

Somerset Policing District
SURVEILLANCE CAMERA SYSTEMS
WITHIN
LICENSED PREMISES
OPERATIONAL REQUIREMENT
GUIDANCE



Amended 12/07/2018
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	8
7	Digital Recording Images	8
8	Image Quality	9
9	Image Retention	9
10	Time and Date Stamp	9
11	Image Integrity	9
12	Security of Equipment	9
13	Lighting	9
14	Signage	10
15	Systems and the Data Protection Act	10
16	Installation	11
17	Commissioning	11
18	Training/Management System	11
19	Service/Maintenance Support	12
20	Checklist – Camera Locations	13
21	Checklist – Operational Requirement	14
22	Data Protection Act 2018 - Compliance Advice	15
23	Small User Checklist	16

1 Introduction

Closed Circuit Television, commonly referred to as CCTV, whilst still popular, the term is no longer accurate. Industry standards often use the term video surveillance system (VSS) in preference to CCTV. In this guide, we have used the term surveillance camera system (or “system” for short). A surveillance camera system includes the cameras and all the related hardware and software for transmitting,

processing and storing the data which is captured. 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 system, or the upgrade of an existing system, within licensed premises. The primary objectives of installing a 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 system 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.

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 surveillance system and is, in part, based upon advice published by the Home Office Centre for Applied Science and Technology (CAST) (formally the Home Office Scientific Development Branch (HOSDB)).

There is a requirement for those operating surveillance systems that meet these minimum standards to ensure suitable auditing procedures for the retention of recorded images and that there is a requirement for any surveillance evidence requested by police to be provided

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 surveillance system?
- What do I want it to do?
- Where should I install cameras?
- How should I record the images?

The Home Office Centre For Applied Science and Technology 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 surveillance system will play in the overall security strategy for the premises.

When a client contracts an installer to design a surveillance 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, surveillance systems comprise 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 Human Identification Test developed by the Centre for Applied Science and Technology as a means of auditing the efficiency of a surveillance system.

Human identification test

The purpose of this test is to help system commissioners and auditors to demonstrate the system under review is capable of providing images that can be identified.

The test consists of nine human faces. A random selection is presented to the camera at an appropriate distance. An operator attempts to match the presented face to a reference list. The operator's accuracy is then scored and used to evaluate the capability of the system to record identifiable images at this distance.

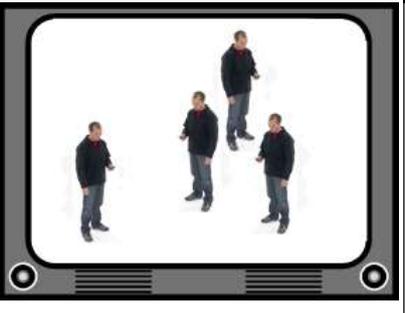
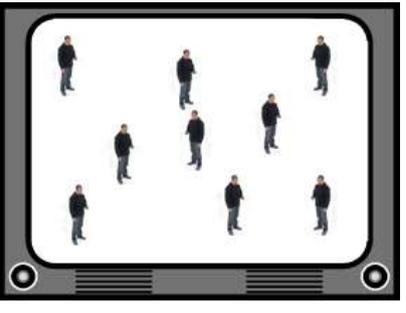
Vehicle registration number (VRN) legibility test

The purpose of this test is to evaluate whether a system can provide images suitable for reading a VRN. The test kit specifies nine segments of VRN characters. A random selection of these segments is shown to the camera at an appropriate distance. An operator attempts to match the presented VRN to a reference list and their accuracy is scored.

Colour rendition test

This test will help to establish whether a surveillance system can provide images with reasonably accurate colour information. The test kit includes a basic colour chart which is presented towards the camera at a suitable distance. The operator can then verify the level of match between the colours on a reference chart and the colours seen through the imaging system.

There are three image standards -

		
<p>Identify 4 mm per pixel or 250 pixels per metre or 100% of the available screen height or 40% Full HD screen height</p>	<p>Recognise 8 mm per pixel or 125 pixels per metre or 50% of the available screen height or 20% Full HD screen height</p>	<p>Observe 16 mm per pixel or 62.5 pixels per metre or 25% of the available screen height or 10% Full HD screen height</p>
<p>Sufficient picture quality and detail to identify an individual beyond reasonable doubt. Must pass HOSDB 'Faces' test.</p>	<p>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.</p>	<p>Some characteristic details of the individual, such as distinctive clothing can be seen. Must be able to distinguish between individuals.</p>
<p>Screen height is how much space vertically a 1.7m tall figure would occupy, as shown in the diagram above.</p>		

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.

In the case of licensed premises, shops & supermarkets; 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 CAST Identification standard images (a minimum of 400 TVL resolutions and **100%** screen target height) and monitor.

In particular cases of licensed premises; The exterior of all entrance/exits will be covered by cameras to a radius of 4 metres of that door capable of providing CAST recognition standard images (a minimum of 400TVL resolution at **100%** screen height) at the monitor.

All internal cameras must be capable of producing CAST Recognition standard images (a minimum of 400 TVL resolutions at **50%** screen target height) at the monitor.

For further information regarding this test please see contact details below

Video team
The Centre for Applied Science and Technology
Woodcock Hill
Sandridge
St Albans
Hertfordshire
AL4 9HQ

email: castenquiries@homeoffice.gsi.gov.uk
switchboard: (+44) (0)1727 865051
fax: (+44) (0)1727 816233

Cameras can be susceptible to interference and vandalism. Cameras should be fitted with robust anti-tamper housing to prevent such actions if they are vulnerable.

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.

With advances in Internet Protocol (IP) cameras, ensure adequate security measures are in place to prevent unauthorised web access.

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 if using older analogue equipment or LED (light emitting diode) a more modern and lower power consumption technology used in flat screen displays. 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 surveillance 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 surveillance 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 50% 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 CAST 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 2018 requires that signage around the area where surveillance 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 Information 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 **Surveillance Systems and the Data Protection Act 2018**

All aspects of the system must comply with the Data Protection Act 2018 and registered with the Information Commissioners Office (ICO) at ICO.org.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 – Data protection - 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 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.

Camera Locations	
All licensed areas must be covered by surveillance system.	
The location of cameras is as important as ensuring that the 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/ Sedgemoor District Council/ Taunton Deane Borough Council/ West Somerset Council –

- *Licensing Officer*
- *Crime Reduction Officer*
- *Crime Prevention Design Advisor*

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.

SURVEILLANCE SYSTEM 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			
	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				

General Data Protection Regulation (GDPR) & Data Protection Act 2018

Compliance Advice

Small User Checklist

Introduction

This checklist is designed to help operators of small systems comply with the legal requirements of the General Data Protection Regulation Act 2018 and the

Data Protection Act 2018; it details the main issues that need to be addressed when operating a surveillance system. When used as part of a regular review process it should help to ensure that the system remains compliant with the requirements of the Act. Compliance is the duty of the owner/operator

It is important that the General Data Protection Regulation 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 surveillance images to investigate a crime and may hamper the prosecution of offenders.

If you use a 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 system remains within the law and that images can be used by the police to investigate crime.

**Small User Checklist
Operation of the Surveillance System**

This surveillance system 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 system and its purpose (this is a legal requirement of the Data Protection Act 2018).

The above controller has considered the need for using a surveillance system and has decided it is required for the prevention and detection of crime and for protecting the safety of staff/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 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 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