV system is to produce evidence, which may be used in Court in accordance with BS.8495. The images must therefore be recorded.

Images must be recorded onto the hard-drive of a digital recorder.

7 Digital Recording Systems

The video format utilised must be PAL or PAL/NTSC.

The system must incorporate sufficient build-in hard-drive capacity to suit the number of cameras installed. The system must record at a minimum of **6 frames per second (fps) on all cameras within the premises, however, cameras covering entrance doors must record at 12fps** (*real time equals 25 frames per second so this would record/capture 20% of action*). This can be achieved either by total capacity of the hard-drive or where appropriate, by event controlled recordings, ie alarm activated or motion activated.

The system must have duplex multiplexing facility or greater, to allow for simultaneous image recording and playback. There must be no interruption in recording during the playback process.

The system must incorporate a means of transferring images from the hard-drive to a format that can be played back on any windows compatible computer.

The image file should therefore be transferred to a WORM (Write Once Read Many Times) media such as CD-R disc. CD-R must be "finalised" or "closed" in the CD-writer before the disc is removed, otherwise the image file may not be viewable.

The system must produce images, which are watermarked as part of the original recording process. There must be no subsequent watermarking of images (ie at the time of transfer to removable media).

The application software required to launch and view recorded images must be either included as part of a standard Microsoft operating system installation or be installed to the recorded media when the data is copied to that media.

The quality of the copied data must be of a high resolution as defined by the PC industry standards, eg 1024 x 768.

The Digital Multiplexer must have the facility to be password protected.

8 Image Quality

The image quality setting of recorded images must be set to the operational requirement rather than to minimise the storage capacity. The system must be capable of producing images to the PSDB Identification and Recognition standards.

The compression standard should be H.263 or H.264, JPEG or MPEG4. The high resolution images should not be heavily compressed therefore providing poor quality playback images.

9 Image Retention

Systems are often set to over-record images after a set period of time. The system should be capable of recording and retaining **31** days of images before over-recording.

10 Time and Date Stamp

Digital recording equipment must record time and date information as part of the image file. The time/date must be accurate.

11 Image Integrity

The integrity of images removed from a hard-drive for evidential purposes is vital. They must be protected at the earliest opportunity to reduce opportunities for challenges in Court. Designating the image as read only can prevent alteration or erasure.

12 Security of Equipment

The monitor and recording equipment should be located in a secure room. Where this is not practicable, the recording equipment must be stored in a **secure** cabinet to prevent unauthorised access, tampering, or removal of images.

13 Lighting

When lighting premises, consideration must be taken into account regarding the following factors, which will dramatically reduce the quality of images recorded –

- Excessive shadows.
- Glare into the lens.
- Back-lighting.
- External lighting.
- Impact of rapid changes in light levels from ‘Disco lighting’, lasers etc

Steps must be taken to eliminate or reduce the impact of such factors.

Particular attention must be given to lighting in the area of public access doors. The lighting must produce “white light” to enable clear images and accurate colour retention.

The fields of view of **all** cameras must be sufficiently well lit to enable them to operate as required under normal working conditions.

14 Signage

Each system installed must include appropriate signage.

The Data Protection Act 1998 requires that signage around the area where CCTV is being used be erected.

The signs should be placed in the proximity of the cameras so that anyone entering a camera zone will be aware that they are entering an observed area. Advice from the Data Protection Commissioner is that signs should be at least A3 size with wording to identify the person or organisation responsible for the scheme, the purpose of the scheme and who to contact regarding complaints about the scheme.

For example –



15 CCTV and the Data Protection Act 1998

All aspects of the CCTV system must comply with the Data Protection Act 1998 and registered with the Information Commissioners Office (ICO) at www.ico.gov.uk . The Office of the Data Protection Supervisor has produced guidance in relation to how the Act should be interpreted, including advice on the required signage. For further information please contact - www.dataprotection.gov.uk

16 Installation

All electrical installation works must be carried out to 17th Edition IEE Wiring Regulations BS7671: 2008. A Minor Works certificate for design, construction, inspection and testing must be provided before completion. The contractor will need to satisfy themselves that existing electrical circuits comply with the current 17th edition electrical regulations before commencing the installation.

17 Commissioning

The complete system must be fully tested, and commissioned in the presence of a representative of the client. The purpose of this test is to determine whether or not the cameras cover the required areas, and if they are capable of providing images to the required standards. An acceptable certificate will need to be signed to prove the installation meets the specification defined.

18 Training/Systems Management

As part of the commissioning procedure, the installer must train the client, or the client's representative, to operate the system and associated equipment effectively. The training must include details of the client's responsibilities in relation to the effective maintenance and management of the system, the provision of user manuals, all relevant handbooks, and technical data. A full workshop manual should be provided.

A separate operator's manual should be provided for system users.

The Client must appoint a trained Data controller who will be responsible for the general administration, operation, maintenance and supervision of the system.

All users must be fully trained in the operation of the system and be made aware of their general legal responsibilities, at all times of operation of the premises there must be a competent person present on the premises capable of replay and export of

recordings quickly onto a removable storage medium. Only VHS tape, CD or DVD will be acceptable, the export method must be proportionate to the storage capacity and pictures should be exported in the native file format at the same quality that they were stored on the system in accordance with BS.8495. This master copy will be available at the time on request of an investigating officer.

An operations manual and code of practice must be provided to cover staff training, fault reporting, maintenance management and evidence handling procedures. The management section should identify the person responsible for the system and daily checking.

19 Service/Management Support

The system must be regularly serviced by qualified operatives to maintain the quality of images recorded; the system must be “fit for purpose”. A record will be kept of all faults, any fault will be “returned to service” within 7 days.

Where any investigating agency becomes aware of three faults within a rolling 12 month period, the system operator will be warned. Where five faults occur within a 12 month rolling period, the matter will be brought to the attention of the licensing authority for breach of conditions attached to the licence.

Each system installed will require a maintenance contract.

CCTV – Camera Locations	
All licensed areas must be covered by CCTV.	
The location of cameras is as important as ensuring that the CCTV System installed is of a high standard. Please see the checkpoint areas listed below for camera locations -	
Entrances/exits and lobby areas	
Pavement area immediately outside entrances of premises	
Corridors to toilet facilities	
Designated Drug Search areas inside premises	
Vending Machines/Gaming Machines	
Gaming areas, ie pool tables	
Bar areas	
Corridor areas	
Internal public areas	
Car Parks	
Beer Gardens/Patio areas	
Security offices (safes)	
Storerooms	
Entrances to living quarters	
Delivery areas	

Camera locations may be specified at the discretion of the Avon & Somerset Police / South Somerset District Council / Mendip Council –

- *Licensing Officer*
- *Community Safety Officer / Crime Reduction Officer*
- *Architectural Liaison Officer*

In respect of any new applications, variations (excluding minor) and premise licence reviews.

Whilst all surveys, reports and recommendations prepared by the Avon and Somerset Constabulary are believed to be accurate and reliable, they are prepared on a voluntary basis without charge. You should note that the Chief Constable, the Avon and Somerset Police Authority and the Home Office will not accept any liability whatsoever, in contract tort (including negligence and breach of statutory duty) or otherwise for any loss, apparatus or materials recommended being found unsuitable, inadequate or defective.

The total elimination of crime cannot of course be guaranteed and in any event is the responsibility of the criminal. However, the range of options mentioned, if implemented, should reduce the opportunity for a crime to be committed.

Crime reduction strategies should be re-assessed on a regular basis.

CCTV OPERATIONAL REQUIREMENT CHECKLIST

1 Name of Premises

2 Date

3 Sheet No

4 Location within premises

Doorway

Corridor

Room

Other

5 Who/What/Where is to be observed?

6 Which activity is to be observed?

7 Why is the activity being observed?

8 Likelihood of an activity occurring - frequency

High

Medium

Low

9 Picture quality achieved

10% R Detect

25% R Observe

50%R Recognition

100% R Identification

10 Lighting conditions

Natural

Light

Artificial Light

Both

11 White Light Requirement

(Public Access Doorway)

Yes

No

12 Additional comments/Notes

*** A CHECKLIST SHOULD BE USED FOR EACH CAMERA OR LOCATION
WITHIN THE PREMISES. PLEASE TICK APPROPRIATE BOXES**

Data Protection Act 1998

Compliance Advice

CCTV Small User Checklist

Introduction

This checklist is designed to help operators of small CCTV systems comply with the legal requirements of the Data Protection Act 1998, and it details the main issues that need to be addressed when operating a CCTV system. When used as part of a regular review process it should help to ensure that the CCTV system remains compliant with the requirements of the Act. Compliance is the duty of the owner/operator

It is important that the Data Protection Act is complied with because failure to do so may result in action being taken under this Act. Failure to comply with Data Protection requirements will also affect the police's ability to use the CCTV images to investigate a crime and may hamper the prosecution of offenders.

If you use a CCTV system in connection with your business you should work through the checklist and address all points listed. This will help you to ensure that your CCTV system remains within the law and that images can be used by the police to investigate crime.

www.dataprotection.gov.uk
data@dataprotection.gov.uk

Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire.
SK9 5AF

Tel No 0303 123 1113

Fax 01625 524510

CCTV Small User Checklist

Operation of the CCTV System

This CCTV equipment and the images recorded by it are controlled by _____ who is responsible for how the system is used and for the notifying of the Information Commissioner about the CCTV system and its purpose (this is a legal requirement of the Data Protection Act 1998).

The above controller has considered the need for using a CCTV system and has decided it is required for the prevention and detection of crime and for protecting the safety of customers. It will not be used for other purposes.

	Checked / Date	By	Date of Next Review
The controller is aware that notification to the Information Commissioner is necessary and must be renewed annually			
Notification has been submitted to the Information Commissioner and the next renewal date recorded			
Cameras have been sited so that their images are clear enough to allow police to use them to investigate a crime			
Cameras have been positioned to avoid capturing the images of persons not visiting the premises			
There are signs showing a CCTV system is in operation visible to people visiting the premises and the controllers contact details are displayed on the sign where it is not obvious who is responsible for the system			
The recorded images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them			
The recorded images will only be retained long enough for any incidents to come to light (eg for a theft to be noticed)			
Recordings will only be made available to law enforcement agencies involved in the prevention and detection of crime, and no other third parties			
The operating equipment is regularly checked to ensure that it is working properly (eg the recording media used is of an appropriate standard and that features on the equipment such as the date and time stamp are correctly set)			
The controller knows how to respond to requests from individuals for access to images relating to that individual. If unsure the controller knows to seek advice from the Information Commissioner as soon as such a request is made			

Please keep this checklist in a safe place until the date of the next review