



Closed Circuit Television (CCTV) Management and Operations Manual

CCTV Management and Operations Manual

Prepared for: Office of Crime Prevention
Western Australia Police

Prepared by: Chris Cabbage, Director & Principal Consultant
*BSc(Sec)Hons, GAICD, AdvDip BusMgt, Dip CrimInv, Dip Pol
Amlec House Pty Ltd.*

Senior Advisor(s): Professor Martin Gill & Professor Clifton Smith

Date: 3 May 2010

COPYRIGHT: The concepts and information contained in this document are the property of Amlec House Pty Ltd and have been exclusively released to Western Australia Police, Western Australia Local Government and Not For Profit Community Organisations. Use or copying of this document in whole or in part beyond the control of the client without the written permission of Amlec House Pty Ltd constitutes an infringement of copyright.

LIMITATION: These management document templates have been prepared on behalf of and for the exclusive use of Amlec House Pty Ltd's Client, Western Australia Police, and is subject to and issued in connection with the provisions of the agreement between Amlec House Pty Ltd and its Client. Amlec House Pty Ltd accepts no liability or responsibility whatsoever for or in respect of any use of or reliance upon this report by any third party.

CONTENTS

1.	CCTV OPERATION SUMMARY	1-6
2.	FOREWORD	2-8
3.	TERMS & DEFINITIONS	3-9
4.	CCTV POLICY STATEMENTS	4-10
4.1.	OWNERSHIP AND CONTROL OF CCTV OPERATIONS.....	4-10
4.2.	ROLE AND PURPOSE OF CCTV OPERATIONS.....	4-10
4.3.	ORGANISATION POLICY FOR CCTV OPERATIONS.....	4-11
5.	CODE OF CONDUCT.....	5-13
6.	CCTV MANAGEMENT PRACTICES	6-15
6.1.	INTRODUCTION.....	6-15
6.2.	KEY PERFORMANCE INDICATORS	6-15
6.3.	OPERATIONAL OBJECTIVES.....	6-15
6.4.	WESTERN AUSTRALIA GUIDELINES	6-16
6.5.	AUSTRALIAN STANDARDS.....	6-16
6.6.	RELEVANT LEGISLATION.....	6-17
6.7.	ACCOUNTABILITY	6-18
6.8.	BREACHES OF THE CODE OF CONDUCT.....	6-18
6.9.	MANAGEMENT FRAMEWORK.....	6-18
6.10.	COMMUNITY SAFETY AND CRIME PREVENTION PLANNING AND CCTV OPERATIONS	6-19
6.11.	KEY ROLES AND RESPONSIBILITIES.....	6-19
6.11.1.	SHIRE OF PINGELLY RESPONSIBILITY	6-19
6.11.2.	WA POLICE RESPONSIBILITY	6-19
6.12.	SURVEILLANCE OFFICER/CEO.....	6-21
6.13.	MONITORING, REVIEW & AUDIT REPORTS & PROTOCOLS	6-22

6.13.1.	MONTHLY MONITORING AND REPORTING.....	6-22
6.13.2.	INDEPENDENT CCTV OPERATION AUDITS	6-22
6.14.	PUBLIC AWARENESS & MEDIA MANAGEMENT.....	6-23
6.14.1.	CCTV SIGNAGE	6-23
6.14.2.	PUBLIC INFORMATION.....	6-23
6.14.3.	MEDIA MANAGEMENT.....	6-24
6.15.	CCTV OPERATION ACCESS CONTROLS	6-24
6.16.	CAMERA MANAGEMENT	6-24
6.16.1.	CAMERA SELECTION.....	6-24
6.16.2.	CAMERA RISK ASSESSMENTS	6-24
6.16.3.	CONTROL AND OPERATION OF CAMERAS	6-25
6.16.4.	MAINTAINING CAMERA OPERATIONS.....	6-25
6.16.5.	RECORDED MATERIAL	6-25
6.16.6.	CONTACT WITH POLICE	6-26
7.	CCTV STANDARD OPERATING PROCEDURES.....	7-27
7.1.	INTRODUCTION.....	7-27
7.2.	CCTV MANAGEMENT.....	7-27
7.3.	MAINTAINING COMPLIANCE AND LOCAL GOVERNMENT BEST PRACTICE	7-27
7.3.1.	REVIEW	7-27
7.3.2.	COMPLAINTS HANDLING	7-27
7.4.	AUTHORISED PERSONNEL - SELECTION AND RECRUITMENT....	7-28
7.5.	SELECTION OF SECURITY CONTRACTORS AND CONSULTANTS ...	7-28
7.5.1.	WA POLICE CONTACTS & BLUE IRIS REGISTER.....	7-28
7.5.2.	JOINT OPERATIONS WITH WA POLICE	7-29
7.6.	CAMERA OPERATION.....	7-29
7.6.1.	CONTROL AND OPERATION OF THE CAMERAS	7-29
7.7.	CAMERA PRESETTING FOR PTZ DIRECTION AND FIELDS OF VIEW	7-29
7.8.	TROUBLESHOOTING, FAULTS AND MAINTENANCE;.....	7-30
7.9.	DATA STORAGE	7-30
7.10.	DATA ACCESS.....	7-30
7.11.	ACCESS TO DESIGNATED SURVEILLANCE OPERATIONS AREAS ..	7-30

7.12.	ACCESS TO AND SECURITY OF THE MONITORS/CONTROL ROOM	7-30
7.13.	CONTINUITY OF EVIDENCE	7-32
7.13.1.	VIEWING OF RECORDED MATERIAL	7-33
7.13.2.	COPYING OF RECORDED MATERIAL	7-33
7.13.3.	RELEASE OF ORIGINAL RECORDED MATERIAL	7-34
7.13.4.	VIDEO IMAGES	7-34
7.13.5.	MASTER COPY SAFEGUARDS	7-34
7.14.	NETWORK CONFIGURATION AND DATA TRANSMISSION	7-36
7.15.	MONITORS AND CONTROLS.....	7-36
7.16.	RECORDING AND STORAGE	7-36
7.16.1.	RECORDING OF IMAGES	7-36
7.17.	SOFTWARE SYSTEM OVERVIEW AND MANUALS.....	7-37
7.18.	SYSTEM WARRANTIES AND MAINTENANCE	7-37
7.19.	WORKSTATION DESIGN AND CAPACITY	7-37
7.20.	GAPS ANALYSIS AND ERROR REPORTING	7-37
7.21.	OPERATION REDUNDANCY AND DISASTER RECOVERY	7-37
8.	MEMORANDUM OF UNDERSTANDING (SAMPLE)	8-38
9.	RELEASE FORM FOR RECORDED MATERIAL.....	9-40
10.	CCTV INCIDENT REPORT	10-41
11.	CAMERA / LOCATION RISK ANALYSIS - QUALITATIVE	42
11.1.	CAMERA RISK ASSESSMENT - Camera Number(s) / Location(s).....	44
12.	AUSTRALIAN & INTERNATIONAL RESEARCH PUBLICATIONS	47

1. CCTV OPERATION SUMMARY

POLICY NUMBER & REFERENCE:	
CCTV SYSTEM OWNER & OPERATOR:	'SHIRE OF PINGELLY'
REPORTING COMMITTEE:	'CHIEF EXECUTIVE OFFICER'
ADOPTED BY COUNCIL: DATE/ COUNCIL MINUTES REF: REPLACES POLICY:	17 July 2013
CCTV OPERATION REPORTS/AUDITS: DATE / COMMITTEE MINUTES REF:	
POLICY AMENDED / REVIEWED: DATE / COMMITTEE MINUTES REF:	
CCTV SYSTEM SUMMARY:	
WA POLICE BLUE IRIS REF:	"NUMBER" (<i>Note: To populate entire Manual - Press Ctrl F - Replace - NUMBER - YOUR REF NUMBER</i>)

DISTRIBUTION OF COPIES

REVISION No.	COPY FOR	QUANTITY	ISSUED TO	DATE

2. FOREWORD

The public perception of CCTV systems in Australia is maturing and concerns of privacy have dissipated over the recognised safety advantages afforded by public space CCTV. It is the responsible and appropriate management of the CCTV system and recorded footage which is the primary focus for public attention and scrutiny.

The CCTV Operation should be recognised as a significant and contributing asset to the SHIRE OF PINGELLY. The broad application of the CCTV Operation in Local Government Management is widely evident and should be acknowledged for its contribution to a range of local and state government activities. There is an inherent but often hidden value which is difficult to document and measure in real dollar terms, however each local government should continue to seek out measurable returns on investment as CCTV Operations develop.

The development of the CCTV Management and Operation Manual is to provide a functional means of managing CCTV in accordance with the WA CCTV Guidelines and related publications, legislation and standards. The Manual is designed to form the basis on which to align strategic and operational functions. Importantly, the manual will provide a ready reference for any issue pertaining to the CCTV system's management, operations, technical specifications and functionality.

Consultant Note

This Manual has been written as a standalone, live document intended for public space CCTV Systems installed by WA local government organisations. The manual is designed to support and be read in conjunction with the WA CCTV Guidelines and related publications.

This manual assumes that there is a common intention amongst all stakeholders to improve the effectiveness of CCTV and ensure the public is appropriately protected by robust and audited protocols. Any aspect of the manual may be amended to suit specific requirements.

Any inquiries concerning the manual may be directed to Chris Cabbage,
ccabbage@amlethouse.com

3. TERMS & DEFINITIONS

“Authorised Personnel” means any delegated officers of the SHIRE OF PINGELLY's Chief Executive Officer and WA Police Commissioner listed in the CCTV Management Spreadsheet.

“Duty Surveillance Officer” means the delegated officer in charge of CCTV Operation, nominated under Authorised Personnel in the CCTV Management Spreadsheet.

"CCTV" or Closed Circuit Television is defined as a television system that transmits images on a 'closed loop' basis, where images are only available to those directly connected to the transmission system. The transmission of closed circuit television images may involve the use of coaxial cable, fibre-optic cable, telephone lines, infra-red and radio transmission systems. A hand held camera is not included in this definition unless it is connected to the SHIRE OF PINGELLY's CCTV transmission system or operated as a covert camera.

"CCTV Management Spreadsheet" accompanies the Manual to record CCTV Operations information and data for reporting purposes.

"CCTV Operations" means all aspects of public space CCTV surveillance management, use, recording, maintenance and access to recorded material.

"Covert or mobile camera" is a camera without a designated, fixed location and is used either to record activity covertly or for short periods of time in a target area. Covert or mobile cameras operated by the SHIRE OF PINGELLY for the purpose of detecting criminal offences or behaviour will be considered to form part of CCTV Operations and will be managed and operated in accordance with this Manual.

"Designated Surveillance Operation Areas" means any room or record relating to CCTV Operations, CCTV hardware, control software administration and where access to recorded material may be gained or available.

"Public place" refers to public reserves, public roads or streets, public bridges, with the addition of public transport and car parks, public wharfs, public baths or swimming pools.

"Private premises" refers any area not openly accessible to the general public, including semi public spaces and includes private residences and private or commercial businesses.

“Situation of concern” means a situation which may lead to a breach of Statute Law, where it appears that a person(s) may be in physical distress, or a situation likely to cause a public disturbance.

"Situation of interest" means any situation which may verify area activity or potentially escalate to a situation of concern.

"Stakeholder" means any organisation or group who has a reasonable and justified interest in aspects of public space CCTV surveillance management, use, recording, maintenance and access to recorded material

For a detailed GLOSSARY OF CCTV TERMS refer to the WA CCTV Technical Advice ([Link here](#)).

4. CCTV POLICY STATEMENTS

4.1. OWNERSHIP AND CONTROL OF CCTV OPERATIONS

The CCTV Operation is owned by and is the sole property of the SHIRE OF PINGELLY;

The SHIRE OF PINGELLY will conduct CCTV Operations in accordance with approved CCTV Management Practices and Authorised Personnel will abide by the Code of Conduct, provided in the CCTV Management and Operations Manual.

The SHIRE OF PINGELLY Duty Surveillance Officer has delegated control over the CCTV Operation.

The SHIRE OF PINGELLY CCTV Organisational Policy establishes the purpose, key functions, and control parameters set by the SHIRE OF PINGELLY, in order to achieve the following:

1. Maintain best practice and standards with reference to the Western Australian CCTV Guidelines, available at www.crimeprevention.wa.gov.au.
2. Manage CCTV Operations in compliance with Australian Standards 4802:2006, Parts 1 – 4, and future or superseding standards.
3. Manage CCTV Operations in compliance with Commonwealth and Western Australia legislation and amendments which may affect the use of CCTV and recorded material. The relevant and primary areas of compliance are privacy laws, camera field's of view and recording parameters, data storage, access control, and freedom of information provisions.
4. Operate, use and maintain CCTV Operations in accordance with the Code of Conduct, acknowledged and signed annually by Authorised Personnel.
5. Operate, use and maintain CCTV Operations to maintain effective oversight of Monitoring, Review, Auditing and Reporting.

4.2. ROLE AND PURPOSE OF CCTV OPERATIONS

The SHIRE OF PINGELLY conducts CCTV Operations in order to:

1. Deter, detect and respond to criminal offences against person or property;
2. Facilitate and support an effective response by SHIRE OF PINGELLY Authorised Personnel, WA Police Officers or other emergency services personnel to situations of concern or interest; and
3. Manage and maintain community safety for residents, traders, retailers, workers, visitors and SHIRE OF PINGELLY staff.

4.3. ORGANISATION POLICY FOR CCTV OPERATIONS

The SHIRE OF PINGELLY's CCTV Policy provides for the manner in which the CCTV Operation will be operated, managed and the reporting protocols to the SHIRE OF PINGELLY's Chief Executive Officer ('CEO') and WA Police.

CCTV Management Practices will ensure CCTV Operations will be conducted in accordance to the following policy statements:

1. The CCTV System will be operated within applicable law, and for the ethical and beneficial purposes for which it is established or which are subsequently agreed in accordance with these approved policy statements.
2. The CCTV System will be operated with due regard to the privacy and civil liberties of individual members of the public, including the rights to freedom of religious and political expression and assembly.
3. The public interest in CCTV Operations will be recognised by ensuring the security and integrity of recorded material.
4. All Stakeholders and Authorised Personnel will act in accordance with the CCTV Operation's Code of Conduct.
5. Access to Designated Surveillance Areas will be restricted to Authorised Personnel or with written authorisation from the designated Duty Surveillance Officer.
6. The SHIRE OF PINGELLY will be accountable to its Stakeholders for the effective management and control of CCTV Operations.
7. CCTV Operations will be monitored and evaluated to verify compliance and report annually on nominated key performance indicators.
8. The SHIRE OF PINGELLY will make public annual reports in relation to CCTV Operations.
9. Recorded material released to Stakeholders shall be verified for accuracy, relevance and must not exceed that necessary to fulfil the purposes of the written request.
10. The retention of, and access to any recorded material will be only for the purposes provided by CCTV Policy Statement 4.2.
11. Recorded material will be retained for thirty one (31) days unless otherwise specified or required in relation to an approved police operation or the investigation of crime or events for court or formal review proceedings by the SHIRE OF PINGELLY. Recorded material, hard copy or electronic will then be erased, deleted or destroyed, with released material destroyed following written confirmation on the original release request.
12. Contact and exchange of information between the SHIRE OF PINGELLY and WA Police will be conducted in accordance with a signed Memorandum of Understanding.
13. Legitimate access may be allowed to live CCTV images which may be required by City Business Unit personnel to view public areas for convenient public area familiarisation or reviewing, monitoring or verifying SHIRE OF PINGELLY maintenance services and public works.
14. Access to CCTV Operations should remain with existing Authorised Personnel with City Business Units allowed to access the system; however any access will be formally recorded and included in monthly reporting.
15. CCTV Operations will make all reasonable attempts to serve the interests of all who may be affected by public space surveillance with a focus on community safety and crime prevention, and not be confined to the interests of the SHIRE OF PINGELLY or operational needs of the WA Police.

5. CODE OF CONDUCT

THIS CODE OF CONDUCT HAS BEEN DEVELOPED TO ENSURE THAT THE HIGHEST ETHICAL STANDARDS ARE MAINTAINED BY ALL AUTHORISED PERSONNEL WHO WORK AT THE SHIRE OF PINGELLY AND WITHIN THE CCTV OPERATION.

NON COMPLIANCE WITH CODE OF CONDUCT

CCTV Operations require the high standards of integrity and honesty. As a consequence, any breach of this Code of Conduct could result in disciplinary action, up to and including dismissal and criminal proceedings.

ETHICAL USE OF CCTV SYSTEMS AND RECORDED MATERIAL

The SHIRE OF PINGELLY as the highest expectation of all Authorised Personnel to:

- At all times, act in an honest and legal manner to carry out duties which reflects community values.
- Treat all live and recorded images in an ethical manner and with the utmost of care, respect and dignity.
- Interact with WA Police and stakeholders in a timely, courteous and cooperative manner.

CONFIDENTIALITY

The SHIRE OF PINGELLY expects Authorised Personnel to ensure confidentiality of information gathered by or from CCTV Operations by not disclosing or discussing any events with unauthorised Personnel or associates who have no direct responsibility relating to CCTV Operations.

In addition, Authorised Personnel will explicitly not identify any involved person or party with family, friends, or acquaintances and will not disclose any information to third parties, including the media without prior written approval in accordance with CCTV Operation Policy.

OPERATING CONDITIONS

In recognition of CCTV Operation environments and Designated Surveillance Areas, Authorised Personnel will carry out duties in a calm, noise free manner, and will leave areas clean, neat and tidy at the end of each shift.

Other than Authorised Personnel, written authorisation is required from the Duty Surveillance Officer, for visitors to enter designated surveillance areas. Visitors will sign a Visitor's Book.

Written reports documenting the recording or reporting of situations of concern, will take place as soon as practicable. Reports must be written in simple, non-offensive English that will not cause offense or embarrassment should the record be made public or subpoenaed.

In the course of carrying out duties, CCTV Operations must not be used for personal benefit or invade individual or group privacy. Cameras should only be used in accordance with Policy Statement 4.2 and have priority for when there is an operational necessity or a reasonable belief that an offence has or is likely to occur.

Recorded material shall only be released when requested in writing on an approved application and authorisation by the Duty Surveillance Officer.

Recorded Material shall not be copied or taken from Designated Surveillance Areas without an approved written application and authorisation by the Duty Surveillance Officer.

CCTV Operational records (hard copy or electronic) can only be destroyed with written authorisation by the Duty Surveillance Officer and in accordance with approved CCTV Operating Procedures.

REPORTING A BREACH OF THE CODE OF CONDUCT

Should any person become aware that an officer of the SHIRE OF PINGELLY's work behaviour is or was inappropriate, and the incident has not been dealt with through normal supervisory procedures, then the person is obliged to report the incident to DESIGNATED PERSON. In return, the DESIGNATED PERSON will guarantee that any reported matters will be handled with sensitivity and without repercussion.

I have read and understood the CCTV Operation's Code of Conduct and agree to abide by these conditions and implications for any breach.

SIGNATURE:..... DATE:.....

6. CCTV MANAGEMENT PRACTICES

6.1. INTRODUCTION

CCTV Management Practices establish the operational objectives and performance indicators for CCTV Operations, with a focus on nominated outcomes relevant to camera locations and other defined target areas.

Each of the key Stakeholder relationships should be defined, with a focus on WA Police. Management protocols and guidelines are supported by the Code of Conduct and a Memorandum of Understanding (MOU).

CCTV Management requires continued commitment for the monitoring, review and audit process, in addition to planning and finance procedures, relating to the CCTV Operations. Executive oversight and CCTV Management should constantly seek out areas for improvement for increased system efficacy.

6.2. KEY PERFORMANCE INDICATORS

Establishing clear and concise Key Performance Indicators (KPI's) for CCTV Operations will allow effective reporting and monitoring of system efficacy and quickly highlight trends concerning fundamental operations, which may require early intervention or closer monitoring by CCTV Management and the CHIEF EXECUTIVE OFFICER.

Recommended CCTV Operation KPI's are to include the following:

1. Possible versus Actual Surveillance Hours conducted.
2. Number of Incidents detected.
3. Number of Incidents responded too.
4. Number of requests/applications for recorded material.
5. Time frame for responding to applications for recorded material.
6. Number of requests for maintenance or system repair.
7. Time frame for maintenance repair and response.

6.3. OPERATIONAL OBJECTIVES

The objectives established for CCTV Operations should be based on measurable criteria, which may include:

- Reducing Reported Crime and Incidents to Police
- Reducing Reported damage and graffiti to the SHIRE OF PINGELLY
- Improving perceptions of safety and reducing Fear of Crime following community consultations.

Targets should be realistic and able to be monitored over a specified term, such as 3, 6 or 12 months, supported by longer term 3 to 5 year plans.

6.4. WESTERN AUSTRALIA GUIDELINES

Western Australian guidelines relating to CCTV Operations should be read in association with the CCTV Management and Operations Manual include:

- WA State CCTV Guidelines
- WA CCTV Technical Advice
- WA CCTV Analogue to Digital CCTV System Migration Guidelines
- WA Planning Commission Designing Out Crime Guidelines.

6.5. AUSTRALIAN STANDARDS

Standards Australia's CCTV standards cover the latest CCTV technologies, procedures and are reported to be the most up to date CCTV standards available in the world). In Australia, best practice CCTV Operation guidelines may refer to the following:

- AS 4806.1–2006–Closed circuit television (CCTV)–Part 1: Management and operation.
Includes chapters on; principles and management of the CCTV system, procedures, personnel, CCTV control room, effective response, privacy and disclosure issues, recorded material management, documentation, licences and CCTV signage. There are appendices on Authorised Personnel recruitment and selection and a summary of current Australian Legislation for all states and territories.
- AS 4806.2–2006–Closed circuit television (CCTV)–Part 2: Application guidelines.
Includes chapters on, general CCTV considerations, system design criteria, objective test plan, installation, commissioning and handover, preventative maintenance, licences and signage. There are appendices on abbreviations and terminology, objective testing techniques, objective tests and measurements using a test chart, objective tests and measurements using a test pattern generator and test targets.
- AS 4806.3–2006–Closed circuit television (CCTV)–Part 3: PAL signal timings and levels.
Includes video signal timings from the Australian Broadcasting and Media Authority Technical Planning Guidelines and video signal level variables for CCTV systems which have been determined from many tests over many years.
- AS 4806.4–2008–Closed circuit television (CCTV)–Part 4: Remote video.
Sets out requirements and recommendations for the design, installation, commissioning, operation and remote monitoring of detector-activated alarm verification, interactive video management and remotely monitored CCTV surveillance systems.
- AS/NZS 1158:2005 Lighting for Roads and Public Spaces.
Defines Category P lighting which is applicable to roads on which the visual requirements of pedestrians are dominant, e.g. local roads and to local area traffic management devices (LATMS) installed on such roads. Also lighting which is applicable to outdoor public areas, other than roads, where the visual requirements of pedestrians are dominant, e.g. outdoor shopping precincts. Subcategories range from P1 to P12.
- AS 2201.1:2007 Security Installations;
- AS/ACIF S009:2008 Cabling Provider Rules;
- AS/NZS 1768:2007 Lightning protection.
- ISO 31000:2009 Risk Management (Supersedes AS/NZ 4360:2004)

- HB 167: 2004 Security Risk Management Handbook.
- AS 2342:1992 Development, testing and implementation of information and safety symbols and symbolic signs.
- AS2416:2002 Provides examples and the display of multiple hazard signage.

6.6. **RELEVANT LEGISLATION**

CCTV Operations will be conducted in accordance with Commonwealth and State Legislative requirements, which includes:

Commonwealth

Privacy Act 1988	Establishes and regulates privacy principles for individuals, corporate entities and personal information.
Surveillance Devices Act 2004	Regulates use of optical surveillance devices without warrant

Western Australia

Criminal Investigation Act 2006	Provides powers for the investigation and prevention of offences and for related matters.
Occupational Health and Safety Act 1984	Regulates the protection of persons at or near workplaces from risks to health and safety
Surveillance Devices Act 1998	Regulates use, installation and maintenance of optical surveillance devices
Security and Related Activities Act 1996	Regulates WA Security Providers
Security and Related Activities Regulations 1997	Regulates WA Security Providers

6.7. ACCOUNTABILITY

The SHIRE OF PINGELLY is responsible for ensuring that CCTV Operations will be reviewed annually subject to evaluation to identify whether its purposes are being complied with and whether objectives are being achieved.

Resources committed to CCTV Operations will include the cost of independent evaluations and public disclosure provisions.

Evaluation of CCTV Operations will include, as a minimum:

- a) Assessment of its impact upon crime;
- b) Assessment of its impact on neighbouring areas;
- c) Assessment on its impact on improving perceptions of safety and reducing 'Fear of Crime' by members of the public.
- d) The views of the public on the operation of the CCTV program;
- e) Compliance with the Code of Conduct, protocols and standard operating procedures; and
- f) Whether the purposes for which the CCTV Operation was established still exist.

The results of evaluations will be considered for future management and functioning of CCTV Operations.

6.8. BREACHES OF THE CODE OF CONDUCT

The CCTV Management and Operations Manual has been established to address the interests of all who may be affected by public CCTV surveillance and will not be confined to the interests of the SHIRE OF PINGELLY or the needs of the Community Safety and Crime Prevention Plan.

Prime responsibility for ensuring the Code of Conduct is adhered to rests with the SHIRE OF PINGELLY. This responsibility includes ensuring that breaches of the Code are investigated and remedied to the extent that breaches of the Code are within the ambit of SHIRE OF PINGELLY power to remedy.

Complaints in relation to any aspect of CCTV Operations must be made in writing to:

The Chief Executive Officer, SHIRE OF PINGELLY, 17 Queen Street Pingelly WA 6308

SHIRE OF PINGELLY will cooperate with the investigation of any complaint about the SHIRE OF PINGELLY CCTV Operations conducted by W.A. Police or Crime and Corruption Commission.

6.9. MANAGEMENT FRAMEWORK

The SHIRE OF PINGELLY has implemented a management framework, namely the (CHIEF EXECUTIVE OFFICER) with oversight responsibilities for CCTV Operations. The (CHIEF EXECUTIVE OFFICER) will maintain a management overview of CCTV Operations with reference to CCTV Policy and Procedures, comprising of this manual.

6.10. COMMUNITY SAFETY AND CRIME PREVENTION PLANNING AND CCTV OPERATIONS

The CCTV Operation should be acknowledged in strategic crime prevention planning with a focus on monitoring priority crimes, providing key statistics on crime prevention initiatives and integrating system design, such as camera placement and acknowledging existing camera positions, with specific crime prevention approaches or initiatives.

6.11. KEY ROLES AND RESPONSIBILITIES

In developing the CCTV Management and Operations Manual, the discrete roles and responsibilities of the CCTV system owner, Duty Surveillance Officer, Authorised Personnel and the police must be made explicit. The responsibilities of each should include the following:

6.11.1. SHIRE OF PINGELLY RESPONSIBILITY

The SHIRE OF PINGELLY is responsible for the following key functions:

- a) developing a Local Crime Prevention Plan which incorporates CCTV strategies
- b) appointing a Duty Surveillance Officer to manage the implementation and operation of CCTV
- c) implementing a comprehensive consultative program with business groups, individuals, government instrumentalities and organisations, and cultural/community groups affected by the program
- d) implementing a community information program
- e) financing the implementation and ongoing costs of CCTV. This includes an independent evaluation of its effectiveness
- f) developing, implementing and monitoring the auditing procedures for the implementation of CCTV as a crime prevention strategy
- g) developing and implementing an effective complaints handling mechanism
- h) monitoring the effectiveness of CCTV as part of a crime prevention strategy
- i) selecting appropriately qualified personnel to install and operate CCTV
- j) providing inductions and training to staff involved in operating and working with the CCTV program
- k) ensuring that all relevant parties comply with the Code of Practice, Protocols and Standard Operating Procedures

6.11.2. WA POLICE RESPONSIBILITY

The WA Police is not responsible for funding or for the operation of the SHIRE OF PINGELLY's CCTV Operation. Police involvement will only be to the level that its resources and priorities allow and will be determined by the local Officer in Charge. However, the WA Police should be consulted and involved in all phases of the process leading to the installation and operation of a scheme, including participation on the CHIEF EXECUTIVE OFFICER and participation on or acting in an advisory capacity to CCTV sub-committees, conducting a crime assessment and determining evaluation procedures

These Standard Operating Procedures set out clearly the guidelines and protocols for communication with the police and the provisions in place for an adequate and appropriate police response to reported incidents. This would include the early identification of emerging incidents to facilitate the timely initiation of police response.

The WA Police will be responsible for:

- a) providing information for and advice on the crime assessment
- b) developing, in consultation with the SHIRE OF PINGELLY the Protocols and Standard Operating Procedures between police and the SHIRE OF PINGELLY in relation to their respective roles in accordance with the MOU.
- c) training local police in their responsibilities in relation to the CCTV Operation as set out in the MOU
- d) ensuring police officers comply with the Code of Conduct and in accordance with the MOU
- e) participating in the evaluation and monitoring processes for the CCTV Operation
- f) determining the appropriate level and priority of responses required to incidents identified by the CCTV cameras, according to available resources and existing priorities.

6.12. SURVEILLANCE OFFICER/CEO

The role and duties of the Surveillance Officer/CEO include:

- a) Act upon any Delegated Authority to ensure Council's Policies and requirements of relevant statutes are exercised and complied with. Report to the CHIEF EXECUTIVE OFFICER or relevant SHIRE OF PINGELLY authority on the requirement in respect of possible litigation or other legal action.
- b) Report to the CHIEF EXECUTIVE OFFICER on any significant need for CCTV System modifications or procedures, where appropriate.
- c) Regularly liaise with the WA Police in respect to recorded incidents, requests for recorded material, crime statistics, general trouble spots and other relevant matters to ensure the activities of the CCTV Operation complement Police priorities.
- d) Liaise with business and community group representatives to ensure their security needs are addressed and catered for whenever possible.
- e) Take an active part in improving the effectiveness of the Community Safety and Crime Prevention Planning in terms of CCTV Operations.
- f) Implement CCTV surveillance strategies to problem areas throughout the SHIRE OF PINGELLY when necessary.
- g) Review this CCTV Management and Operations Manual adopted in respect to the needs of the SHIRE OF PINGELLY and recommend changes when necessary.
- h) Keep abreast of CCTV technology, practices and all introduced amendments to related legislation and where necessary introduce changes to maintain operational and legislative compliance.
- i) Assume responsibility for the CCTV Management Spreadsheet and monitor incident reports for correct completion in respect to names, addresses, vehicle descriptions if applicable etc. and that the evidence obtained in respect to each is of a sufficient quality to support prosecutions in the event of contested matters.
- j) Act on delegated authority in conjunction with the release and destruction of recorded material after assessing the evidence available and the circumstances of the matter.
- k) Ensuring compliance with the CCTV Code of Conduct.
- l) Act on delegated authority to allow visitors to access Designated Surveillance Areas when considered appropriate or necessary.
- m) Ensure CCTV related complaints, correspondence and reports are effectively investigated, prepared and completed within required time frames.
- n) Ensure that Authorised Personnel perform at a high level through the development, training and management of CCTV Operations.
- o) Represent and promote CCTV Operations and the interests of the SHIRE OF PINGELLY when required to attend various meetings, public forums or as a member of an advisory group.
- p) Foster a high standard of public relations in support of CCTV Operations.

6.13. MONITORING, REVIEW & AUDIT REPORTS & PROTOCOLS

6.13.1. MONTHLY MONITORING AND REPORTING

The CCTV Operation Spreadsheet should be presented for review in a monthly dashboard style report to the CHIEF EXECUTIVE OFFICER for a review of the following:

- a) Strategic Objectives are linked with clear updated outcomes.
- b) Assessment of KPI's and trends.
- c) The number and type of incidents reported.
- d) The number of cameras operational versus total number of cameras
- e) CCTV System faults, types and acceptable response timeframes
- f) Closely monitor trends or spikes of activity, such as total number of incidents and set targets for review or triggers for trend response for the following month.
- g) Include Monthly System real dollar value from the monthly Asset Register depreciation.

CCTV System Annual Reports should be presented with an Executive Summary and written with a view of being released to the public on the SHIRE OF PINGELLY website. The topics covered within the annual report should include details of the following:

- a) A description of the system and the geographical area(s) of operation.
- b) The system's policy statement.
- c) The purpose and scope of the system.
- d) Any changes to the operation or management of the CCTV system.
- e) Any changes that have been made to the policy.
- f) Any proposals to expand or reduce the operation of the system.
- g) Details of the CCTV Operation's achievements during the previous 12 months. The assessment of the system's performance should include an assessment of the CCTV system's impact on crime levels and types of crime in the area covered by the system.
- h) The aims and objectives for the next 12 months.
- i) The amount and type of data that has been stored, and whether this amount is excessive in terms of likely need.
- j) The amount and type of data that has been destroyed, and whether the data has been destroyed in accordance with privacy and other compliance criteria.

6.13.2. INDEPENDENT CCTV OPERATION AUDITS

In accordance with AS4806.1:2006 Part 3.4 where CCTV Systems operate within the public domain, consideration should be given to an independent audit before publication of the annual

report. As a minimum, an independent CCTV Operation Audit should be conducted every two years.

CCTV System Independent Reports should be addressed to the SHIRE OF PINGELLY Chief Executive Officer and submitted to the CHIEF EXECUTIVE OFFICER for management of audit recommendations. Audit reports are not required to be released to the public. The audit should consider the following:

- a) Independent verification of the attainment of objectives and procedures.
- b) Random audits of the access and data logs and the release and destruction of recorded material.
- c) Review and evaluate CCTV Policy Statements and compliance.
- d) Review and evaluate procedures and costs for the release or viewing of information.
- e) Review of any proposed System Expansion/Upgrade, Commissioning and Testing protocols;
- f) Review and verification of the existing or suitable CCTV network configuration, coverage, functionality, effectiveness and efficacy.
- g) Review of the existing or suitable CCTV Surveillance or Monitoring Centre design and functionality;
- h) Evaluation of current and future public space design and construction considerations, including a Crime or Incident Prevention Policy;
- i) Assessment of future land use expectations, needs, including public transport and traffic management considerations;
- j) Assessment of related strategic planning and vision statements;
- k) Assessment and review of related target area works, studies and incidents.

6.14. PUBLIC AWARENESS & MEDIA MANAGEMENT

6.14.1. CCTV SIGNAGE

The importance of effectively placing CCTV signage in the monitored area cannot be underestimated. Location, height and existing visual distractions are major factors which contribute to the effectiveness of a sign when installed. CCTV signage should be considered to be a safety orientated sign and used for crime prevention purposes.

Signage can play a critical role in a CCTV Operation's effectiveness on influencing behaviour and perceptions of safety within the public space. It is recommended that signs be erected at all formal or high traffic access points within the monitored area and at each camera location. Signs should be checked regularly for damage or theft.

As referred to in AS4806.1:2006, Part 11, signage at all CCTV system site entries (as a minimum) shall comply with the applicable Federal, State and Territory Privacy and Surveillance Legislation and shall comply with the requirements of AS 2342. For other examples and the display of multiple hazards, also refer to AS2416-2002.

It is important that CCTV signage be installed in positions which allow the best opportunity to capture the attention of pedestrians and thus improve safety and crime risk management:

6.14.2. PUBLIC INFORMATION

The SHIRE OF PINGELLY will make available this manual on the SHIRE OF PINGELLY website.

Public inquiries and complaints in relation to the SHIRE OF PINGELLY CCTV Operation must be made in writing to:

Chief Executive Officer, SHIRE OF PINGELLY, 17 Queen Street Pingelly WA 6308

6.14.3. MEDIA MANAGEMENT

The SHIRE OF PINGELLY holds a range of public events throughout the year, as well as, the release of media articles and news stories. A schedule of suitable stories and events, related to and consistent with CCTV Operation objectives, may be considered by the CHIEF EXECUTIVE OFFICER to promote the use and effectiveness of CCTV Operations to public stakeholders.

The release of any recorded material to the media will be only for the purposes provided by CCTV Policy Statement 4.2.

6.15. CCTV OPERATION ACCESS CONTROLS

Access to **Designated Surveillance Operation Areas** will be restricted to Authorised Personnel.

6.16. CAMERA MANAGEMENT

6.16.1. CAMERA SELECTION

Cameras should be risk assessed for the public area's environmental and lighting conditions, mounting options, the type of area activity to be expected.

The selection criteria for each camera placement and location should be documented and the effectiveness of the installation should be measurable and reviewed annually. An objective measurement is the camera's purpose, either to *detect*, *recognise* or *identify*. The effectiveness of the camera should therefore be found to directly attribute to safety, perception of safety, control of crime or assist City or Area management functions. This design base will allow documented design, commissioning, performance and monitoring of each camera and subsequently, the whole system.

Each camera should be housed in a vandal resistant, tinted environmental dome, rated to IP66, which both protects the camera and ensures that the camera itself, such as lens direction, is not clearly visible or accessible from the ground.

The location of the cameras should be clearly apparent to the public.

The CCTV System should be reviewed and specified to ensure maximum resolution and picture quality.

A replacement or upgrade program based on system value should be implemented for the proceeding three (3) to five (5) years.

6.16.2. CAMERA RISK ASSESSMENTS

AS/NZS 31000:2009: Risk Management describes how the objectives of analysis are to separate acceptable risks from major risks. Risk analysis involves the consideration of the sources of risk, their consequences and the likelihood that those consequences may occur.

It is important to recognise how the CCTV camera will influence the consequences of any particular risk event which will impact in different ways within the target area. Financial costs, personal harm (physical and psychological), legal consequences and damage to reputation may all result from a single incident.

6.16.3. CONTROL AND OPERATION OF CAMERAS

FIXED CAMERAS

Fixed cameras should be selected for defined fields of view which have a designated and defined purpose, either to detect, recognise or identify. Refer to the WA CCTV Guidelines for detailed information on fixed cameras.

CONTROL OF PTZ CAMERAS

The operation and use of cameras will be in accordance with the Code of Conduct, Code of Practice, and Standard Operating Procedures.

Cameras will not be used to look into or monitor adjacent or nearby premises or buildings, unless it is explicitly for following (in real time) participants in a 'situation of concern', which originated in the public domain.

Any misuse is to be treated as a breach of the Code and subject to disciplinary action.

No audio will be recorded in public places.

Only Authorised Personnel will have access to camera operating controls

All Authorised Personnel will be made aware that recordings are subject to routine audit and they may be required to justify their interest in a particular member of the public or premises.

6.16.4. MAINTAINING CAMERA OPERATIONS

At any time, CCTV Management should provide an overview of the CCTV Operation, as follows:

1. Maintenance of CCTV recording equipment in a fully functional working order;
2. Maintenance of clear, recorded vision from each camera at all times with records of down times.
3. Monitoring for obstructions (foliage, umbrella's, street trees and signage) and report on treatments against obstructions;
4. Ensuring any equipment fault is recorded and attended to in the shortest possible time frame;
5. Ensuring all Authorised Personnel contact lists are updated and current;

For further information on live CCTV monitoring, refer to Part 12: Research Publications.

6.16.5. RECORDED MATERIAL

The retention of and access to recorded material will be only for the purposes provided by the Code of Practice and retrieved and treated in accordance with the Code of Conduct.

Recorded material will be retained for 31 days unless they are required in relation to the investigation of crime or for court proceedings.

Remnant recorded material will be purged following 31 days.

Access to and use of recorded material and photographs will only take place:

- in compliance with the needs of police in connection with the investigation of crime; or
- if necessary for the purpose of legal proceedings.

Recorded material and photographs will not be sold or used for commercial purposes or the provision of entertainment. Such practice will be a breach of the Code of Conduct and subject to dismissal proceedings.

The showing of recorded material to the public will be allowed only in accordance with the public and media management policy or in accordance with the needs of the police in connection with the investigation of crime or in any other circumstances justified and authorised by law. The CEO must formally approve any such action.

Use of recorded material by the media should only occur to gain public information with respect to the identity of a person/s wanted in connection with a criminal investigation. Subject to the concurrence of the Police, the CEO may approve such releases. In such case the recognisable characteristics of other people in the footage shall be obscured.

Appropriate security measures and audit trails will be established against unauthorised access, alteration, disclosure, accidental loss or inadvertent destruction of recorded material.

Recorded material will be treated according to defined procedures and audit trails to ensure continuity of evidence.

6.16.6. CONTACT WITH POLICE

Contact related to CCTV Operations between SHIRE OF PINGELLY Authorised Personnel and the W.A. Police will be conducted strictly in accordance with the Code of Conduct and Code of Practice.

Police officers will not be permitted to remove any recorded material, operate CCTV equipment or have contact with recorded material at any time unless under the terms of this Code of Practice, the Protocols or Standard Operating Procedures or specified in an MOU or following the execution of a search warrant or other relevant, lawful process.

The Pingelly Police have and maintain a live feed from the Council CCTV system for operational purposes.

7. CCTV STANDARD OPERATING PROCEDURES

7.1. INTRODUCTION

These Standard Operating Procedures (SOPs) provides an initial framework for the establishment of tailored procedures specific to the CCTV Operations implemented by the SHIRE OF PINGELLY. The objectives of the SOPs are:

- a) To provide personnel with all the safety, health, environmental and operational information necessary to perform their roles and responsibilities properly.
- b) To ensure that CCTV Operations are performed consistently to maintain quality control of processes and recorded material.
- c) To ensure that CCTV Operations continue with minimal disruption and are conducted to a prescribed standard.
- d) To ensure that any system failures or faults are detected and responded to efficiently and rectified as soon as possible
- e) To ensure that approved procedures are followed in compliance with SHIRE OF PINGELLY and legislative requirements.

7.2. CCTV MANAGEMENT

The SHIRE OF PINGELLY Surveillance Officer shall record all requests for recorded material, all material copied, number of surveillance hours, system faults and maintenance, and access to Designated Surveillance Areas.

The CCTV records shall be kept in a secure location and shall not be altered or have information removed at any time without the approval of the Duty Surveillance Officer.

Exchange of information between WA Police and the SHIRE OF PINGELLY is to be noted and recorded subjectively.

7.3. MAINTAINING COMPLIANCE AND LOCAL GOVERNMENT BEST PRACTICE

7.3.1. REVIEW

These procedures shall be reviewed every 5 years and a report on key performance indicators submitted to the Chief Executive Officer and Coordinator of the WA Blue IRIS Program.

7.3.2. COMPLAINTS HANDLING

Wherever a complaint indicates that an information privacy security principle has been breached, the SHIRE OF PINGELLY must conduct an internal review, subsequently reviewable by a statutory body or independent third party.

Complaints which do not indicate a breach of the *Privacy Act 1988* can be handled in the manner set out by the SHIRE OF PINGELLY's complaints handling practice.

7.4. AUTHORISED PERSONNEL - SELECTION AND RECRUITMENT

All Authorised Personnel must be duly authorised by the SHIRE OF PINGELLY to undertake defined roles.

All SHIRE OF PINGELLY Authorised Personnel shall have a police clearance certificate.

All Authorised Personnel shall follow these procedures at all times;

All Authorised Personnel shall sign the approved Code of Conduct;

The employment of Authorised Personnel will comply with all relevant SHIRE OF PINGELLY policies and in accordance with relevant industrial awards and legislation, including equal opportunity and occupational health and safety.

The SHIRE OF PINGELLY will ensure that the selection process provides for thorough validation of the suitability of candidates to work in a CCTV Operations environment.

Authorised Personnel will be subject to disciplinary proceedings in the event of actions that do not comply with the conditions of the Code of Conduct. Where it is proved that personnel have breached any of the conditions of the Code of Conduct, these personnel will not be permitted to access to Designated Surveillance Areas. In appropriate circumstances, the SHIRE OF PINGELLY reserves the right to terminate employment. These conditions will be detailed in all employment contracts.

The Surveillance Officer will ensure that all visitors are briefed regarding the requirements of the Code of Conduct.

7.5. SELECTION OF SECURITY CONTRACTORS AND CONSULTANTS

There is a role for private sector security providers to assist the SHIRE OF PINGELLY in the provision of CCTV Operations and related services, including CCTV design, system installation and system maintenance.

All security providers to the SHIRE OF PINGELLY must provide appropriately qualified personnel and hold relevant licences in accordance with the *Security and Related Activities Act 1996* and current membership of a Security Industry Association guided by a Code of Conduct.

The SHIRE OF PINGELLY should use preferred security providers as recommended by the WA Local Government Association (www.walga.asn.au)

7.5.1. WA POLICE CONTACTS & BLUE IRIS REGISTER

For the day-to-day purposes, the SHIRE OF PINGELLY's contact officer with the Police will either be the Officer in Charge of the local police station or the Police call number 131 444. As appropriate, the Officer in Charge or delegated police officers will liaise with the SHIRE OF PINGELLY Surveillance Officer in regard to police activity with significance for the operation and management of the CCTV System.

Approval for the police use of the CCTV system in any manner will be subject to their agreement to comply with a Memorandum of Understanding and Code of Conduct.

The presence of a Police Officer in Designated Surveillance Areas for a pre-planned operation or ongoing incident is permitted, subject to authorization being given by the Duty Surveillance Officer. Police Officers may direct the operation of cameras.

The SHIRE OF PINGELLY CCTV System will be registered with the WA Police Blue Iris program. If sought by police and viable, a remote control facility at the Police Operations Centre may be allowed. The WA Police must advise the SHIRE OF PINGELLY Duty Surveillance Officer should they wish to access the SHIRE OF PINGELLY CCTV System and may direct cameras during a live incident, provided the actions requested comply with the SHIRE OF PINGELLY CCTV Management and Operations Manual.

A written record will be maintained of any use of the system at the request of the Police. This record will include details of the Police Officer making the request, details of an authorising officer, time and date of the request and reasons for the request.

7.5.2. JOINT OPERATIONS WITH WA POLICE

The WA Police and the SHIRE OF PINGELLY have entered into a Memorandum of Understanding for CCTV Operations;

The SHIRE OF PINGELLY acknowledges the WA Police as a key stakeholder in CCTV Operations;

Members of the WA Police may request the cooperation of the SHIRE OF PINGELLY CCTV Operations for the purpose of surveillance relating to lawful WA Police operations and investigations;

Joint operation requests shall be made by the WA Police officer responsible for coordinating the operation or investigation;

The request shall detail the times and general purpose for which surveillance support is requested;

The CEO may decline to provide cooperation in accordance with the Code of Conduct and Code of Practice;

The CEO may withdraw cooperation at any time during the operation in accordance with the Code of Conduct and Code of Practice

7.6. CAMERA OPERATION

7.6.1. CONTROL AND OPERATION OF THE CAMERAS

Control Room equipment and the remote control of cameras will only be operated by Authorised Personnel or persons/staff under training. All these people will act with the utmost probity.

All use of cameras and recording equipment will accord with the purposes and key objectives of the CCTV System, as developed in training and specific operational instructions, and shall comply with the Code of Conduct.

Cameras will not be used to look into private property without cause. Operational procedures shall be adopted to ensure restraints upon the use of cameras in connection with private premises.

New or proposed camera locations should be determined on the basis of crime statistics provided by the WA Police and other considerations such as input from CCTV operators, City stakeholders, community groups and innovative crime prevention initiatives carried out by the SHIRE OF PINGELLY.

The List of Cameras and Locations is to be maintained in the CCTV Management Spreadsheet.

7.7. CAMERA PRESETTING FOR PTZ DIRECTION AND FIELDS OF VIEW

All cameras will have designated preset fields of view for different times of the day and week. Each PTZ camera will scan the public space to a defined schedule and where system programming allows. Refer to the CCTV System's Operation and Technical Manual for camera setup and scheduling.

7.8. TROUBLESHOOTING, FAULTS AND MAINTENANCE;

All faults and maintenance activity must be recorded.

Faults and Maintenance activity is to reported.

7.9. DATA STORAGE

Refer to the CCTV System's Operation and Technical Manual for storage configuration and commissioning.

Images on reusable media should be copied from the original storage medium in the original file format onto a secure media. This secure media could be Write Only Read Many (WORM) or secure network storage. The term 'secure server' should be taken to mean an environment, including a security management system, which is accredited to a level of at least 'RESTRICTED', as approved by Duty Surveillance Officer. Once the images and associated data have been copied onto the secure media, it should not be possible to have the data overwritten or altered.

The generation of the secure copy should be carried out as soon as possible after the capture to reduce the time and opportunity for the accidental or malicious alteration to images. All imagery Master or Working Copies should be appropriately identified in order to facilitate the storage, retrieval and eventual disposal of case material.

In terms of evidential value there is no difference between bit-for-bit copies of the data on the Master, Working Copies and the images on the storage medium. This does not remove the necessity to protect the Master as an exhibit in case of challenges to evidence handling procedures or image manipulation. The software required for viewing proprietary formats must be available otherwise the images will be inaccessible. It is advisable to store any replay software with each recording to assist with the correct viewing of the files.

The choice of using network storage or WORM should be guided by factors such as volume of data, predicted storage time and longevity of WORM media. Master evidence not stored on WORM requires equivalent levels of protection such as access control and tamper-proof usage logs.

7.10. DATA ACCESS

7.11. ACCESS TO DESIGNATED SURVEILLANCE OPERATIONS AREAS

Only Authorised Personnel are permitted entry to Designated Surveillance Operations Areas;

Other visitors to Surveillance Operations must be authorised by the SHIRE OF PINGELLY duty officer and a record made of the purpose of the visit;

Authorised Personnel and visitors must wear an approved identification card at all times whilst in Designated Surveillance Operations Areas;

Entry to Designated Surveillance Operations Areas is to be secured at all times with physical and electronic access control protocols; and

Authorised identification must be produced in order to gain entry to Designated Surveillance Operations Areas.

7.12. ACCESS TO AND SECURITY OF THE MONITORS/CONTROL ROOM

Access to view monitors, whether to operate the equipment or view the images is strictly limited to staff with that responsibility.

A Control Room Main Log will contain details of all recordings made in relation to 16.8 above. Details of any visitors authorised by this Code, including times of arrival and departure and details of any telephone calls, will be recorded separately.

The Control Room will remain locked at all times. A coded door lock, or similar should strictly control access with a key override. Routine access will only be granted to Authorised Personnel and those under training, as approved by the Duty Surveillance Officer.

It is important that visits do not interrupt the efficiency of the system. Casual or informal visits will not be permitted. Organised parties shall be allowed for lawful and proper reasons to visit and the Duty Surveillance Officer should be present during all organised visits.

Public access to or the demonstration of monitors will not be permitted except for lawful and proper reasons.

Visits by no more than two Police Officers at any one time will be permitted provided that they are on duty and the visit is in connection with liaison, training or purposes of the system. Visit protocols should be in accordance with the MOU.

Security procedures will be the subject of independent audits.

7.13. CONTINUITY OF EVIDENCE

Evidence, in terms of a still image or video footage, is the presentation of visual facts about a crime or an individual that the prosecution presents to the court in support of their case. The image will be presented either as hard copy or on a screen. It is possible to make a bit-for-bit identical copy of a digital image file.

In evidential terms there is no distinction between the copy and the primary or original file because the files are the same and have the same evidential weight. It is not important whether the file is on a stand-alone or networked computer, a server, or on any type of storage medium. This assumes the operation of adequate security against unauthorised and unrecorded access.

If no discipline is applied there can be any number of identical files. For evidential purposes it is essential to be able to demonstrate that the images are authentic and have originated from the files captured in the camera and recorded to the first medium.

Integrity verification is the process of confirming that the data (image, CCTV clip, etc) presented is complete and unaltered since time of acquisition. Relevant questions concerning integrity might include: "Has data been added to, or removed from the file?"; "Has the data within the file been changed?"

Authentication is the process of substantiating that the data is an accurate representation of what it purports to be. Relevant questions concerning authentication would deal with issues such as: "Was the image taken at the time stated?"; "Was the image taken at the place stated?"

It should be noted that standard image processing techniques such as lightness or contrast changes would affect the image integrity but not the image authenticity; however, a change to the clock on a CCTV system could affect the image authenticity but not affect the image integrity. Robust audit trails are required in order to maintain image authenticity.

The audit trail should include the following information (with date and time of action) when available and if appropriate:

- a) Details of the case.
- b) Classification of the image (and any special handling instructions, if relevant) and the name of the person who classified the image.
- c) If the image is third-party generated, information about point of transfer including whether the image is the Master copy, a Working Copy or an exhibit derived from a Working Copy.
- d) Information about capture equipment and/or hardware and software used, including details of the maintenance log relating to capture equipment and calibration of hardware and software.
- e) Identity of the capture operative including third parties and image retrieval officers, where applicable.
- f) Details of exhibits and disclosure officer(s).
- g) Description of the images captured, including sequencing.
- h) Details of retrieval or seizure process and point of transfer, if applicable.
- i) Creation and definition of the Master copy and associated metadata.
- j) Storage of the Master copy.
- k) Any access to the Master copy.
- l) Viewing of the Master and Working Copies, including a record of any associated viewing logs.
- m) Details and reasons for any selective capture.

- n) Any editing applications which may alter the image.
- o) Any details of processing applications allowing replication by a comparatively trained individual.
- p) Electronic history log of processing applications.
- q) Any copying required to ensure longevity of the data.
- r) Cross References on the Master and Working Copies;
- s) Any copying carried out as part of a migration strategy to ensure the replay longevity of the image;
- t) Disposal details and retention time periods.

7.13.1. VIEWING OF RECORDED MATERIAL

WA Police officers, legal representatives acting on behalf of individuals engaged in legal proceedings related to a recorded incident or individuals acting as their own legal counsel in relation to a recorded incident may request to view recorded material relating to an incident or investigation.

Such a request must specify the date, time and location of the incident which the person wishes to view.

Requests by police, legal representatives and individuals shall be made in writing and lodged with the Duty Surveillance Officer.

Requests to view recorded material shall be responded to as soon as reasonably practicable and otherwise within five (5) working days. Police requests are to be dealt with as a priority and response times noted as a key performance indicator.

7.13.2. COPYING OF RECORDED MATERIAL

In most cases a CD or DVD writer will suffice for exporting **single images** and **short video clips** under about ten minutes in length.

For exporting **longer video clips** and for large scale **archiving**, the system should provide one of the following:

- the ability to export video to an external 'plug and play' hard drive via a USB or Firewire connection
- Network port
- Removable hard drive

The Duty Surveillance Officer may authorise the copy of original material where a recorded incident is the subject of police investigation, prosecution or legal proceedings;

Copying of original recorded material is to be made only by SHIRE OF PINGELLY Duty Surveillance Officers or an authorised SHIRE OF PINGELLY Officer. (LIST IN CCTV Management Spreadsheet);

Recording Mediums are to be marked "original" (one only) and "copy" and certified as such by the Duty Surveillance Officer.

Certified copies of recorded material may only be released to the WA Police, legal representatives acting on behalf of individuals engaged in legal proceedings related to a recorded incident, or individuals acting as their own legal counsel in relation to a recorded incident

Certified copies will only be released to the parties named in the written request when permission to do so has been received from an authorised officer of the SHIRE OF PINGELLY and on the completion of the appropriate documentation.

7.13.3. RELEASE OF ORIGINAL RECORDED MATERIAL

Original recordings and still photographs shall not be released to any person or third party unless requested under a search warrant or by court summons or by a recognised legal instrument; and

At no time shall original or copied recordings or still photographs be released to any media organisation, journalist or other individual or group without the approval of the Chief Executive Officer of the SHIRE OF PINGELLY.

7.13.4. VIDEO IMAGES

To allow ease of current and future use of the recordings for investigations and appeals, etc, the CD/DVD should include:

- a) the image sequence or sequences clearly identified;
- b) an easily-read text file stating any requirements for special hardware or software for replay;
- c) all associated metadata (time and date should be bound to the relevant images);
- d) licence-free software enabling the sequences to be viewed correctly;

Other items that could be included:

- a) text data about the originating camera or system;
- b) audit trails;
- c) authentication or verification software;
- d) short test sequence to confirm that the recorded image sequences are being replayed correctly.

7.13.5. MASTER COPY SAFEGUARDS

There are various media on which images can be captured, both reusable and non-reusable. Irrespective of their nature, early transition from 'capture' to 'defining the Master' phases is extremely important. The integrity of images needs to be protected at the earliest stages as this reduces the opportunities for challenges at court.

Accidental alteration or erasure could be detected by noting image number sequences and prevented by:

- a) designating the image file as read only;
- b) activating the mechanical write protect mechanism;
- c) transferring to WORM (Write once read many) media

Protection can also be achieved by controlling access to the file or media by electronic password and/or controlling the viewing of images by electronic encryption.

The Procedure does not rely on any form of 'electronic' protection but neither does it preclude its use. There are several methods for 'electronically' verifying the integrity of an image file. Once applied, any change to the pixel values will be detected although the nature and location of the changes may not be indicated.

7.13.5.1. File integrity techniques

If a 'hash' function is applied to an image, a unique numerical value is calculated for the whole image. The number is embedded in the metadata of the image file. A change in pixel value causes the 'hash' function value to change. This is the basis for most 'authentication' software. Manufacturer specific software for image integrity is becoming increasingly prevalent, as are non-destructive (i.e. fully reversible) editing techniques.

7.13.5.2. Watermarking

Watermarking describes visibly insignificant changes made to the pixel values to incorporate information which changes if the image file is altered. The watermark may then become visible on the picture or even make it unreadable. The primary use for watermarking is to protect the intellectual property rights of the photographer or film maker. Its use may lead to claims that the image is not authentic because the pixels have been changed, therefore the use of watermarking is not recommended for image integrity.

7.13.5.3. Encryption

The image file is encrypted so that the file cannot be opened except with the correct decryption key. This has particular value if images are to be transmitted to or from remote sites. Loss or corruption of either the key or the data may make files unrecoverable.

7.13.5.4. Handling

Images should also be protected from accidental deletion by the careful handling of media. Media should be stored in clean, dry environments and kept away from strong magnetic fields, strong light and chemical contamination. Some media such as CDs and SmartMedia will be damaged if allowed to become dirty or scratched.

The Master is defined and will be documented as such. It will then be stored securely pending its production (if required) at court as an exhibit. Only in the event of any doubt being cast on the integrity of the images will the Master be viewed.

A Working Copy is usually produced simultaneously, or immediately after the Master is defined. The Working Copy, as its name implies, is the version that will be used for investigation and to assist in the preparation of the prosecution file.

All use and movement of the Master will be logged in the audit trail. Similarly any significant use, enhancement and distribution of Working Copies should be logged. The aim is to support the presentation of evidence through legal proceedings. All audit trails should be disposed of when the image files and any analogue copies are disposed of.

7.13.5.5. Define Master and produce Working Copy

The core of the Procedure is the production, definition and storage of a Master which can be examined if required by the court to confirm the integrity of the images. The Master should be:

- a) labelled or named (with due care to the longevity of label and readability of medium);
- b) stored in a form and manner, with software if required, so that the images may be viewed in the future;
- c) kept in accordance with exhibit protocol;
- d) never used, except to make further copies together with appropriate audit trail, or by order of the court to verify integrity.

Police policies should be developed to cater for these requirements. Image files should be in the same format as:

- a) received by the police in the case of third party images
- b) first captured on medium in/or attached to camera;
- c) as recorded after transmission from camera.

7.13.5.6. *Produce Working Copies*

Working Copies can be in many forms. The files can be copied onto any suitable medium or distributed electronically (if a secure system is in place) for circulation to the investigating officers and SHIRE OF PINGELLY. Issues of quality control, security and resource management need to be considered.

7.14. NETWORK CONFIGURATION AND DATA TRANSMISSION

Refer to the CCTV System's Operation and Technical Manual for detailed Network Configuration Requirements and Data Transmission requirements with reference to the WA CCTV Guidelines and Technical Advice for appropriate set up and commissioning.

Enter Technical Design information in the CCTV Management Spreadsheet - System Overview.

7.15. MONITORS AND CONTROLS

Refer to the CCTV System's Operation and Technical Manual for detailed Network Configuration Requirements and Data Transmission requirements with reference to the WA CCTV Guidelines and Technical Advice for appropriate set up and commissioning.

Enter Technical Design information in the CCTV Management Spreadsheet - System Overview.

7.16. RECORDING AND STORAGE

Refer to the CCTV System's Operation and Technical Manual for detailed Network Configuration Requirements and Data Transmission requirements with reference to the WA CCTV Guidelines and Technical Advice for appropriate set up and commissioning.

Enter Technical Design information in the CCTV Management Spreadsheet - System Overview.

7.16.1. RECORDING OF IMAGES

CCTV images may only be recorded by the SHIRE OF PINGELLY

All information recorded, collected and collated by means of CCTV Operations shall remain the sole property of the SHIRE OF PINGELLY

Any incident recorded and selected for review shall be noted in the daily register including date, time and category of incident.

The date, time and category of incident shall be noted on the recorded medium (CD Rom, DVD, USB, HDD) and electronic file name.

All recorded material shall be kept in secured storage, including electronically, under the control of the SHIRE OF PINGELLY

All original residual recordings shall be erased after **31** days after the date of the recording unless the footage has been reviewed or a request is made in writing for it to be held.

All written requests for access to original video recordings shall be filed with the CCTV Management and Operations Manual.

Authorised Personnel may view any footage on a random basis in accordance with the Code of Conduct and Code of Practice.

The Duty Surveillance Officer shall view the daily register and reports will be submitted on a monthly basis, or as otherwise directed.

7.17. SOFTWARE SYSTEM OVERVIEW AND MANUALS

All CCTV System's Operation and Technical Manuals will form part of the CCTV Management and Operations Manual.

Electronic Copies will be provided and stored for ease of access.

7.18. SYSTEM WARRANTIES AND MAINTENANCE

A record of system warranties and maintenance requirements will be formulated and integrated with maintenance and cleaning schedules.

7.19. WORKSTATION DESIGN AND CAPACITY

The design and capacity of monitoring workstations will be monitored for efficacy and comparison to alternative designs will be made to other CCTV Operations of a similar size.

7.20. GAPS ANALYSIS AND ERROR REPORTING

CCTV Operational gaps and errors must be acknowledged and treated wherever possible. Consideration to the business case of rectifying identified gaps and error reporting is the responsibility of the CHIEF EXECUTIVE OFFICER.

7.21. OPERATION REDUNDANCY AND DISASTER RECOVERY

Refer to the CCTV System's Operation and Technical Manual for detailed Redundancy Configuration Requirements and recovery of data following power outages, system faults and other impediments to operations.

CCTV Operations should be integrated into the SHIRE OF PINGELLY's Business Continuity Planning and Local Area Emergency Management Plans.

8. MEMORANDUM OF UNDERSTANDING (SAMPLE)

This MEMORANDUM OF UNDERSTANDING is made on DATE
BETWEEN:

SHIRE OF PINGELLY: CEO

And

WESTERN AUSTRALIA POLICE: Regional Inspector

PURPOSE

The CCTV Operation was established by the SHIRE OF PINGELLY to contribute to the safety and security of persons and property within the confines of the SHIRE OF PINGELLY.

West Australia Police are concerned with enhancing the quality of life and well-being of the community by contributing safety and security.

The purpose of this agreement is to facilitate a collaborative cooperative approach to enhancing the safety and security of persons and property within the SHIRE OF PINGELLY.

SHIRE OF PINGELLY CONTRIBUTION

The SHIRE OF PINGELLY is responsible for the operation of the CCTV System on a 7 day, 24 hour basis.

The CCTV Operation will be operated in accordance with the SHIRE OF PINGELLY policies and procedures developed in conjunction with Ministry of Justice guidelines.

The SHIRE OF PINGELLY will maintain an effective record of daily occurrences, incidents and visitors to the CCTV Operations Room.

The SHIRE OF PINGELLY will maintain appropriate systems and processes to ensure the secure retention and disposal of recorded material.

The SHIRE OF PINGELLY will provide operational and evidentiary assistance to Western Australia Police to facilitate policing operations and the successful investigation and prosecution of offences.

WESTERN AUSTRALIA POLICE CONTRIBUTION

Subject to operational requirements, Western Australia Police is responsible for providing:

Western Australia Police will provide appropriate support and response to identified incidents and issues.

Western Australia Police will maintain an effective record of daily occurrences, incidents and activities for the CCTV Operations target areas.

Western Australia police will seek approval from the SHIRE OF PINGELLY prior to conducting operations which utilise CCTV Operations.

CONFLICT RESOLUTION

Conflicts which cannot be resolved by operations personnel will be directed to the Duty Surveillance Officer, SHIRE OF PINGELLY and the Officer in Charge, NAME Police Station for resolution.

If unable to be resolved at that level, issues will be referred to the CHIEF EXECUTIVE OFFICER, SHIRE OF PINGELLY and the LOCAL DISTRICT OFFICER.

TERM

The term of this memorandum of understanding is 2 years (or as otherwise agreed) from the date this undertaking is signed.

REVIEW AND TERMINATION

During the term and prior to each anniversary of the commencement of this agreement, the parties agree that the Memorandum of Understanding will be reviewed in order to determine whether both the SHIRE OF PINGELLY and Western Australia Police agree to continue.

Following such a review, either party may terminate its obligations under this Memorandum of Understanding by sending notice of such termination to the other party in writing.

AGREEMENT

The parties understand and agree that this Memorandum of Understanding is a clear statement of their intentions as to the matters stated and that the agreement will not be legally binding.

SIGNED for and behalf of

the **SHIRE OF PINGELLY** by: Signature

NAME

TITLE

OFFICE

SIGNED for and behalf of

WESTERN AUSTRALIA POLICE

by: Signature

NAME

RANK

STATION

9. RELEASE FORM FOR RECORDED MATERIAL

REQUEST FOR RECORDED IMAGES FROM CCTV SURVEILLANCE RECORDS

To: Chief Executive Officer, SHIRE OF PINGELLY

It is requested that Copy Marked _____ or Photograph showing an Incident on (date/s) _____ between time(s) _____ and _____ be released to me for the purpose of Evidence / Investigations which are subject to Police / Ranger / Security/ Civil Litigation inquires or proceedings.

We / I accept full responsibility for this Copy / Photograph whilst it is in our/my possession and understand that We / I am **NOT** at liberty to make or release copies of the footage or permit other persons to make copies or lend it to persons other than for the purpose for which the copy was made.

The Copy/Photograph will **NOT** be released to the Media under any circumstances unless authorised by the Chief Executive Officer of the SHIRE OF PINGELLY.

We / I accept responsibility for advising the SHIRE OF PINGELLY as to the estimated date of return or destruction of this property and that it be returned in the same serviceable condition as obtained.

INCIDENT TYPE

- Offence against the Person (Type _____)
- Offence against Property (Type _____)
- Police Operation or Investigation (Type _____)
- Security or Ranger Services (Type _____)
- Civil Litigation or Subpoena Served (Type _____)

COPY HANDED TO

SIGNED: _____
NAME: _____
RANK & NO: _____
DATE: _____
STATION/SECTION: _____
DATE: _____

SHIRE OF PINGELLY

SIGNED: _____
Duty Surveillance Officer

COPY/PHOTOGRAPH RETURNED: Date: _____ Signed _____

COPY/PHOTOGRAPH DESTROYED: Date: _____ Signed _____

10. CCTV Incident Report

(Note: This document is provided as an example only and Councils are encouraged to develop their own document)

Location: _____ **Report No:**.....

Incident	Other Emergency	Local Authority	Other
Assault – minor	Fire	Repair/maintenance	List...
Assault – serious	Water	Environment	
Malicious Damage	Medical	Traffic	
Traffic	Power	Waste	
Trespass		Health	
Stealing		Ordinance/breach	
Robbery		Safety	
Intoxicated Person			
Information only	Community	CCTV Maintenance	
Security	Cash escort	Cameras	
Street offence	Demonstrations	Recording equip.	
Other...	Special Events	Monitoring equip.	
	Parade	Optic fibre	
	Security	House keeping	

Organisations Responding	Police / Fire / Ambulance / SHIRE OF PINGELLY
	Ref No. TIME NOTIFIED TIME RESPONDED

NARRATIVE

FOOTAGE TIME(s)

Incident Recording Details	Officer Name	DATE
	Camera No(s)	
	Other References	

11. CAMERA / LOCATION RISK ANALYSIS - QUALITATIVE

AS/NZS 4360:2004: Risk Management describes how the objectives of analysis are to separate acceptable risks from major risks. Risk analysis involves the consideration of the sources of risk, their consequences and the likelihood that those consequences may occur.

Consequence

AS/NZS 31000:2009 Risk Management describes that it is important to recognise that the consequences of any particular risk event may impact in different ways at different levels. Financial costs, personal harm (physical and psychological), legal consequences and damage to reputation may all result from a single incident.

Table 1 shows the AS/NZS 31000:2009 Risk Management descriptors for consequence:

Table 1: Qualitative measures of consequence or impact

Level	Descriptor	Description
1	Minimal	< \$2000 (< \$1000): Isolated brief coverage, single media outlet: Stakeholders experience minimal disadvantage (days): Process breakdown or inefficiencies that have a limited impact on the achievement of an objective: Minor injury requiring first aid only
2	Minor	\$2,000 – \$50,000 (< \$10,000): Minor negative coverage, limited circulation for one day: Minority of stakeholders experience disadvantage (days - weeks): Process breakdown that impedes the achievement of one or more objectives or some inefficiencies in key processes: Minor injuries requiring medical attention
3	Moderate	\$50,000 - \$5,000,000 (< \$50,000): Negative coverage lasting for several days, and/or frequent reoccurrence for several weeks: Multiple stakeholders experience significant disadvantage (weeks): Process breakdown that impedes the achievement of an important objective or causes extensive inefficiencies in key processes: Multiple casualties requiring hospital attention
4	Major	\$5,000,000 - \$100,000,000 (< \$5,000,000): Negative significant coverage, appearing consistently over weeks: Multiple stakeholders severely disadvantaged (weeks - months): Serious process breakdown that substantially impedes the achievement of a core objective: Multiple severe injuries, or a single fatality
5	Catastrophic	> \$100,000,000 (> \$5,000,000): Extreme negative coverage causing public outcry appearing consistently over weeks: Majority of stakeholders severely disadvantaged (months): Serious process breakdown that prevents the achievement of mission critical objectives: Multiple severe injuries, including fatalities

Likelihood

Table 2 shows the AS/NZS 31000:2009 Risk Management descriptors for likelihood:

Table 2: Qualitative measures of likelihood

Level	Descriptor	Description
A (=5)	Almost Certain	Over 99% probability or 'happens often', or could occur within 'days to weeks'
B (=4)	Likely	>50% probability or 'could easily happen', or could occur within 'weeks to months'
C (=3)	Possible	>10% probability or 'could happen, has occurred before', or could occur within 'a year or so'
D (=2)	Unlikely	>1% probability or 'has not happened yet, but could', or could occur 'after several years'
E (=1)	Rare	<1% probability or 'conceivable but only in extreme circumstances': exceptionally unlikely, even in the long term future or a '100 year event' or greater

Qualifying the risk

Table 3 shows the AS/NZS 31000:2009 Risk Management qualitative risk analysis matrix for level of risk.

Table 3: Qualitative risk analysis matrix

Likelihood	Consequences				
	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
A - Almost Certain	High	High	High	Extreme	Extreme
B - Likely	Moderate	High	High	Extreme	Extreme
C - Possible	Low	Moderate	High	High	Extreme
D - Unlikely	Low	Low	Moderate	High	Extreme
E - Rare	Low	Low	Low	Moderate	High

Legend

Extreme risk: immediate action required
 Moderate risk: management responsibility must be specified

High risk: senior management attention needed
 Low risk: managed by routine procedures.

11.1. **CAMERA RISK ASSESSMENT - Camera Number(s) / Location(s)**

This preliminary camera risk evaluation, as shown in Table 4 is formulated as a guide only. The identified risks should be ranked based on available information and opinion by the SHIRE OF PINGELLY. A crime and CCTV risk workshop is recommended annually to accurately evaluate and rank risks in line with current crime prevention strategy and objectives. Crime risks should be rated in accordance with the Community Safety and Crime Prevention Plan priorities.

Table 4: Camera (Number) Risk Assessment

<i>Key security risks</i>	<i>Comment on the risk or give an example to clarify the risk</i>	<i>Existing controls presently in place to mitigate against the risk</i>	<i>Adequacy of existing controls, use excellent =1 generally adequate =3 inadequate =5, none=7</i>	<i>Likelihood use 5 = Almost Certain 4= Likely 3 = Possible 2 = Unlikely 1 = Rare</i>	<i>Consequence use 5 = Catastrophic 4 = Major 3 = Moderate 2 = Minor 1 = Minimal</i>	<i>Likelihood x Consequence</i>	<i>Risk rating</i>	<i>Treatments proposed, indicate treatment, person responsible, due date, review process</i>
Burglary								
Violence / Assaults								
Stealing Offences								

CAMERA RISK ASSESSMENT - Camera Number(s) / Location(s) (CONTINUED)

<i>Key security risks</i>	<i>Comment on the risk or give an example to clarify the risk</i>	<i>Existing controls presently in place to mitigate against the risk</i>	<i>Adequacy of existing controls, use excellent =1 generally adequate =3 inadequate =5, none=7</i>	<i>Likelihood use 5 = Almost Certain 4 = Likely 3 = Possible 2 = Unlikely 1 = Rare</i>	<i>Consequence use 5 = Catastrophic 4 = Major 3 = Moderate 2 = Minor 1 = Minimal</i>	<i>Likelihood x Consequence</i>	<i>Risk rating</i>	<i>Treatments proposed, indicate treatment, person responsible, due date, review process</i>
Robbery (Stealing with Violence)								
Anti-Social Behaviour								
Vandalism/ Criminal Damage								
Sexual Offences								

CRIME RISK ASSESSMENT - Camera Number(s) / Location(s) (CONTINUED)

<i>Key security risks</i>	<i>Comment on the risk or give an example to clarify the risk</i>	<i>Existing controls presently in place to mitigate against the risk</i>	<i>Adequacy of existing controls, use excellent =1 generally adequate =3 inadequate =5, none=7</i>	<i>Likelihood use 5 = Almost Certain 4= Likely 3 = Possible 2 = Unlikely 1 = Rare</i>	<i>Consequence use 5 = Catastrophic 4 = Major 3 = Moderate 2 = Minor 1 = Minimal</i>	<i>Likelihood x Consequence</i>	<i>Risk rating</i>	<i>Treatments proposed, indicate treatment, person responsible, due date, review process</i>
Motor vehicle theft/break in/damage								
Vehicle Driving Offences								
Drug related offences								

12. Australian & International Research Publications

1. *Addressing the CCTV Skills Shortage*, Security Insider Oct/Nov 2008. Available at <http://www.cctvcertification.com.au/forum.html>
2. *Assessing the impact of CCTV: The South City Case Study*, 2005, Home Office Online Report 11/05. Available at <http://rds.homeoffice.gov.uk/rds/pdfs05/rdsolr1105.pdf>
3. Cohen, N., Gattuso, J., and MacLennan-Brown, K. (2009). *CCTV Operational Requirements Manual*. Publication No. 28/09. Home Office Scientific Development Branch: Sandridge UK. Available at http://scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/28_09_CCTV_OR_Manual.pdf?view=Binary
4. Cohen, N., Gattuso, J., MacLennan-Brown, K. *CCTV Operational Requirements Manual Is your CCTV system fit for purpose?* Publication No. 55/06 Home Office Scientific Development Branch, Video Evidence Analysis Programme. Available at <http://scienceandresearch.homeoffice.gov.uk/hosdb>
5. Cohen, N, MacLennan-Brown, K. *Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems v2.0* Publication No. 66/08 2.0 Home Office Scientific Development Branch, Video Evidence Analysis Programme. Available at <http://scienceandresearch.homeoffice.gov.uk/hosdb>
6. Diffley, C and Wallace, E (1998). *CCTV: Making It Work, Training Practices For CCTV Operators*, Police Scientific Development Branch, Home Office Police Policy Directorate Publication 9/98.
7. Draft framework for the intended Australian CCTV Standard 4806.5 referring to Digital and Networking in CCTV (*Draft2, prepared by Vlado Damjanovski, August 2008*). Available at <http://www.asial.com.au/Assets/278/1/Australian48065draft02.pdf>
8. *i-LIDS User Guide Imagery Library for Intelligent Detection Systems* Publication No. 29/09 v2.1 Home Office Scientific Development Branch, Video Evidence Analysis Programme Available at <http://scienceandresearch.homeoffice.gov.uk/hosdb>
9. *Implementing a strategy for the identification, retrieval and evaluation of CCTV evidence in major investigations* Home Office Scientific Development Branch, Video Evidence Analysis Programme. Available at <http://scienceandresearch.homeoffice.gov.uk/hosdb>
10. NSW Government Policy Statement and Guidelines for the Establishment and Implementation of CCTV in Public Places. Available at [http://www.lawlink.nsw.gov.au/lawlink/cpd/ll_cpd.nsf/vwfiles/cctv.pdf/\\$file/cctv.pdf](http://www.lawlink.nsw.gov.au/lawlink/cpd/ll_cpd.nsf/vwfiles/cctv.pdf/$file/cctv.pdf)
11. *Video Evidence Analysis Programme Update* February 2008, Publication No. 07/08 Home Office Scientific Development Branch, Video Evidence Analysis Programme. Available at <http://scienceandresearch.homeoffice.gov.uk/hosdb>
12. Wilson, D. and Sutton, A. (2003). *Open-Street CCTV in Australia: A comparative study of establishment and operation*. Available at <http://www.criminologyresearchcouncil.gov.au/reports/200102-26.pdf>

For more Australian Institute of Criminology CCTV publications, visit

<http://search.aic.gov.au/search/search.cgi?query=CCTV&collection=aic-all&live=aic&form=simple>

For more Home Office CCTV publications visit

<http://scienceandresearch.homeoffice.gov.uk/hosdb/cctv-imaging-technology/CCTV-and-imaging-publications>