Office of
Crime Prevention

WESTERN AUSTRALIA

Closed Circuit Television (CCTV) Technical Advice

CONTENTS

1 INTRODUCTION

Since the introduction of Closed Circuit Television (CCTV) as a means of addressing crime and security concerns within communities, the popularity and use of this technology has rapidly increased. Countless systems have been installed in an ever increasing range of locations for the purpose of reducing the likelihood that the location will be the subject of criminal activity and anti-social behaviour.

... this advice provides a 'starting point' upon which specific technical decisions can be based.

However, CCTV can be expensive to implement, manage and maintain, and as it is an application specific technology, poorly designed systems or systems installed for the wrong purposes may be ineffective and expensive to correct.

This document has been developed by a panel of industry experts to provide advice and support to potential owners and users of CCTV. It has been developed to assist those individuals with little or no technical experience in the implementation or use of CCTV.

The document outlines a set of suggested system requirements and technical considerations that CCTV owners and users may seek to apply within their own systems. As CCTV system design must be based on the findings of a properly undertaken risk assessment as well as location and owner or user needs, this advice provides a 'starting point' upon which specific technical decisions can be based.

Similarly, given that the definitive test for determining the successful technical installation of a CCTV system is the extent to which the images displayed on the system's monitor in live view mode and in playback mode meet the identified needs of the CCTV owner, the specific technical advice provided within this document is intended to act only as a set of 'guide-posts' to assist CCTV owners and users meet this ultimate outcome.

The technical advice within this document addresses suggested technical considerations for a range of CCTV system sizes and common purposes including private use, use within small businesses and the retail sector, use within semi-public spaces such as schools, hospitals and licensed premises and CCTV use within public spaces.

It is important to note that the technical advice has been developed for security purposes rather than occupational health and safety or alternative workplace purposes. As such, it is intended to support the Western Australia Closed Circuit Television (CCTV) Guidelines. CCTV owners and users reading this technical advice should also read the Western Australia Closed Circuit Television (CCTV) Guidelines.

This technical advice is not able or intended to provide a means of selecting the most suitable CCTV system for a particular user or application. Owners of CCTV systems should determine their own objectives and risks and where appropriate engage qualified and licensed CCTV consultants and installers in order to select and operate an appropriate system.

The WA Police – Office of Crime Prevention can not provide legal interpretation of legislation relating to CCTV and content within this technical advice should not be viewed as such. The WA Police – Office of Crime Prevention recommends that organisations employing CCTV should seek legal advice to ensure compliance with Western Australian and Commonwealth legislation.

2 GLOSSARY

Angle of View. The angular range that can be focused within the image size. Small focal lengths give a wide angle of view, and large focal lengths give a narrow angle of view. Sometimes referred to as Field of View.

Bandwidth. The number of cycles per second (Hertz) expressing the difference between the lower and upper limiting frequencies of a frequency band; also, the width of a band of frequencies.

Bitmap (BMP). A pixel-by-pixel description of an image. Each pixel is a separate element. Also a computer file format.

Closed-circuit television (CCTV). The use of video cameras to transmit a signal to a specific place, on a limited set of monitors.

CODEC. A codec is a device or computer program capable of encoding and/or decoding a digital data stream or signal. The word codec is a portmanteau (a blending of two or more words) of 'compressor-decompressor' or, more accurately, 'coder-decoder'.

Colour Rendition. The quality of the reproduction of colours under a given illumination.

Common Intermediate Format (CIF). Also known as FCIF (Full Common Intermediate Format), is a format used to standardize the horizontal and vertical resolutions in pixels of YCbCr sequences in video signals. Terms also used are 2CIF (2 x CIF) and 4CIF (4 x CIF).

Compression. The reduction in gain at one level of a picture signal with respect to the gain at another level of the same signal.

Contrast. The range of light to dark values in a picture or the ratio between the maximum and minimum brightness values.

Data Transmission. The physical transfer of data (a digital bit stream) over a point-to-point or point-to-multipoint transmission medium.

Definition. The fidelity of a television system to the original scene.

Extra Low Voltage (ELV). Alternating current (AC) voltage less than 50V, or direct current (DC) voltage less than 120V.

Field of View (FOV). The maximum angle of view that can be seen through a lens or optical instrument.

Frames per second (fps). Is the frequency (rate) at which an imaging device produces unique consecutive images called frames.

H.264. Also known as MPEG-4 AVC is a standard for video compression.

Infra Red (IR). Is a wavelength of light which is above the visible light spectrum and is used for discrete illumination in CCTV systems.

Joint Photographic Experts Group (JPEG). A group that has recommended a compression algorithm for still digital images that can compress with ratios of over 10:1. Also the name of the format itself.

Light. Electromagnetic radiation detectable by the eye, ranging in wavelength from about 400 to 750 nm.

Lux (lx). Light unit for measuring illumination. It is defined as the illumination of a surface when luminous flux of 1 lumen falls on an area of 1 m^2. It is also known as lumen per square meter, or meter-candelas.

Motion JPEG (M-JPEG). An informal name for a class of video formats where each video frame or interlaced field of a digital video sequence is separately compressed as a JPEG image.

MPEG-4. A patented collection of methods for the compression of audio and visual digital data.

CCTV
For your personal safety and security CCTV cameras are in constant operation
Evidence can be used in a Court of Law

Open Application Programming Interface (Open API). This describes sets of technologies that enable websites to interact with each other by using SOAP, Javascript and other web technologies.

Open Network Video Interface Forum (ONVIF). A global and open industry forum that is facilitating the development and use of a global open standard for the interface of network video products.

Pixel. Short for 'picture element'. A pixel is the smallest area of a television picture capable of being delineated by an electrical signal passed through the system of part thereof. The number of picture elements (pixels) in a complete picture, and their geometric characteristics of vertical height and horizontal width, provide information on the total amount of detail which the raster can display and on the sharpness of the detail.

Physical Security Interoperability Alliance (PSIA). A global consortium of physical security manufacturers and systems integrators focused on promoting interoperability of IP enabled security devices across all segments of the security community.

PTZ camera. Pan, tilt and zoom camera.

Resolution. A measure of the ability of a camera or television system to reproduce detail. The number of picture elements that can be reproduced with good definition.

Uninterruptible Power Supply (UPS). A power supply that is used to maintain power in the event of a power outage.

Video analytics or Video motion detection. A process of determining motion by complicated electronic analysis of picture signal and or neural computing techniques.

Video monitor or Video display. A device for converting a video signal into an image.

Video signal. An electrical signal containing all of the elements of the image produced by a camera or any other source of video information.

Zoom lens. A camera lens that can vary the focal length while keeping the object in focus, giving an impression of coming closer to or going away from an object.

3 POLICY AND MANAGEMENT

Policy, management and procedural considerations are important factors in the successful implementation of CCTV. Owners and managers of CCTV systems, or at the very least those employing CCTV in a commercial context, should ensure that formal, written documentation outlining the overarching policies, procedures, and responsibilities related to the use of the CCTV system is developed and maintained. Formal policies should, at a minimum, address the following:

- Roles and responsibilities;
- Data access and data sharing;
- Data integrity and continuity of evidence;
- Code of practice and penalties for non-compliance;
- Signage;
- Security requirements for the CCTV infrastructure;
- Compliance with legislation;
- Training;
- Use of equipment;
- Storage of information;
- System minimum standards;
- Complaints handling; and
- Audit and review processes.

Further information on the development and implementation of formal policies and procedures can be obtained within the Western Australia Closed Circuit Television (CCTV) Guidelines.

The Western Australia Police – Office of Crime Prevention, in partnership with the State CCTV Working Group has produced a range of policy and standard operating procedure templates for CCTV owners. These templates can be obtained by contacting the Office of Crime Prevention on (08) 9222 9733 or www.crimeprevention.wa.gov.au.

4 CABLING PLATFORMS

CCTV signals can also be transmitted via wireless network connection, microwave and laser light.

An important and often overlooked factor in the development and implementation of CCTV is the cabling required for the transmission of CCTV signals to the digital recording device or control room. Often CCTV owners will seek to install CCTV without due consideration being given to the location and system's cabling needs. As cabling infrastructure can be expensive to install, it is imperative that CCTV owners obtain the correct cabling for their desired system.

A range of cabling platforms are available for the delivery of CCTV signals. These usually include coaxial cabling, fibre optic cabling or Ethernet. However CCTV signals can also be transmitted via wireless network connection, microwave and laser light.

To ensure that the appropriate cabling infrastructure is obtained, the CCTV owner should obtain a full survey on existing cabling infrastructure, and cabling needs based on the owner's proposed system. This work should be undertaken by a communications cabling company or a licensed security installation company with appropriate CCTV experience.

The Office of Crime Prevention in partnership with the State CCTV Working Group has developed the General Overview on Developing Strategies Relating to Closed Circuit Television (CCTV) Migration from Analogue to Digital (IP) CCTV Systems. This document provides some general information on cabling platforms and typologies. Further information on cabling platforms can be obtained by consulting this document. Copies can be obtained by contacting the Office of Crime Prevention on (08) 9222 9733 or www.crimeprevention.wa.gov.au.

5 POWER CONSIDERATIONS

All CCTV cameras require a power supply; these are usually:

- 12 volts DC
- 24 volts AC
- 240 volts AC
- POE (Power over Ethernet)

Most internal cameras are rated at ELV either 12 Volts DC or 24V AC.

This allows for the power supplies to be remotely located away from the camera and to have a back-up power supply attached, usually an Uninterruptible Power Supply (UPS).

12 volts DC / 24 volts AC

CCTV cameras using 12V DC or 24V AC as their power source are the most common types of CCTV units installed today. When selecting these cameras for a particular installation the following criteria need to be taken in to account:

- The electrical current draw of each camera and the impedance of the cable reticulation for the designated feed.
- If more than 1 camera is to be powered from a common power feed, the aggregate current draw from each camera along with the impedance of the cable reticulation for the designated feed.
- The use of filtered regulated power supplies that are of the correct rating to suit the load of the connected cameras. It is recommended that a 25% overhead be allowed when calculating the power supply requirements to cater for future cable degradation.

12V DC

The use of line locked cameras with Positive and Negative power inputs is standardised so they are installed in the correct polarity power inputs on each device.

Allowance:

500MA per Full Body or Dome Camera (Non IR)

2.5A – 3A for a Pan Tilt Zoom Camera

Incorporation of an External Sync Generator is recommended to minimise roll aspects when switching between cameras connected to viewing device.

24V AC

The use of line locked cameras with Active and Neutral power inputs is standardised so they are installed in the same power inputs on each device to ensure power synchronisation.

Allowance:

250MA per Full Body or Dome Camera (Non IR)

2.5A – 3A for a Pan Tilt Zoom Camera

240 volts AC

240 Volt cameras must be installed by persons that are qualified to work in that environment.

POE (Power over Ethernet)

With the introduction of Internet Protocol (IP) based cameras, CCTV systems are able to take advantage of Power Over Ethernet or POE. Through the use of POE enabled switches, camera vision and power is delivered through the network cable plugged in to the rear of the camera.

Care should be taken to ensure that:

- The rating of the selected POE switch delivers sufficient power for camera operation. Minimum output per switch output should be in the order of 500ma per switch channel (Typically Non PTZ or Infra Red) for full body or Dome Cameras.
- The current draw of the camera does not exceed the rating of the POE switch.

When using IP Cameras or POE infrastructure do not operate the camera more than 90 meters from the POE rated switch.

As this system uses the IT infrastructure to deliver the signal to the control and recording equipment the use of UPS is recommended for all equipment between the camera and recording device to cater for power disruptions.

Since the 3rd of October 2003, a security installer must conform to the Cabling Provider Rules contained within the *Telecommunications Act 1997* (Cth), which states that a Cabler must hold, as a minimum, a Restricted Registration before they can carry out cabling behind a compliant device in a domestic or commercial installation.

Any cabling work carried out that is considered ELV and is connected to a device that has the potential to be connected to the telecommunications network i.e. CCTV DVR, encoder or camera with provision for a remote connection, or a group of computers/devices connected together as a Local Area Network that may or may not be connected to the internet must also be carried out by a registered Cabler.

6 TECHNICAL ADVICE

The following technical advice identifies suggested technical considerations for a range of CCTV system sizes and common purposes. The technical advice is set out within matrices which identify common areas of technical concern and the corresponding advice, highlighting a suggested response for achieving effective use of CCTV for the purpose identified.

6.1 Public Spaces

Closed Circuit Television in public spaces has been the subject of a wide range of documentation, both within Australia and internationally. This documentation has been aimed at achieving the best and most effective use of the technology within the public realm.

The technical advice contained within S6.1 is based on the implementation of CCTV within spaces such as open air car-parks and open streets. It must be stressed that due to the application specific nature of CCTV, the following provides only general advice relating to the technical considerations relevant to the use of CCTV within public spaces.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Cameras	A range of camera types may be utilised for this application. These include: • Monochrome (black & white) • Colour • Day/Night (combines colour and monochrome) Monochrome cameras generally offer higher resolution and are relatively inexpensive, but are mostly used only in extremely low lighting conditions. Colour cameras generally offer a better overall representation of the scene (subject to adequate lighting) as well as higher identification capabilities. Day/night cameras combine the advantages of monochrome and colour cameras. They are much more sensitive to low light environments and are also able to be used with infra red lighting. Cameras also have basic functionality types including: • PTZ – Pan, tilt, zoom (where the camera may controlled along the horizontal and vertical planes and may zoom in and out on an object. • Fixed (the camera is pointed at a fixed spot and does not allow for control of movement). • IP (internet protocol cameras – cameras which interface directly with a computer network). Cameras may also contribute to the quality of images through the type, size and sensitivity of the image sensor contained within the camera as well as the compression algorithm applied within the camera. Lenses should match the format of the selected camera's image sensor and be of such a design that presence of Infra Red should not affect the sharpness of the image or focal point.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Light Levels and Placement	Balanced white lighting with levels sufficient to allow for identification of individuals. Lighting levels should be at a minimum of 40-60 Lux. Lights should create intersecting cones of illumination and be placed to prevent shadows and dark spots. Lights should be located behind the camera to avoid backlighting of the target and should not be placed within the field of view to avoid glare. For further information refer to Australian Standard S1.3.43 AS4806.2: 2006.
Colour Rendition	Colour rendition depends on the type and level of lighting within the scene. White light is best to achieve good colour rendition. Florescent lights or metal halide lighting is preferable. Avoid colour lighting such as low pressure sodium (yellow) lighting in camera areas. Where possible, consider the use of energy efficient lighting, however, this should not be to the detriment of system operation.
Scene Contrast	Consideration should be given to the effect of reflective surfaces (lights/sun reflecting off windows or other reflective surfaces) on image capture. In areas of widely varying lighting levels such as entry doors consideration should be given to the installation of day/night wide dynamic cameras. IR (infra red) flood lights may be considered for illuminating dark areas. However, IR reflects differently off a range of materials and has a tendency to 'wash-out' faces. This has implications for identification of individuals and therefore the use of IR flood lights are not recommended for use with cameras which have been installed for the purpose of obtaining identifying information unless a scene test has been carried out to verify results.
Fields of View	The CCTV system should be developed based on the findings of a risk assessment. Each FOV should therefore reflect the purpose and objectives of the entire system. In addition, the purpose and objectives of each camera/location within system should be specified and documented within a duty statement. Each camera/location should have its own documented duty statement. The system (including camera placement and FOV) should be designed and used to compliment other security operations.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Fields of View (continued)	Insofar as the FOV meets the documented objectives of the entire CCTV system, FOVs to be considered may include: • higher camera/wide angle for viewing detecting movement and activities within a large area; • vehicle entrances and exits from car parks; stairs; • elevators; and • pedestrian entry/exits. FOV should avoid 'tops of heads' shots, distances or angles of view which make detection or identification problematic (refer to S3.7 AS4806.2:2006 for relevant object/screen size ratio). Consideration should be given to the use of pre-determined camera duty cycles (FOV pathways or locations pre-programmed into camera operation). The choice of camera type (monochrome, colour, day/night, fixed or PTZ) must be reflected in the objectives of the system and the purpose for which each camera is installed. Vandal and weather proof dome cameras are most appropriate to ensure camera security, however system owners may wish to consider other forms of vandalism/theft prevention. Any internal cameras should be positioned at a height of 1800mm-2400mm. External cameras may need to be positioned higher, however, placement height should not impede the camera's ability to capture identifying information. FOV should be tested in the desired resolution by playing back stored images from the recording device to ensure that the level of detail that is captured is not adversely affected by a FOV setting. i.e. one that may prevent the capture of the required level of detail through covering too wide an area, for example. FOV should not include areas where private activities (as defined within the *Surveillance Devices Act 1998 WA* – See WA Closed Circuit Television (CCTV) Guidelines for further information) may be observed. E.g. neighbouring properties, changing rooms, toilets, etc. System owners should consider masking areas of FOV that are not owned or managed by the system owner or where private activities may take place. **Masking involves the use of software within the camera or recording device to obscure areas within the camera's FOV as defined by the user, so that these areas are not viewed or recorded by the system.**

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Image Resolution	Image resolution requirements should be based on the findings of a risk assessment and the system's stated objectives. To detect activity within a FOV, systems should record at a minimum resolution of 4CIF (704 x 576 TV Lines) at a rate of 10 frames per second. To recognise actions (what is happening) within a FOV systems should record at a minimum resolution of 4CIF (704 x 576 TV Lines) at a rate 12.5 - 15 frames per second. To identify individuals or vehicles within a FOV systems should record at a minimum resolution of 4CIF (704 x 576 TV Lines) at a rate 10-25fps (particularly if the subject/object is moving rapidly). Day/night progressive scan or Mega Pixel cameras will yield the best quality images for this application. However, Mega Pixel cameras can increase storage requirements by in excess of 20 times the indicated MPEG figures per camera. Premises should, as best as possible, have clearly signalled and controlled entrance and exit zones to allow for quality images of individuals entering and exiting premises to be obtained.
Camera Placement	Cameras in public spaces are most often mounted on poles. When utilising poles for the mounting of CCTV cameras consider the following: • Pole height; • Footings, including any engineering requirements; • Environmental conditions (wind, etc); and • Pole shape and elasticity. Cameras should have their own poles or be fixed mounted (to buildings). When considering camera placement, consideration should be given to tampering and vandalism prevention.
Signage	It is recommended that signage is displayed at location entrances and exits. Signage should also be placed within premises where CCTV is operating (i.e. inside enclosed car parks, elevators, stair wells). See S9 AS4806.2:2006 – signage standards.
Data Transmission and Protocols	See WA Police/OCP Analogue to Digital Migration Strategy for information on data transmission protocols.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
File Export	Files should be able to be exported from the recording device in the following standards: • Mpeg4 • Jpeg • MJpeg • H.264 (and superseding standards) Data should be able to be played on Windows Media format or in common AVI format. See WA Police suggested standard for minimum file export requirements within the WA Closed Circuit Television (CCTV) Guidelines document.
Bandwidth Considerations	Systems which utilise a premises' computer network place demands on the capacity and bandwidth of the network. When considering a network based CCTV system, be aware of the following issues: • Number of cameras: The more cameras a system has, the larger bandwidth requirements. • Resolution: The higher the resolution required by the system, the greater the amount of bandwidth required. • Storage capabilities: The higher the bandwidth required by the system, the greater the system storage requirements. • Frames per second (fps): The higher the number of frames per second captured by the camera/system, the greater the amount of bandwidth required. • Linking additional devices (network video recorders/alarms/sensors/telemetry) to the network increases the bandwidth requirements.
Open Application Programming Interface (API) systems versus propriety systems.	Proprietary equipment may have an impact on future expansion or replacement of cameras. This may effectively lock a customer into the long-term use of one manufacturer's technology/equipment. Both the Open Network Video Interface Forum (ONVIF) and Physical Security Interoperability Alliance (PSIS) specifications define a common protocol for the exchange of information between network video devices including automatic device discovery, video streaming and intelligence metadata. The ONVIF and PSIA specification allows for interoperability between network video products regardless of manufacturer. CCTV equipment sourced from manufacturers who are members of the ONVIF group or PSIA may provide greater flexibility for future system expansion and component replacement. See www.onvif.org and www.psialliance.org

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Displays	Split displays (multiple images on a screen) may be most appropriate for monitoring systems installed for this application.
Video analytics (VA) and Video motion detection (VMD)	The use of video motion detection (VMD) or video analytics (VA) is most often application specific and should be based on the findings of a risk assessment and the system's stated objectives. VA or VMD may be considered for use if locations are not actively monitored or during non-business hours. To be effective VA and VMD must trigger a response and therefore should be tempered into location alarms. The system owners should ensure that there is a capacity to provide a timely response to any alarms. VA or VMD alarms should not however be connected to premises "Alarm Dialler" for the purposes of generation of an external alarm to a Central Monitoring Station (CMS) unless the CMS has the ability to remotely interrogate the video system for the purpose of video verification. When implementing VA or VMD consideration should be given to the impact that the environment (trees, wind, insects) may have on the system.
Video CODEC (Coding/Decoding)	Preferred video coding/decoding systems include: • Mpeg4; • MJpeg, • H.264 (or current industry standard). Image resolution should be specified as to the quality of the resolution required for the relevant CIF rating. This is required due to the way modern CODECs insert information between the "I" Frame. As such each CIF rating further is defined in GOOD / BETTER / BEST at each level.
Image Retention	Data from all cameras should be kept for a minimum of 31 days as suggested in Australian Standard S8.3 AS4806.1:2006. Data should be recorded on DVR equipment, Storage Area Network (SAN)/network storage or otherwise retained digitally. Stored images should be protected through archiving & the utilisation of fault tolerant RAID configurations to protect against drive failure.
Compression	Image compression should be kept as low as possible giving due consideration to the objectives of the individual camera in question and the system as a whole.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Storage Capacity	The amount of data storage required will be determined by the objectives of the system and system design (including: frames per second, resolution, data retention requirements). **Detecting activity:** A resolution of 4CIF at a minimum of 10 frames per second for a minimum period of 31 days: Required Storage per Camera: H264 105.5 GB Standard to 460GB Best Quality 4 CIF Mpeg 4 153.2 GB Quiet Scene to1.15 TB Busy scene **Recognising actions:** A resolution of 4CIF at 15 frames per second for a minimum of 31 days: Required Storage per Camera: H264 105.5 GB Standard to 460GB Best Quality 4 CIF Mpeg 4 153.2 GB Quiet Scene to1.15 TB Busy scene **Identification:** A resolution of 4CIF at 10-25 frames per second for a minimum period of 31 days: Required Storage per Camera: H264 188.44 GB Standard to 823 GB Best Quality 4 CIF Mpeg 4 268.2 GB Quiet Scene to 1.61 TB Busy scene Data should be regularly backed-up and retained.
System Validation	When exported, image data should also include: • Time/date stamp; • Camera location; • Camera identifier. • Watermarking or method of verifying the original image for authenticity ensuring tamper prevention.
System Registration	The system should be registered on the WA Police's Blue Iris CCTV register. https://blueiris.wa.gov.au.
System Maintenance	A budget should be identified and allocated for auditing and maintenance of the system. Maintenance of system components should be undertaken regularly, however, camera dome cleaning should be undertaken on a more frequent basis.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Policies/ Staff Training / Knowledge	Policy documents for the implementation and use of the CCTV system should be developed and retained by the organisation. Policy documents should: • Outline the objectives of the CCTV system; • Identify (through diagrams) camera locations; • Provide statements of camera views (what areas the cameras can view); and • Duty statements for each camera within the system. Policies should also indicate who may access data and establish protocols for sharing data within and outside the organisation. A minimum of one person on each shift should have access to stored data. System Standard Operating Procedures should be developed. These should include documents such as: • staff manuals; • Incident logs; • evidence logs; and • data back-up procedures. CCTV owner should also undertake an annual audit and evaluation of the system's use and outcomes. All staff interacting with system, its location or requests for data should be provided with an appropriate degree of training in its operation. Training/Staff Knowledge should include: • The use of the system including: data review, search and export; • Policy/Standard Operating Procedures (SOPs). (SOPs should be stored with system); • Use of incident logs/chain of evidence logs (these should be maintained and kept with system); • Contents and location of staff manual (including all policies, forms and SOPs). These should be established and kept with system. Managers should be aware of relevant Australian Standards and should seek to implement these. For more information see the WA Closed Circuit Television (CCTV) Guidelines.
Additional Considerations	UPS (uninterruptible power supply) should be considered insofar as its use is aligned with system objectives.

6.2 Semi-Public Spaces: Institutions

Individuals often encounter what can be described as ‘semi-public space’. This is usually defined as a private space accessible to the general public, e.g. a shop, licensed premises or hospital. It is space to which the public does not have free and full access, but contains services or spaces that require granting the public a degree of ‘conditional’ access.

For the purposes of this advice, “institutions” include hospitals, schools and other semi-public indoor locations.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Cameras	A range of camera types may be utilised for this application. These include: • Monochrome (black & white) • Colour • Day/Night (combines colour and monochrome) Monochrome cameras generally offer higher resolution and are relatively inexpensive, but are mostly used only in extremely low lighting conditions. Colour cameras generally offer a better overall representation of the scene (subject to adequate lighting) as well as higher identification capabilities. Day/night cameras combine the advantages of monochrome and colour cameras. They are much more sensitive to low light environments and are also able to be used with infra red lighting. Cameras also have basic functionality types including: • PTZ – Pan, tilt, zoom (where the camera may controlled along the horizontal and vertical planes and may zoom in and out on an object. • Fixed (the camera is pointed at a fixed spot and does not allow for control of movement). • IP (internet protocol cameras – cameras which interface directly with a computer network). Cameras may also contribute to the quality of images through the type, size and sensitivity of the image sensor contained within the camera as well as the compression algorithm applied within the camera. Lenses should match the format of the selected camera’s image sensor and be of such a design that presence of Infra Red should not affect the sharpness of the image or focal point.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Light Levels and Placement	External – Balanced white lighting with levels sufficient to allow for identification of individuals. Lighting levels should be at a minimum of 40-60 Lux. Lighting should be as even as possible. Lights should create intersecting cones of illumination and be placed to prevent shadows and dark spots. Lights should be located behind the camera to avoid backlighting of the target and should not be placed within the field of view to avoid glare. Internal – cameras should be directed away from lighting sources to avoid glare. Lighting should be as even as possible. At a minimum, internal lighting should avoid sharp bright spots or dark areas. In low lighting levels consider the installation of day/night cameras. For further information refer to Australian Standard S1.3.43 AS4806.2:2006 (CCTV) and AS4485.2:1997 (Security for Health Care Facilities).
Colour Rendition	Colour rendition depends on the type and level of lighting within the scene. White light is best to achieve good colour rendition. Florescent lights or metal halide lighting is preferable. Avoid colour lighting such as low pressure sodium (yellow) lighting in camera areas (particularly entry and exits). Where possible, consider the use of energy efficient lighting, however, this should not be to the detriment of system operation.
Scene Contrast	Consideration should be given to the effect of reflective surfaces (lights/sun reflecting off windows or other reflective surfaces) on image capture. Down lights may be preferable, however care should be taken to avoid dark spots and unconnected pools of light. Walls with white/light colour paint may improve scene contrast by allowing better scene illumination in lower levels of lighting. Low sheen paint may reduce acute light reflection from surfaces. In areas of widely varying lighting levels such as entry doors consideration should be given to the installation of day/night wide dynamic cameras.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Scene Contrast (continued)	IR (infra red) flood lights may be considered for illuminating dark areas. However, IR reflects differently off a range of materials and has a tendency to 'wash-out' faces. This has implications for identification of individuals and therefore the use of IR flood lights are not recommended for use with cameras which have been installed for the purpose of obtaining identifying information unless a scene test has been carried out to verify results.
Field of View (FOV)	The CCTV system should be developed based on the findings of a risk assessment. Each FOV should therefore reflect the purpose and objectives of the entire system. In addition, the purpose and objectives of each camera/location within system should be specified and documented within a duty statement. Each camera/location should have its own documented duty statement. The system (including camera placement and FOV) should be designed and used to compliment other security operations. Premises should, as best as possible, have clearly signalled and controlled entrance and exit zones to allow for quality images of individuals entering and exiting premises to be obtained. Insofar as the FOV meets the documented objectives of the entire CCTV system, FOVs to be considered may include: • At entrances to buildings; • Location access points; • Entrances to offices; • Points of sale/cash handling locations; and • High value stock/medications/assets; Wider views should be used to detect activities in areas such as those that are unable to be viewed by staff or are not regularly surveilled by security staff. AS4485.2:1997 states that CCTV should be placed at designated entry and exits points, pharmacy and nuclear waste storage areas (biohazard waste). FOV should avoid 'tops of heads' shots, distances or angles of view which make detection or identification problematic (refer to S3.7 AS4806.2:2006 for relevant object/screen size ratio). Any internal cameras should be positioned at a height of 1800mm-2400mm. External cameras may need to be positioned higher, however placement height should not impede the camera's ability to capture identifying information. FOV should be tested in the desired resolution by playing back stored images from the recording device to ensure that the level of detail that is captured is not adversely affected by a FOV setting. i.e. one that may prevent the capture of the required level of detail through covering too wide an area, for example.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Field of View (continued)	FOV should not include areas where private activities (as defined within the *Surveillance Devices Act 1998 WA* – See WA Closed Circuit Television (CCTV) Guidelines for further information) may be observed. E.g. neighbouring properties, changing rooms, toilets, etc. System owners should consider masking areas of FOV that are not owned or managed by the system owner or where private activities may take place. **Masking involves the use of software within the camera or recording device to obscure areas within the camera's FOV as defined by the user, so that these areas are not viewed or recorded by the system.** Vandal proof dome cameras are most appropriate to enhance camera resistance to tampering or vandalism. External camera placements should also consider the impact of weather conditions when determining camera choice.
Image Resolution	Image resolution requirements should be based on the findings of a risk assessment and the system's stated objectives. These systems should record at a minimum of 4CIF (704 x 576 TV lines) and at 6 frames per second.
Signage	It is recommended that signage is displayed at location entrances and exits. Signage should also be placed within premises where CCTV is operating. Consideration should be given to formally advising employees that CCTV is used throughout the facility or that they are subject to CCTV monitoring (within the bounds of appropriate privacy legislation). This may also be achieved through employment documentation such as conditions of employment. See Australian Standard S9 AS4806.2:2006 for signage standards.
Data Transmission and Protocols	See WA Police/OCP Analogue to Digital Migration Strategy for information on data transmission protocols.
File Export	Files should be able to be exported from the recording device in the following standards: • Mpeg4 • Jpeg • MJpeg • H.264 (and superseding standards) Data should be able to be played on Windows Media format or in common AVI format. See WA Police suggested standard for minimum file export requirements within the WA Closed Circuit Television (CCTV) Guidelines document.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Bandwidth Considerations	Systems which utilise a premises' computer network place demands on the capacity and bandwidth of the network. When considering a network based CCTV system, be aware of the following issues: • Number of cameras: The more cameras a system has, the larger bandwidth requirements. • Resolution: The higher the resolution required by the system, the greater the amount of bandwidth required. • Storage capabilities: The higher the bandwidth required by the system, the greater the system storage requirements. • Frames per second (fps): The higher the number of frames per second captured by the camera/system, the greater the amount of bandwidth required. • Linking additional devices (network video recorders/alarms/sensors/telemetry) to the network increases the bandwidth requirements.
Open Application Programming Interface (API) systems versus propriety systems	Proprietary equipment may have an impact on future expansion or replacement of cameras. This may effectively lock a customer into the long-term use of one manufacturer's technology/equipment. Both the Open Network Video Interface Forum (ONVIF) and Physical Security Interoperability Alliance (PSIS) specifications define a common protocol for the exchange of information between network video devices including automatic device discovery, video streaming and intelligence metadata. The ONVIF and PSIA specification allows for interoperability between network video products regardless of manufacturer. CCTV equipment sourced from manufacturers who are members of the ONVIF group or PSIA may provide greater flexibility for future system expansion and component replacement. See www.onvif.org and www.psialliance.org
Displays	Where practical, displays should be placed at building entrances/access points to alert visitors/users to the presence of CCTV surveillance. For live monitoring, displays should be placed in a secured office. Multiple displays (a number of individual television screens) are preferred to split displays (multiple images on a screen) for this application.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Video analytics (VA) and Video motion detection (VMD)	The use of video motion detection (VMD) or video analytics (VA) is most often application specific and should be based on the findings of a risk assessment and the system's stated objectives. VA or VMD may be considered for use if locations are not actively monitored or during non-business hours. To be effective VA and VMD must trigger a response and therefore should be tempered into location, alarms. The system owners should ensure that there is a capacity to provide a timely response to any alarms. VA or VMD alarms should not however be connected to premises "Alarm Dialler" for the purposes of generation of an external alarm to a Central Monitoring Station (CMS) unless the CMS has the ability to remotely interrogate the video system for the purpose of video verification. When implementing VA or VMD consideration should be given to the impact that the environment (e.g. trees, wind, insects) may have on the system.
Video CODEC (Coding/Decoding)	Preferred video coding/decoding systems include: • Mpeg4; • MJpeg, • H.264 (or current industry standard). Image resolution should be specified as to the quality of the resolution required for the relevant CIF rating. This is required due to the way modern CODECs insert information between the "I" Frame. As such each CIF rating further is defined in GOOD / BETTER / BEST at each level. Data from all cameras should be kept for a minimum of 31 days as suggested in Australian Standard S8.3 AS4806.1:2006.
Image Retention	Data should be recorded onto Digital Video Recording (DVR) equipment or otherwise retained digitally. Stored images should be protected through archiving & the utilisation of fault tolerant RAID configurations to protect against drive failure.
Compression	Image compression should be kept as low as possible giving due consideration to the objectives of the individual camera in question and the system as a whole.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Storage Capacity	The amount of data storage required will be determined by the objectives of the system and system design (including: frames per second, resolution, data retention requirements).
	At a minimum, storage capacity should be adequate to ensure that data is retained:
	Operational/General recording: A resolution of 4CIF at a minimum of 6 frames per second for a minimum period of 31 days.
	Required Storage per Camera:
	H264 64 GB Standard to 274 GB Best Quality 4 CIF Mpeg 4 80.46 GB Quiet Scene to 957 GB Busy scene
	Duress/Alarm activation: A resolution of 4CIF at 25 frames per second for a minimum period of 31 days.
	Required Storage per Camera:
	H264 188.44 GB Standard to 823 GB Best Quality 4 CIF Mpeg 4 268.2 GB Quiet Scene to 1.61 TB Busy scene
	Data should be regularly backed-up and retained.
System Validation	When exported, image data should also include:
	• Time/date stamp; • Camera location; • Camera identifier, • Watermarking or method of verifying the original image for authenticity ensuring tamper prevention.
System Registration	System should be registered on the WA Police's Blue Iris CCTV register. https://blueiris.wa.gov.au.
	A budget should be identified and allocated for auditing and maintenance of the system.
System Maintenance	Maintenance of system components should be undertaken regularly, however, camera dome cleaning should be undertaken on a more frequent basis.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Policies/ Staff Training / Knowledge	Policy documents for the implementation and use of the CCTV system should be developed and retained by the organisation. Policy documents should: • Outline the objectives of the CCTV system; • Identify (through diagrams) camera locations; • Provide statements of camera views (what areas the cameras can view); and • Duty statements for each camera within the system. Policies should also indicate who may access data and establish protocols for sharing data within and outside the organisation. A minimum of one person on each shift should have access to stored data. System Standard Operating Procedures should be developed. These should include documents such as: • staff manuals; • Incident logs; • evidence logs; and • data back-up procedures. CCTV owner should also undertake an annual audit and evaluation of the system's use and outcomes. All staff interacting with system, its location or requests for data should be provided with an appropriate degree of training in its operation. Training/Staff Knowledge should include: • The use of the system including: data review, search and export. • Policy/Standard Operating Procedures (SOPs). (SOPs should be stored with system). • Use of incident logs/chain of evidence logs (these should be maintained and kept with system). • Contents and location of staff manual (including all policies, forms and SOPs). These should be established and kept with system. Managers should be aware of relevant Australian Standards and should seek to implement these. For more information see the WA Closed Circuit Television (CCTV) Guidelines.
Additional Considerations	UPS (uninterruptible power supply) should be considered insofar as its use is aligned with system objectives.

6.3 Semi-Public Spaces: Retail or Pharmacy

Although retail space is private property, it is space which is opened to the public for the specific purpose of trade. As with most semi-public space, members of the public have limited access to this space, with access strictly defined by legislation and premises' owners.

The technical advice contained within S6.3 is based on the implementation of CCTV within semi-public spaces such as retail outlets and pharmacies.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Cameras	A range of camera types may be utilised for this application. These include: • Monochrome (black & white) • Colour • Day/Night (combines colour and monochrome) Monochrome cameras generally offer higher resolution and are relatively inexpensive, but are mostly used only in extremely low lighting conditions. Colour cameras generally offer a better overall representation of the scene (subject to adequate lighting) as well as higher identification capabilities. Day/night cameras combine the advantages of monochrome and colour cameras. They are much more sensitive to low light environments and are also able to be used with infra red lighting. Cameras also have basic functionality types including: • PTZ – Pan, tilt, zoom (where the camera may controlled along the horizontal and vertical planes and may zoom in and out on an object. • Fixed (the camera is pointed at a fixed spot and does not allow for control of movement). • IP (internet protocol cameras – cameras which interface directly with a computer network). Cameras may also contribute to the quality of images through the type, size and sensitivity of the image sensor contained within the camera as well as the compression algorithm applied within the camera.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Light Levels and Placement	External – Balanced white lighting with levels sufficient to allow for identification of individuals. Lighting levels should be at a minimum of 160 Lux. Lights should create intersecting cones of illumination and be placed to prevent shadows and dark spots. Lighting should be as even as possible. Lights should be located behind the camera to avoid backlighting of the target and should not be placed within the field of view to avoid glare. Internal – cameras should be directed away from lighting sources to avoid glare. Lighting should be as even as possible. At a minimum, internal lighting should avoid sharp bright spots or dark areas. Refer to Australian Standard S1.3.43 AS4806.2:2006.
Colour Rendition	Colour rendition depends on the type and level of lighting within the scene. White light is best to achieve good colour rendition. Florescent lights or metal halide lighting is preferable. Avoid colour lighting such as low pressure sodium (yellow) lighting in camera areas (particularly entry and exits). Where possible consider the use of energy efficient lighting, however, this should not be to the detriment of system operation.
Scene Contrast	Consideration should be given to the effect of reflective surfaces (lights/sun reflecting off windows or other reflective surfaces) on image capture. In areas of widely varying lighting levels such as entry doors consideration should be given to the installation of day/night wide dynamic cameras. Down lights may be preferable, however care should be taken to avoid dark spots and unconnected pools of light. Walls with white/light colour paint may improve scene contrast by allowing better scene illumination in lower levels of lighting. Low sheen paint may reduce acute light reflection from surfaces. IR (infra red) flood lights may be considered for illuminating dark areas. However, IR reflects differently off a range of materials and has a tendency to 'wash-out' faces. This has implications for identification of individuals and therefore the use of IR flood lights are not recommended for use with cameras which have been installed for the purpose of obtaining identifying information unless a scene test has been carried out to verify results.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Field of View (FOV)	The CCTV system should be developed based on the findings of a risk assessment. Each FOV should therefore reflect the purpose and objectives of the entire system. In addition, the purpose and objectives of each camera/location within system should be specified and documented within a duty statement. Each camera/location should have its own documented duty statement. The system (including camera placement and FOV) should be designed and used to compliment other security operations. Premises should, as best as possible, have clearly signalled and controlled entrance and exit zones to allow for quality images of individuals entering and exiting premises to be obtained. Insofar as the FOV meet the objectives of the system, FOV to be considered may include: • Entrances to building; • Cash register or point of sale; • High value stock; • Vulnerable stock; • Locations where cash is counted; and • Car parks. Wider views should be used to detect activities in areas such as corners or those unable to be viewed by staff. FOV should avoid 'tops of heads' shots, distances or angles of view which make detection or identification problematic (refer to S3.7 AS4806-2:2006 for relevant object/screen size ratio). FOV should be tested in the desired resolution by playing back stored images from the recording device to ensure that the level of detail that is captured is not adversely affected by a FOV setting. i.e. one that may prevent the capture of the required level of detail through covering too wide an area, for example. FOV should not include areas where private activities (as defined within the *Surveillance Devices Act 1998 WA* – See WA Closed Circuit Television (CCTV) Guidelines for further information) may be observed. E.g. neighbouring properties, changing rooms, toilets, etc. System owners should consider masking areas of FOV that are not owned or managed by the system owner or where private activities may take place. **Masking involves the use of software within the camera or recording device to obscure areas within the camera's FOV as defined by the user, so that these areas are not viewed or recorded by the system.** Vandal proof dome cameras are most appropriate to enhance camera resistance to tampering or vandalism. External camera placements should also consider the impact of weather conditions when determining camera choice.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Image Resolution	Image resolution requirements should be based on the findings of a risk assessment and the system’s stated objectives. Systems should record at a minimum of 4CIF (704 x 576 TV lines) and at a minimum of 10 frames per second during operational hours and a minimum of 6 frames per second during non-operational hours. Systems may utilise a live view resolution of 2 CIF (704 x 240).
Placement	Cameras located within retail premises may be mounted to the building’s ceiling, walls or on other fixed elements of the building’s structure. Internal cameras should be placed at a height of 1800mm-2400mm. External cameras may need to positioned higher, however, placement height should not impede ability to capture identifying information. Vandal proof dome cameras are most appropriate to enhance camera resistance to tampering or vandalism. It is recommended that signage is displayed at location entrances and exits. Signage should also be placed within premises where CCTV is operating. It is recommended that a monitor be placed at entrances to show identification images to patrons as they enter.
Signage	Consideration should be given to formally advising employees that CCTV is used throughout the facility or that they are subject to CCTV monitoring (within the bounds of appropriate privacy legislation). This may also be achieved through employment documentation such as conditions of employment. See Australian Standard S9 AS4806.2:2006.
Data Transmission and Protocols	See WA Police/OCP Analogue to Digital Migration Strategy for information on data transmission protocols.
File Export	Files should be able to be exported from the recording device in the following standards: • Mpeg4 • Jpeg • MJpeg • H.264 (and superseding standards) Data should be able to be played on Windows Media format or in common AVI format. See WA Police suggested standard for minimum file export requirements within the WA Closed Circuit Television (CCTV) Guidelines document.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Bandwidth Considerations	Systems which utilise a premises' computer network place demands on the capacity and bandwidth of the network. When considering a network based CCTV system, be aware of the following issues: • Number of cameras: The more cameras a system has, the larger bandwidth requirements. • Resolution: The higher the resolution required by the system, the greater the amount of bandwidth required. • Storage capabilities: The higher the bandwidth required by the system, the greater the system storage requirements. • Frames per second (fps): The higher the number of frames per second captured by the camera/system, the greater the amount of bandwidth required. • Linking additional devices (network video recorders/alarms/sensors/telemetry) to the network increases the bandwidth requirements.
Open Application Programming Interface (API) systems versus propriety systems	Proprietary equipment may have an impact on future expansion or replacement of cameras. This may effectively lock a customer into the long-term use of one manufacturer's technology/equipment. Both the Open Network Video Interface Forum (ONVIF) and Physical Security Interoperability Alliance (PSIS) specifications define a common protocol for the exchange of information between network video devices including automatic device discovery, video streaming and intelligence metadata. The ONVIF and PSIA specification allows for interoperability between network video products regardless of manufacturer. CCTV equipment sourced from manufacturers who are members of the ONVIF group or PSIA may provide greater flexibility for future system expansion and component replacement. See www.onvif.org and www.psialliance.org
Displays	Where practical, displays should be placed at building entrances/access points to alert visitors/users to the presence of CCTV surveillance. For live monitoring, displays should be placed at the point of sale area or within secured offices. Split displays (multiple images on a screen) may be most appropriate for monitoring systems installed for this application.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Video analytics (VA) and Video motion detection (VMD)	The use of video motion detection (VMD) or video analytics (VA) is most often application specific and should be based on the findings of a risk assessment and the system's stated objectives. VA or VMD may be considered for use during non-business hours. To be effective VA and VMD must trigger a response and therefore should be tempered into location, alarms. The system owners should ensure that there is a capacity to provide a timely response to any alarms. VA or VMD alarms should not however be connected to premises "Alarm Dialler" for the purposes of generation of an external alarm to a Central Monitoring Station (CMS) unless the CMS has the ability to remotely interrogate the video system for the purpose of video verification. When implementing VA or VMD consideration should be given to the impact that the environment (e.g. trees, wind, insects) may have on the system.
Video CODEC (Coding/Decoding)	Preferred video coding/decoding systems include: • Mpeg4; • MJpeg, • H.264 (or current industry standard). Image resolution should be specified as to the quality of the resolution required for the relevant CIF rating. This is required due to the way modern CODECs insert information between the "I" Frame. As such each CIF rating further is defined in GOOD / BETTER / BEST at each level.
Compression	Image compression should be kept as low as possible giving due consideration to the objectives of the individual camera in question and the system as a whole.
Image Retention	Data from all cameras should be kept for a minimum of 31 days as suggested in Australian Standard S8.3 AS4806.1:2006. Data should be recorded onto Digital Video Recording (DVR) equipment or otherwise retained digitally. Stored images should be protected through archiving & the utilisation of fault tolerant RAID configurations to protect against drive failure.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Storage Capacity	The amount of data storage required will be determined by the objectives of the system and system design (including: frames per second, resolution, data retention requirements). At a minimum, storage capacity should be adequate to ensure that data is retained: **Operational/General recording:** A resolution of 4CIF at a minimum of 10 frames per second for a minimum period of 31 days. Required Storage per Camera: H264 105.5 Standard to 460GB Best Quality 4 CIF Mpeg 4 153 GB Quiet scene to1.15 TB Busy scene **Non operational (out of hours) recording:** A resolution of 4CIF at a minimum of 6 frames per second for a minimum period of 31 days. Required Storage per Camera: H264 64 GB Standard to 274 GB Best Quality 4 CIF Mpeg 4 80.46 GB Quiet scene to 957 GB Busy scene **Duress/Alarm activation:** A resolution of 4CIF at 25 frames per second for a minimum period of 31 days. Required Storage per Camera: H264 188.44 GB Standard to 823 GB Best Quality 4 Mpeg 4 268.2 GB Quiet Scene to 1.61 TB Busy scene Data should be regularly backed-up and retained.
System Validation	When exported, image data should also include: • Time/date stamp; • Camera location; • Camera identifier • Watermarking or method of verifying the origonal image for authenticity ensuring tamper prevention.
System Registration	System should be registered on the WA Police's Blue Iris CCTV register. https://blueiris.wa.gov.au.
System Maintenance	Maintenance of system components should be undertaken regularly, however, camera dome cleaning should be undertaken on a more frequent basis.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Policies/ Staff Training / Knowledge	Policy documents for the implementation and use of the CCTV system should be developed and retained by the organisation. Policy documents should: • Outline the objectives of the CCTV system; • Identify (through diagrams) camera locations; • Provide statements of camera views (what areas the cameras can view); and • Duty statements for each camera within the system. Policies should also indicate who may access data and establish protocols for sharing data within and outside the organisation. A minimum of one person on each shift should have access to stored data. System Standard Operating Procedures should be developed. These should include documents such as: • staff manuals; • Incident logs; • evidence logs; and • data back-up procedures. CCTV owner should also undertake an annual audit and evaluation of the system's use and outcomes. All staff interacting with system, its location or requests for data should be provided with an appropriate degree of training in its operation. Training/Staff Knowledge should include: • The use of the system including: data review, search and export. • Policy/Standard Operating Procedures (SOPs). (SOPs should be stored with system). • Use of incident logs/chain of evidence logs (these should be maintained and kept with system). • Contents and location of staff manual (including all policies, forms and SOPs). These should be established and kept with system. Managers should be aware of relevant Australian Standards and should seek to implement these. For more information see the WA Closed Circuit Television (CCTV) Guidelines.

6.4 Semi-Public Space: Licensed Premises

The use of CCTV to improve security at licensed premises is of significant public interest due to the well established relationship between the consumption of alcohol and crime or other alcohol-related harm.

The security of licensed premises in Western Australia is regulated via licensing conditions imposed on licensed premises under the *Liquor Control Act 1988*. Under the Act, certain types of license applications and existing licenses may be required to have certain security measures in place. The Western Australian Department of Racing, Gaming and Liquor have developed policy guidelines on security at licensed premises and minimum standards for CCTV Security Systems (available at www.drgl.wa.gov.au).

Again, it must be stressed that due to the application specific nature of CCTV, the following provides only general advice to the technical considerations relevant to the use of CCTV within licensed premises.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Cameras	A range of camera types may be utilised for this application. These include: • Monochrome (black & white) • Colour • Day/Night (combines colour and monochrome) Monochrome cameras generally offer higher resolution and are relatively inexpensive, but are mostly used only in extremely low lighting conditions. Colour cameras generally offer a better overall representation of the scene (subject to adequate lighting) as well as higher identification capabilities. Day/night cameras combine the advantages of monochrome and colour cameras. They are much more sensitive to low light environments and are also able to be used with infra red lighting. Cameras also have basic functionality types including: • PTZ – Pan, tilt, zoom (where the camera may controlled along the horizontal and vertical planes and may zoom in and out on an object. • Fixed (the camera is pointed at a fixed spot and does not allow for control of movement). • IP (internet protocol cameras – cameras which interface directly with a computer network). Cameras may also contribute to the quality of images through the type, size and sensitivity of the image sensor contained within the camera as well as the compression algorithm applied within the camera. Lenses should match the format of the selected camera's image sensor and be of such a design that presence of Infra Red should not affect the sharpness of the image or focal point.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Light Levels and Placement	External – Balanced white lighting with levels sufficient to allow for identification of individuals. Lighting levels should be at a minimum of 160 Lux. Lights should create intersecting cones of illumination and be placed to prevent shadows and dark spots. Lighting should be as even as possible. Lights should be located behind the camera to avoid backlighting of the target and should not be placed within the field of view to avoid glare. Internal – cameras should be directed away from lighting sources to avoid glare. Lighting should be as even as possible. At a minimum, internal lighting should avoid sharp bright spots or dark areas. Fluctuating lighting such as strobe lighting or dance floor lighting may impede camera operation. In low lighting levels consider the installation of day/night or wide dynamic cameras. Refer to Australian Standard S1.3.43 AS4806.2:2006.
Colour Rendition	Colour rendition depends on the type and level of light within the scene. White light is best to achieve good colour rendition. Florescent lights or metal halide lighting is preferable. Avoid colour lighting in camera areas (particularly entry and exits). Where possible consider the use of energy efficient lighting, however, this should not be to the detriment of system operation.
Scene Contrast	Consideration should be made as to the effect of reflective surfaces (light reflecting off mirrors/walls/counter tops etc). Down lights may be preferable, however care should be taken to avoid dark spots and unconnected pools of light. In areas of widely varying lighting levels such as entry doors consideration should be given to the installation of day/night wide dynamic cameras. Walls with white/light colour paint may improve scene contrast by allowing better scene illumination in lower levels of lighting. Low sheen paint may reduce harsh light reflection from surfaces. IR (infra red) flood lights may be considered for illuminating internal (dark) areas. However, IR reflects differently off a range of materials and has a tendency to 'wash-out' faces and therefore have implications for identification of individuals and therefore is not recommended unless a scene test has been carried out to verify results.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Field of View (FOV)	The CCTV system should be developed based on the findings of a risk assessment. Each FOV should therefore reflect the purpose and objectives of the entire system. In addition, the purpose and objectives of each camera/location within system should be specified and documented within a duty statement. Each camera/location should have its own documented duty statement. The system (including camera placement and FOV) should be designed and used to compliment other security operations. The systems should be designed and used to compliment internal security patrols. Premises should, as best as possible, have clearly signalled and controlled entrance and exit zones to allow for quality images of individuals entering and exiting premises to be obtained. Insofar as the FOV meets the documented objectives of the entire CCTV system, FOVs to be considered may include: • Premises entrances and exits; • Point of sales areas; • Coat rooms; • Entrance to dance floor; and • Bar areas. Wider views should be used to detect activities in areas such as corners and seating areas or those areas unable to be viewed by staff or security staff. FOV should avoid 'tops of heads' shots, distances or angles of view which make detection or identification problematic (refer to S3.7 AS4806.2:2006 for relevant object/screen size ratio). The choice of camera type (monochrome, colour, day/night, fixed or PTZ) must be reflected in the objectives of the system and the purpose for which each camera is installed. Vandal and weather proof dome cameras are most appropriate to ensure camera security, however system owners may wish to consider other forms of vandalism/theft prevention. FOV should be tested in the desired resolution by playing back stored images from the recording device to ensure that the level of detail that is captured is not adversely affected by a FOV setting. i.e. one that may prevent the capture of the required level of detail through covering too wide an area, for example. FOV should not include areas where private activities (as defined within the *Surveillance Devices Act 1998 WA* – See WA Closed Circuit Television (CCTV) Guidelines for further information) may be observed. E.g. changing rooms, toilets, etc.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Image Resolution	Image resolution requirements should be based on the findings of a risk assessment and the system's stated objectives. Systems should record at a minimum of 4CIF (704 x 576 TV lines) and at 25 frames per second during operational hours and 6-10 frames per second during non-operational hours. Systems can utilise a live view resolution of 2 CIF (704 x 240).
Placement	Cameras in licensed premises may be mounted to the building's ceiling, walls or on other fixed elements of the building's structure. Internal cameras should be placed at a height of 1800mm-2400mm. External cameras may need to positioned higher, however, placement height should not impede ability to capture identifying information. Vandal proof dome cameras are most appropriate to enhance camera resistance to tampering or vandalism. The attached risk matrix provides further camera placement recommendations based on the likely risk of an incident occurring (See Risk Matrix for further camera placement advice).
Signage	It is recommended that signage is displayed at location entrances and exits. Signage should also be placed within premises where CCTV is operating. It is recommended that a monitor be placed at entrances to show identification images to patrons as they enter. Consideration should be given to formally advising employees that CCTV is used throughout the facility or that they are subject to CCTV monitoring (within the bounds of appropriate privacy legislation). This may also be achieved through employment documentation such as conditions of employment. See Australian Standard S9 AS4806.2:2006.
Data Transmission and Protocols	See WA Police/OCP Analogue to Digital Migration Strategy for information on data transmission protocols.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
File Export	Files should be able to be exported from the recording device in the following standards: • Mpeg4; • Jpeg; • MJpeg; • H.264 (and superseding standards). Data should be able to be played on Windows Media format or in common AVI format. See WA Police suggested standard for minimum file export requirements within the WA Closed Circuit Television (CCTV) Guidelines document.
Bandwidth Considerations	Systems which utilise a premises' computer network place demands on the capacity and bandwidth of the network. When considering a network based CCTV system, be aware of the following issues: • Number of cameras: The more cameras a system has, the larger bandwidth requirements. • Resolution: The higher the resolution required by the system, the greater the amount of bandwidth required. • Storage capabilities: The higher the bandwidth required by the system, the greater the system storage requirements. • Frames per second (fps): The higher the number of frames per second captured by the camera/system, the greater the amount of bandwidth required. • Linking additional devices (network video recorders/alarms/sensors/telemetry) to the network increases the bandwidth requirements.
Open Application Programming Interface (API) systems versus propriety systems	Proprietary equipment may have an impact on future expansion or replacement of cameras. This may effectively lock a customer into the long-term use of one manufacturer's technology/equipment. Both the Open Network Video Interface Forum (ONVIF) and Physical Security Interoperability Alliance (PSIS) specifications define a common protocol for the exchange of information between network video devices including automatic device discovery, video streaming and intelligence metadata. The ONVIF and PSIA specification allows for interoperability between network video products regardless of manufacturer. CCTV equipment sourced from manufacturers who are members of the ONVIF group or PSIA may provide greater flexibility for future system expansion and component replacement. See www.onvif.org and www.psialliance.org

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Displays	Where practical, displays should be placed at building entrances/access points to alert visitors/users to the presence of CCTV surveillance.
	For live monitoring, displays should be placed within secured offices.
	Multiple displays (a number of individual television screen) are preferred to split displays (multiple images on a screen) for this application.
Video analytics (VA) and Video motion detection (VMD)	The use of video motion detection (VMD) or video analytics (VA) is most often application specific and should be based on the findings of a risk assessment and the system's stated objectives.
	VA or VMD may be considered for use during non-business hours.
	To be effective VA and VMD must trigger a response and therefore should be tempered into location, alarms. The system owners should ensure that there is a capacity to provide a timely response to any alarms.
	VA or VMD alarms should not however be connected to premises "Alarm Dialler" for the purposes of generation of an external alarm to a Central Monitoring Station (CMS) unless the CMS has the ability to remotely interrogate the video system for the purpose of video verification.
	When implementing VA or VMD consideration should be given to the impact that the environment (e.g. trees, wind, insects) may have on the system.
Video CODEC (Coding/Decoding)	Preferred video coding/decoding systems include: • Mpeg4; • MJpeg, • H.264 (or current industry standard).
	Image resolution should be specified as to the quality of the resolution required for the relevant CIF rating. This is required due to the way modern CODECs insert information between the "I" Frame.
	As such each CIF rating further is defined in GOOD / BETTER / BEST at each level.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Image Retention	Data should be kept for a minimum of 14 days as per Department of Racing Gaming and Liquor policy.
	Data should be recorded on DVR equipment, computer network or otherwise retained digitally.
	Stored images should be protected through archiving & the utilisation of fault tolerant RAID configurations to protect against drive failure.
Compression	Image compression should be kept as low as possible giving due consideration to the objectives of the individual camera in question and the system as a whole.
Storage Capacity	The amount of data storage required will be determined by the objectives of the system and system design (including: frames per second, resolution, data retention requirements).
	At a minimum, storage capacity should be adequate to ensure that data is retained:
	Operational/General recording: A resolution of 4CIF at 25 frames per second for a minimum period of 14 days.
	Required Storage per Camera:
	H264 94 GB Standard to 412 GB Best Quality 4 CIF Mpeg 4 134 GB Quiet Scene to 800 GB Busy scene
	Non operational (out of hours) recording: A resolution of 4CIF at a minimum of 6 frames per second for a minimum period of 14 days.
	Required Storage per Camera:
	H264 30 GB Standard to 137 GB Best Quality 4 CIF Mpeg 4 40 GB Quiet scene to 453 GB Busy scene
	Duress/Alarm activation: A resolution of 4CIF at 25 frames per second for a minimum period of 14 days.
	Required Storage per Camera:
	H264 94 GB Standard to 412 GB Best Quality 4 CIF Mpeg 4 134 GB Quiet Scene to 800 GB Busy scene
	Data back-ups should be made and retained as per Department of Racing Gaming and Liquor policy.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
System Validation	When exported, image data should also include: • Time/date stamp; • Camera location; • Camera identifier; and • Watermarking or method of verifying the origonal image for authenticity ensuring tamper prevention.
System Registration	System should be registered on the WA Police's Blue Iris CCTV register. https://blueiris.wa.gov.au.
System Maintenance	Maintenance of system components should be undertaken regularly, however, camera dome cleaning should be undertaken on a more frequent basis.
Policies/Staff Training / Knowledge	Policy documents for the implementation and use of the CCTV system should be developed and retained by the organisation. Policy documents should: • Outline the objectives of the CCTV system; • Identify (through diagrams) camera locations; • Provide statements of camera views (what areas the cameras can view); and • Duty statements for each camera within the system. Policies should also indicate who may access data and establish protocols for sharing data within and outside the organisation. A minimum of one person on each shift should have access to stored data. System Standard Operating Procedures should be developed. These should include documents such as: • staff manuals; • Incident logs; • evidence logs; and • data back-up procedures. CCTV owner should also undertake an annual audit and evaluation of the system's use and outcomes. All staff interacting with system, its location or requests for data should be provided with an appropriate degree of training in its operation. Training/Staff Knowledge should include: • The use of the system including: data review, search and export. • Policy/Standard Operating Procedures (SOPs). (SOPs should be stored with system). • Use of incident logs/chain of evidence logs (these should be maintained and kept with system).

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Policies/Staff Training / Knowledge (continued)	• Contents and location of staff manual (including all policies, forms and SOPs). These should be established and kept with system. Managers should be aware of relevant Australian Standards and should seek to implement these. For more information see the WA Closed Circuit Television (CCTV) Guidelines.

Security Events	**Camera Placement Locations**
High likelihood of capturing security events	Street frontage at main entrance Entrances and exits Car park Entry cashier Bar area Entrance to dance floor
Low likelihood of capturing security events	Office Areas Cash register Staff only areas (e.g. lockers) Cash counting areas Seating areas Dance floor Toilets

6.5 Private Spaces: Commercial or Industrial Premises

Private premises are, for the most part, only accessible to selected members of the public by invitation or for narrowly defined set of purposes such as business or private activities.

Commercial or industrial premises are generally only accessible to employees or those individuals invited to the location. State legislation regulates the behaviour of individuals at commercial and industrial premises to ensure the safety of employees and visitors to these sites.

Although workplace safety may be the primary concern at these premises, they may also be targeted for a range of crimes ranging from graffiti to terrorism. Therefore, CCTV may be an appropriate tool to assist with not only operational or workplace safety surveillance, but also security surveillance; although the former requires a different set of objectives and suggested standards than set out within this document.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Cameras	A range of camera types may be utilised for this application. These include: • Monochrome (black & white) • Colour • Day/Night (combines colour and monochrome) Monochrome cameras generally offer higher resolution and are relatively inexpensive, but are mostly used only in extremely low lighting conditions. Colour cameras generally offer a better overall representation of the scene (subject to adequate lighting) as well as higher identification capabilities. Day/night cameras combine the advantages of monochrome and colour cameras. They are much more sensitive to low light environments and are also able to be used with infra red lighting. Cameras also have basic functionality types including: • PTZ – Pan, tilt, zoom (where the camera may controlled along the horizontal and vertical planes and may zoom in and out on an object. • Fixed (the camera is pointed at a fixed spot and does not allow for control of movement). • IP (internet protocol cameras – cameras which interface directly with a computer network). Cameras may also contribute to the quality of images through the type, size and sensitivity of the image sensor contained within the camera as well as the compression algorithm applied within the camera. Lenses should match the format of the selected camera's image sensor and be of such a design that presence of Infra Red should not affect the sharpness of the image or focal point.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Light Levels and Placement	External – Balanced white lighting with levels sufficient to allow for identification of individuals. Lighting levels should be at a minimum of 40-60 Lux. Lighting should be as even as possible. Lights should create intersecting cones of illumination and be placed to prevent shadows and dark spots. Lights should be located behind the camera to avoid backlighting of the target and should not be placed within the field of view to avoid glare. In low lighting levels consider the installation of day/night or wide dynamic cameras. Refer to Australian Standard S1.3.43 AS4806.2:2006.
Colour Rendition	Colour rendition depends on the type and level of lighting within the scene. White light is best to achieve good colour rendition. Florescent lights or metal halide lighting is preferable. Avoid colour lighting such as low pressure sodium (yellow) lighting in camera areas (particularly entry and exits). Where possible, consider the use of energy efficient lighting, however, this should not be to the detriment of system operation.
Scene Contrast	Consideration should be given to the effect of reflective surfaces (lights/sun reflecting off windows or other reflective surfaces) on image capture. In areas of widely varying lighting levels such as entry doors consideration should be given to the installation of day/night wide dynamic cameras. Down lights may be preferable, however care should be taken to avoid dark spots and unconnected pools of light. Walls with white/light colour paint may improve scene contrast by allowing better scene illumination in lower levels of lighting. Low sheen paint may reduce acute light reflection from surfaces. IR (infra red) flood lights may be considered for illuminating dark areas. However, IR reflects differently off a range of materials and has a tendency to 'wash-out' faces. This has implications for identification of individuals and therefore the use of IR flood lights are not recommended for use with cameras which have been installed for the purpose of obtaining identifying information unless a scene test has been carried out to verify results.

CONSIDERATION

TECHNICAL STANDARD(S) / ADVICE

Field of View (FOV)

The CCTV system should be developed based on the findings of a risk assessment. Each FOV should therefore reflect the purpose and objectives of the entire system. In addition, the purpose and objectives of each camera/location within system should be specified and documented within a duty statement. Each camera/location should have its own documented duty statement. The system (including camera placement and FOV) should be designed and used to compliment other security operations.

Premises should, as best as possible, have clearly signalled and controlled entrance and exit zones to allow for quality images of people and vehicles entering and exiting premises to be obtained.

Insofar as the FOV meets the documented objectives of the entire CCTV system, FOVs to be considered may include:

- All site entrances (access control/gatehouses);
- Any points of perceived perimeter vulnerability;
- Building/office access points;
- Sensitive/vulnerable infrastructure; and
- High value stock/medications/assets.

Wider views should be used to detect activities in areas such as those that are unable to be viewed by staff or are not regularly surveilled by security staff.

FOV should avoid 'tops of heads' shots, distances or angles of view which make detection or identification problematic (refer to S3.7 AS4806.2:2006 for relevant object/screen size ratio).

Consideration should be given to the use of pre-determined camera duty cycles (FOV pathways or locations pre-programmed into camera operation).

The choice of camera type (monochrome, colour, day/night, fixed or PTZ) must be reflected in the objectives of the system and the purpose for which each camera is installed. Vandal and weather proof dome cameras are most appropriate to ensure camera security, however, system owners may wish to consider other forms of vandalism/theft prevention.

Any internal cameras should be positioned at a height of 1800mm-2400mm. External cameras may need to be positioned higher, however placement height should not impede the camera's ability to capture identifying information.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Field of View (FOV) (continued)	FOV should be tested in the desired resolution by playing back stored images from the recording device to ensure that the level of detail that is captured is not adversely affected by a FOV setting. i.e. one that may prevent the capture of the required level of detail through covering too wide an area, for example. FOV should not include areas where private activities (as defined within the *Surveillance Devices Act 1998 WA* – See WA Closed Circuit Television (CCTV) Guidelines for further information) may be observed. E.g. neighbouring properties, changing rooms, toilets, etc. System owners should consider masking areas of FOV that are not owned or managed by the system owner or where private activities may take place. **Masking involves the use of software within the camera or recording device to obscure areas within the camera's FOV as defined by the user, so that these areas are not viewed or recorded by the system.** Note that CCTV used for operational surveillance/occupational health and safety purposes will require different objectives and minimum requirements to those stated within this document.
Image Resolution	Image resolution requirements should be based on the findings of a risk assessment and the system's stated objectives. These systems should record at a resolution of 4CIF (704 x 576 TV lines) and at a minimum of 6 frames per second.
Signage	It is recommended that signage is displayed at location entrances and exits. Signage should also be placed within premises where CCTV is operating (i.e. inside enclosed car parks, elevators, stair wells). Consideration should be given to formally advising employees that CCTV is used throughout the facility or that they are subject to CCTV monitoring (within the bounds of appropriate privacy legislation). This may also be achieved through employment documentation such as conditions of employment. See Australian Standard S9 AS4806.2:2006 for signage standards.
Data Transmission and Protocols	See WA Police/OCP Analogue to Digital Migration Strategy for information on data transmission protocols.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
File Export	Files should be able to be exported from the recording device in the following standards: • Mpeg4; • Jpeg; • MJpeg; • H.264 (and superseding standards) Data should be able to be played on Windows Media format or in common AVI format. See WA Police suggested standard for minimum file export requirements within the WA Closed Circuit Television (CCTV) Guidelines document.
Bandwidth Considerations	Systems which utilise a premises' computer network place demands on the capacity and bandwidth of the network. When considering a network based CCTV system, be aware of the following issues: • Number of cameras: The more cameras a system has, the larger bandwidth requirements. • Resolution: The higher the resolution required by the system, the greater the amount of bandwidth required. • Storage capabilities: The higher the bandwidth required by the system, the greater the system storage requirements. • Frames per second (fps): The higher the number of frames per second captured by the camera/system, the greater the amount of bandwidth required. • Linking additional devices (network video recorders/alarms/sensors/telemetry) to the network increases the bandwidth requirements.
Open Application Programming Interface (API) systems versus propriety systems	Proprietary equipment may have an impact on future expansion or replacement of cameras. This may effectively lock a customer into the long-term use of one manufacturer's technology/equipment. Both the Open Network Video Interface Forum (ONVIF) and Physical Security Interoperability Alliance (PSIS) specifications define a common protocol for the exchange of information between network video devices including automatic device discovery, video streaming and intelligence metadata. The ONVIF and PSIA specification allows for interoperability between network video products regardless of manufacturer. CCTV equipment sourced from manufacturers who are members of the ONVIF group or PSIA may provide greater flexibility for future system expansion and component replacement. See www.onvif.org and www.psialliance.org

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Displays	Where practical, displays should be placed at building entrances/access points to alert visitors/users to the presence of CCTV surveillance. For live monitoring, displays should be placed in a secured office. Multiple displays (television screens) are preferred to split displays (multiple images on a screen).
Video analytics (VA) and Video motion detection (VMD)	The use of video motion detection (VMD) or video analytics (VA) is most often application specific and should be based on the findings of a risk assessment and the system's stated objectives. VA or VMD may be considered for use if locations are not actively monitored or during non-business hours. To be effective VA and VMD must trigger a response and therefore should be tempered into location, alarms. The system owners should ensure that there is a capacity to provide a timely response to any alarms. VA or VMD alarms should not however be connected to premises "Alarm Dialler" for the purposes of generation of an external alarm to a Central Monitoring Station (CMS) unless the CMS has the ability to remotely interrogate the video system for the purpose of video verification. When implementing VA or VMD consideration should be given to the impact that the environment (e.g. trees, wind, insects) may have on the system.
Video CODEC (Coding/Decoding)	Preferred video coding/decoding systems include: • Mpeg4; • MJpeg, • H.264 (or current industry standard). Image resolution should be specified as to the quality of the resolution required for the relevant CIF rating. This is required due to the way modern CODECs insert information between the "I" Frame. As such each CIF rating further is defined in GOOD / BETTER / BEST at each level.
Image Retention	Data from all cameras should be kept for a minimum of 31 days as suggested in Australian Standard S8.3 AS4806.1:2006. Data should be recorded onto Digital Video Recording (DVR) equipment or otherwise retained digitally. Stored images should be protected through archiving & the utilisation of fault tolerant RAID configurations to protect against drive failure.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Compression	Image compression should be kept as low as possible giving due consideration to the objectives of the individual camera in question and the system as a whole.
Storage Capacity	The amount of data storage required will be determined by the objectives of the system and system design (including: frames per second, resolution, data retention requirements). At a minimum, storage capacity should be adequate to ensure that data is retained: **Operational/General recording:** A resolution of 4CIF at a minimum of 6 frames per second for a minimum period of 31 days. Required Storage per Camera: H264 64 GB Standard to 274 GB Best Quality 4 CIF Mpeg 4 80.46 GB Quiet scene to 957 GB Busy scene **Duress/Alarm activation:** A resolution of 4CIF at 25 frames per second for a minimum period of 31 days. Required Storage per Camera: H264 188.44 GB Standard to 823 GB Best Quality 4 CIF Mpeg 4 268.2 GB Quiet Scene to 1.61 TB Busy scene
System Validation	When exported, image data should also include: • Time/date stamp; • Camera location; • Camera identifier; and • Watermarking or method of verifying the origonal image for authenticity ensuring tamper prevention.
System Registration	System should be registered on the WA Police's Blue Iris CCTV register. https://blueiris.wa.gov.au.
System Maintenance	A budget should be identified and allocated for auditing and maintenance of the system. Maintenance of system components should be undertaken regularly, however, camera dome cleaning should be undertaken on a more frequent basis.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Policies/Staff Training / Knowledge	Policy documents for the implementation and use of the CCTV system should be developed and retained by the organisation. Policy documents should: • Outline the objectives of the CCTV system; • Identify (through diagrams) camera locations; • Provide statements of camera views (what areas the cameras can view); and • Duty statements for each camera within the system. Policies should also indicate who may access data and establish protocols for sharing data within and outside the organisation. A minimum of one person on each shift should have access to stored data. System Standard Operating Procedures should be developed. These should include documents such as: • staff manuals; • Incident logs; • evidence logs; and • data back-up procedures. CCTV owner should also undertake an annual audit and evaluation of the system's use and outcomes. All staff interacting with system, its location or requests for data should be provided with an appropriate degree of training in its operation. Training/Staff Knowledge should include: • The use of the system including: data review, search and export. • Policy/Standard Operating Procedures (SOPs). (SOPs should be stored with system). • Use of incident logs/chain of evidence logs (these should be maintained and kept with system). • Contents and location of staff manual (including all policies, forms and SOPs). These should be established and kept with system. Managers should be aware of relevant Australian Standards and should seek to implement these. For more information see the WA Closed Circuit Television (CCTV) Guidelines.
Additional Considerations	UPS (uninterruptible power supply) should be considered insofar as its use is aligned with system objectives.

6.6 Private Spaces: Private Residential

Many individuals and families are now choosing to install CCTV as part of their home security systems. The large range of relatively inexpensive do-it-yourself CCTV installation kits has made the use of CCTV a much more attractive and popular option for modern home security.

The installation and use of CCTV should, however, be based on the outcomes of a well considered risk assessment and home owners should become familiar with any legislation regulating the use of devices such as CCTV.

Should owners of private residences wish to install CCTV, the following technical advice may assist them to select a system that may provide an appropriate level of quality for their needs.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Cameras	A range of camera types may be utilised for this application. These include: • Monochrome (black & white) • Colour • Day/Night (combines colour and monochrome) Monochrome cameras generally offer higher resolution and are relatively inexpensive, but are mostly used only in extremely low lighting conditions. Colour cameras generally offer a better overall representation of the scene (subject to adequate lighting) as well as higher identification capabilities. Day/night cameras combine the advantages of monochrome and colour cameras. They are much more sensitive to low light environments and are also able to be used with infra red lighting. Cameras also have basic functionality types including: • PTZ – Pan, tilt, zoom (where the camera may controlled along the horizontal and vertical planes and may zoom in and out on an object. • Fixed (the camera is pointed at a fixed spot and does not allow for control of movement). • IP (internet protocol cameras – cameras which interface directly with a computer network). The use of power over internet (POI) cameras may be an option for increasing the energy efficiency of a system. Cameras may also contribute to the quality of images through the type, size and sensitivity of the image sensor contained within the camera as well as the compression algorithm applied within the camera. Lenses should match the format of the selected camera's image sensor and be of such a design that presence of Infra Red should not affect the sharpness of the image or focal point.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Light Levels and Placement	External – Balanced white lighting with levels sufficient to allow for the identification of individuals. Minimum lighting level of 160 Lux. Lights should allow create intersecting cones of illumination and be placed to prevent shadows and dark spots. Lights should be located behind the camera to avoid backlighting of the target and should not be placed within the field of view to avoid glare. Internal – cameras should be directed away from lighting sources to avoid glare. Lighting should be as even as possible. At a minimum, internal lighting should avoid sharp bright spots or dark areas.In low lighting levels consider the installation of day/night cameras. Refer to Australian Standard S1.3.43 AS4806.2:2006.
Colour Rendition	Colour rendition depends on the type and level of light within the scene. White light is best to achieve good colour rendition. Florescent lights or metal halide lighting is preferable. Avoid colour lighting such as low pressure sodium (yellow) lighting in camera areas (particularly entry and exits). Where possible, consider the use of energy efficient lighting, however, this should not be to the detriment of system operation.
Scene Contrast	Consideration should be given to the effect of reflective surfaces (lights/sun reflecting off mirrors/windows/walls/hallways or other reflective surfaces) on image capture. In areas of widely varying lighting levels such as entry doors consideration should be given to the installation of day/night wide dynamic cameras. Down lights may be preferable, however care should be taken to avoid dark spots and unconnected pools of light. Walls with white/light colour paint may improve scene contrast by allowing better scene illumination in lower levels of lighting. Low sheen paint may reduce acute light reflection from surfaces.
Field of View (FOV)	The CCTV system should be developed based on the findings of a risk assessment. Each FOV should therefore reflect the purpose and objectives of the entire system. In addition, the purpose and objectives of each camera/location within system should be specified and documented within a duty statement. Each camera/location should have its own documented duty statement.

CONSIDERATION

TECHNICAL STANDARD(S) / ADVICE

Field of View (FOV)
(continued)

Insofar as the FOV meets the documented objectives of the entire CCTV system, FOVs to be considered may include:

- Entrances to building/property;
- Driveways/vehicle storage areas; and
- Yard areas.

Wider views should be used to detect activities in areas such as yards/side access routes or those areas unable to be easily viewed from within the premises.

FOV should avoid 'tops of heads' shots, distances or angles of view which make detection or identification problematic (refer to S3.7 AS4806.2:2006 for relevant object/screen size ratio).

Consideration should be given to the use of pre-determined camera duty cycles (FOV pathways or locations pre-programmed into camera operation).

The choice of camera type (monochrome, colour, day/night, fixed or PTZ) must be reflected in the objectives of the system and the purpose for which each camera is installed. Vandal and weather proof dome cameras are most appropriate to ensure camera security, however system owners may wish to consider other forms of vandalism/theft prevention.

Any internal cameras should be positioned 1800mm-2400mm above ground. External cameras may need to be positioned higher however, placement height should not impede the camera's ability to capture identifying information.

FOV should be tested in the desired resolution by playing back stored images from the recording device to ensure that the level of detail that is captured is not adversely affected by a FOV setting. i.e. one that may prevent the capture of the required level of detail through covering too wide an area, for example.

FOV should not include areas where private activities (as defined within the *Surveillance Devices Act 1998 WA* – See WA Closed Circuit Television (CCTV) Guidelines for further information) may be observed. E.g. neighbouring properties including windows, yards and pool areas, toilets, etc.

System owners should consider masking areas of FOV that are not owned or managed by the system owner, where private activities may take place. **Masking involves the use of software within the camera or recording device to obscure areas within the camera's FOV as defined by the user, so that these areas are not viewed or recorded by the system.**

Vandal proof dome cameras are most appropriate to ensure camera security.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Image Resolution	Image resolution requirements should be based on the findings of a risk assessment and the system's stated objectives. Systems should record at a minimum of 4CIF (704 x 576 TV lines) and at 6 frames per second.
Signage	It is recommended that signage is displayed at the location's frontage. Visitors should be informed that CCTV is in operation within the location. See Australian Standard S9 AS4806.2:2006.
Data Transmission and Protocol	See WA Police/OCP Analogue to Digital Migration Strategy for information on data transmission protocols.
File Export	Files should be able to be exported from the recording device in the following standards: • Mpeg4; • Jpeg; • MJpeg; • H.264 (and superseding standards) Data should be able to be played on Windows Media format or in common AVI format. See WA Police suggested standard for minimum file export requirements within the WA Closed Circuit Television (CCTV) Guidelines document.
Cabling Infrastructure and Bandwidth Limitations	Systems which utilise a premises' computer network place demands on the capacity and bandwidth of the network. When considering a network based CCTV system, be aware of the following issues: • Number of cameras: The more cameras a system has, the larger bandwidth requirements. • Resolution: The higher the resolution required by the system, the greater the amount of bandwidth required. • Storage capabilities: The higher the bandwidth required by the system, the greater the system storage requirements. • Frames per second (fps): The higher the number of frames per second captured by the camera/system, the greater the amount of bandwidth required. • Linking additional devices (network video recorders/alarms/sensors/telemetry) to the network increases the bandwidth requirements.

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
Open Application Programming Interface (API) systems versus propriety systems.	Proprietary equipment may have an impact on future expansion or replacement of cameras. This may effectively lock a customer into the long-term use of one manufacturer's technology/equipment. Both the Open Network Video Interface Forum (ONVIF) and Physical Security Interoperability Alliance (PSIS) specifications define a common protocol for the exchange of information between network video devices including automatic device discovery, video streaming and intelligence metadata. The ONVIF and PSIA specification allows for interoperability between network video products regardless of manufacturer. CCTV equipment sourced from manufacturers who are members of the ONVIF group or PSIA may provide greater flexibility for future system expansion and component replacement. See www.onvif.org and www.psialliance.org
Displays	Split displays (multiple images on a screen) may be most appropriate for monitoring systems installed for this application.
Video analytics (VA) and Video motion detection (VMD)	The use of video motion detection (VMD) or video analytics (VA) is most often application specific and should be based on the findings of a risk assessment and the system's stated objectives. VA or VMD should be considered during hours/occasions where occupants are absent or not able to provide natural surveillance over property (e.g. sleeping hours). To be effective VA and VMD must trigger a response and therefore should be tempered into location, alarms. The system owners should ensure that there is a capacity to provide a timely response to any alarms. VA or VMD alarms should not however be connected to premises "Alarm Dialler" for the purposes of generation of an external alarm to a Central Monitoring Station (CMS) unless the CMS has the ability to remotely interrogate the video system for the purpose of video verification. When implementing VA or VMD consideration should be given to the impact that the environment (trees, wind, insects) may have on the system.

CONSIDERATION | **TECHNICAL STANDARD(S) / ADVICE**

Video CODEC
(Coding/Decoding)

Preferred video coding/decoding systems include:

- Mpeg4;
- MJpeg,
- H.264 (or current industry standard).

Image resolution should be specified as to the quality of the resolution required for the relevant CIF rating. This is required due to the way modern CODECs insert information between the "I" Frame. As such each CIF rating further is defined in GOOD / BETTER / BEST at each level.

Image Retention

Data from all cameras should be kept for a minimum of 31 days as suggested in Australian Standard S8.3 AS4806.1:2006.

Data should be recorded on DVR equipment, Storage Area Network (SAN)/network storage or otherwise retained digitally.

Stored images should be protected through archiving and the utilisation of fault tolerant RAID configurations to protect against drive failure.

Compression

Image compression should be kept as low as possible giving due consideration to the objectives of the individual camera in question and the system as a whole.

Storage Capacity

The amount of data storage required will be determined by the objectives of the system and system design (including: frames per second, resolution, data retention requirements).

At a minimum, storage capacity should be adequate to ensure that data is retained:

Operational/General recording: A resolution of 4CIF at a minimum of 6 frames per second for a minimum period of 31 days.

Required Storage per Camera:

H264	64 GB Standard to 274 GB Best Quality 4 CIF
Mpeg 4	80.46 GB Quiet scene to 957 GB Busy scene

Duress/Alarm activation: A resolution of 4CIF at 25 frames per second for a minimum period of 31 days.

Required Storage per Camera:

H264	188.44 GB Standard to 823 GB Best Quality 4 CIF
Mpeg 4	268.2 GB Quiet Scene to 1.61 TB Busy scene

CONSIDERATION	TECHNICAL STANDARD(S) / ADVICE
System Validation	When exported, image data should also include: • Time/date stamp; • Camera location; • Camera identifier; and • Watermarking or method of verifying the origonal image for authenticity ensuring tamper prevention.
System Registration	The system should be registered on the WA Police's Blue Iris CCTV register. https://blueiris.wa.gov.au.
System Maintenance	Maintenance of system components should be undertaken regularly, however, camera dome cleaning should be undertaken on a more frequent basis.
Training	The owner should ensure that they: • Are familiar with system components; • Are able to view and export data when necessary; • Are aware of legal issues surrounding location and FOV of cameras; and • Maintain documented camera view/location maps and duty statements.

Further information

Enquiries regarding this document or requests for further information should be directed to:

The Office of Crime Prevention
Western Australia Police
Level 5, 197 St George's Terrace
Perth WA 6000

Ph: (08) 9222 9733
E: crimeprevention@ocp.wa.gov.au
www.crimeprevention.wa.gov.au

WebLinks

https://blueiris.wa.gov.au
www.crimeprevention.wa.gov.au
www.drgl.wa.gov.au
www.onvif.org
www.psialliance.org

Legislation

Surveillance Devices Act 1998 (WA)

Liquor Control Act 1988 (WA)

Australian Standards

AS4806.1-2006: Closed circuit television (CCTV) Part 1: Management and Operation
AS4806.2-2006: Closed circuit television (CCTV) Part 2: Application guidelines

Acknowledgements

The Office of Crime Prevention wishes to thank and acknowledge the contribution of the following individuals or organisations in the development of this document: WA Police, Western Australia CCTV Working Group members, Western Australia CCTV Working Group Technical Advice Sub-committee members, Australian Security Industry Association, Security Agents Institute of Western Australia, Department of Education, Public Transport Authority, Main Roads WA.

Office of
Crime Prevention

Western Australian Police
Office of Crime Prevention
Level 5, 197 St Georges Terrace
PERTH, WESTERN AUSTRALIA 6000
Telephone: 08 9222 9733
Facsimile: 08 9222 8705
Email: crimeprevention@ocp.wa.gov.au
Website: www.crimeprevention.wa.gov.au

APRIL 2010 • 4284 Design Design