

# **CCTV Management and Operations Manual**



# Contents

<b>Amendments.....</b>	<b>3</b>
FOREWORD .....	4
1.0 STRATEGIC AND CORPORATE PLAN ALIGNMENT .....	4
2.0 TERMS AND DEFINITIONS.....	5
3.0 CCTV POLICY STATEMENTS .....	6
3.1 Ownership and Control of CCTV .....	6
3.2 Role and Purpose of CCTV .....	6
3.3 Organisation Policy for CCTV.....	6
3.4 CCTV Operating Practices .....	6
3.5 Code of Conduct .....	7
3.6 Confidentiality .....	7
3.7 Operating Conditions .....	8
3.8 Reporting a Breach of the Code of Conduct.....	8
4.0 CCTV MANAGEMENT PRACTICES.....	9
4.1 Introduction .....	9
4.2 Key Performance Indicators.....	9
4.3 Operational Objectives.....	9
4.4 Western Australian Guidelines.....	9
4.5 Australian Standards .....	9
4.6 Relevant Legislation.....	10
4.7 Accountability .....	11
4.8 Breaches of the Code of Conduct.....	11
4.9 Management Framework .....	11
4.10 Community Safety and Crime Prevention Planning and CCTV Operations .....	12
4.11 Key Roles and Responsibilities .....	12
4.12 CSCP Officers in Relation to CCTV Management and Operation.....	13
4.13 Monitoring, Review and Audit Reports and Protocols.....	13
4.14 Public Awareness and Media Management.....	14
4.15 CCTV Operation access controls.....	14
4.16 Camera Management .....	14
5.0 CCTV STANDARD OPERATING PROCEDURES .....	17
5.1 Introduction .....	17
5.2 CCTV Management Spreadsheet.....	17
5.3 Maintaining Compliance and Local Government Best Practice.....	17
5.4 Authorised Personnel – Selection and Recruitment.....	18
5.5 Selection of Contractors and Consultants.....	19
5.6 Surveillance Duties and Tasking .....	19
5.7 Camera Operation .....	22
5.8 CCTV System Expansion and Upgrades .....	23

5.9 Troubleshooting, Faults and Maintenance.....	23
5.10 Data Storage .....	23
5.11 Data Access .....	23
5.12 Continuity of Evidence.....	24
5.13 Viewing of Recorded Material .....	25
5.14 Operation Redundancy and Disaster Recovery .....	27

# Amendments

Proposal for amendments to this plan should be forwarded to Manager of Safer Communities

[illegible]

# FOREWORD

The public perception of CCTV systems in Australia has matured with the widespread installation of residential and commercial systems. Privacy concerns have lessened with the recognised safety advantages afforded by public space CCTV. The responsible and appropriate management of our CCTV system and recorded footage could however still be a focus of public attention and scrutiny.

The CCTV Operation should be recognised as a significant and contributing asset to the City of Belmont (The City). 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 actual monetary terms, however the City of Belmont will continue to seek out measurable returns on investment as CCTV Operations develop.

The CCTV Management and Operations Manual (MOM) provides a functional means of managing the City's CCTV and Analytics systems, it ensures compliance with current legislation, Guidelines, Standards and relevant publications. The MOM aligns with strategic and operational functions. In addition, the MOM provides a practical guide for any issue pertaining to the City's CCTV system management, operation, technical specification, and functionality.

## 1.0 STRATEGIC AND CORPORATE PLAN ALIGNMENT

The Strategic Community Plan 2024-2034 outlines our community's shared vision and aspirations.

It details the City's future, with five key performance areas of People, Place, Planet, Prosperity, and Performance.

The primary area of alignment for community safety under the Strategic Community Plan is People with supporting alignment under Place, Prosperity and Performance.

### • Strategic Community Plan 2024 – 2034

#### PEOPLE

Desired Outcomes	Objectives	Supporting Strategies and Plans
1 A safe, healthy community.	1.1 Facilitate improved community safety. 1.2 Facilitate community health and wellbeing. 1.3 Grow participation in sport and recreation activities.	<ul style="list-style-type: none"><li>Community Safety Strategy 2018-2021</li><li>Safer Communities Plan 2020-2023</li><li>Recreation Strategy 2022-2025</li></ul>

### • Corporate Business Plan 2025 – 2029

The City's Corporate Business Plan is designed to help steer the outlined outcomes of which CCTV forms part of this.

#### Our plan for the future

##### Outcome 1. A safe, healthy community.

Objectives	Actions		Informing Strategies	Lead	25-26	26-27	27-28	28-29
 1.1 Facilitate improved community safety.	1.1.1	Adopt and implement the Community Safety Strategy 2025-2028.	Community Safety Strategy	Manager Safer Communities	•	•	•	•
	1.1.2	Implement the requirements of the Safer Communities Operational Plan 2025 -2028.	Safer Communities Operational Plan	Manager Safer Communities	•	•	•	•
	1.1.3	Continue to improve and enhance the City's CCTV network and coverage by updating older systems with a focus on high activity areas.	Community Safety Strategy	Manager Safer Communities	•	•	•	•
	1.1.4	Advocate for Western Power to roll out underground power and SMART streetlighting across the City of Belmont.		Director Infrastructure Services	•	•	•	•
	1.1.5	Roll out LED lighting upgrades in parks and suburbs where the City owns streetlight infrastructure.	Environment and Sustainability Strategy	Director Infrastructure Services	•	•	•	•
	1.1.6	Promote community safety initiatives that empower the community.	Community Safety Strategy	Manager Safer Communities	•	•	•	•
	1.1.7	Engage and work closely with community partners, including the Community Safety Alliance, to improve and promote safety and address perception of crime.	Community Safety Strategy	Manager Safer Communities	•	•	•	•

## 2.0 TERMS AND DEFINITIONS

**“Authorised Personnel”** means any officer of the City of Belmont authorised by the Chief Executive Officer (CEO) or the WA Police Commissioner as listed in the CCTV Management Spreadsheet., including the City approved CCTV contractor

**“Community Safety and Crime Prevention Officers (CSCP)”** are Authorised Personnel in charge of daily CCTV Operations

**“CCS - Coordinator Community Safety”** oversees the CSCP Officers and monitors the activities of Authorised Personnel

**“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 City of Belmont's CCTV transmission system or operated as a covert camera.

**“CCTV (Video) Analytics”** refers to the process of using advanced technology, such as artificial intelligence and machine learning, to analyse the data generated by surveillance cameras.

**“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 used either to record activities covertly or for short periods of time. Covert or mobile cameras operated by the City of Belmont maybe used for the purposes of detecting illegal activities or behaviours, and form part of CCTV Operations and would be managed and operated in accordance with this Manual.

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

**“MSC - Manager Safer Communities”**, oversees Community Safety Section including the City’s CCTV management requirements,

**“Public place”** is generally an indoor or outdoor area, whether privately or publicly owned, to which the public have access by right or by invitation, expressed or implied, whether by payment of money or not,

**“Private premises”** refers to any area not openly accessible to the 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 legislation, where it appears that a person(s) may be in physical distress, or a situation likely to cause a public disturbance.

**“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.

**“Vehicle CCTV”** means outward facing fixed cameras on a City authorised vehicle (BCW and Rangers), designed to capture activities within the public realm during normal duties.

## 3.0 CCTV POLICY STATEMENTS

### 3.1 Ownership and Control of CCTV

The CCTV network is solely owned and operated by the City of Belmont.

The City operates its CCTV in accordance with this approved CCTV Management Practices, and all Authorised Personnel must abide by the Code of Conduct, within the Manual. (Annexure 1).

The City's Manager Safer Communities (MSC) Coordinator Community Safety (CCS) and Community Safety and Crime Prevention (CSCP) Officers and Community Safety and Emergency Management Officer have authorised control over the CCTV Operations.

This Manual and the City CCTV and Video Analytics Policy (the Policy) establish the purpose, key functions, and control parameters set by the City, to achieve the following:

1. Maintain best practice and standards with reference to the WA Police State CCTV Strategy
2. Manage CCTV Operations in compliance with Australian Standards, 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 fields 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 CCTV Code of Conduct.
5. Maintain effective oversight in the Monitoring, Reviewing, Auditing and Reporting of the CCTV operations.

### 3.2 Role and Purpose of CCTV

The City operates its CCTV to:

1. Deter, detect, investigate and respond to potential breaches of local, and State law against a person(s), and or property.
2. Facilitate and support an effective response by City's Authorised Personnel, WA Police or other emergency services personnel to situations of community concern or public interest.
3. Manage and maintain community safety for residents, traders, retailers, workers, visitors, and City staff.
4. Monitor and protect City assets.

### 3.3 Organisation Policy for CCTV

The Policy (Policy59) details how the CCTV will be operated and managed and references the reporting protocols for both internal and external stakeholders.

### 3.4 CCTV Operating Practices

The City will ensure CCTV is conducted in accordance with the following operating practices:

1. The CCTV and Analytics System (CCTVAS) 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 approved policies.
2. The CCTVAS 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 City's CCTV Code of Conduct.
5. Access to Designated Surveillance Areas will be restricted to Authorised Personnel only or with written authorisation from the MSC, CCS and CSCP Officers.

6. The City will be accountable to its Stakeholders for the effective management and control of CCTV and Analytics Operations.
8. Recorded material released to Stakeholders must only contain the evidence requested and not exceed the intended purposes of the written request.
9. The retention, and access to any recorded material will be predominantly for assisting WA Police and other formally approved agencies or internal departments in detecting and responding to reported offences and to facilitate an effective response to situations of concern or interest to the Belmont Community.
10. CCTV footage will be retained for thirty-one (31) days unless otherwise specified. While most CCTV footage will be automatically deleted over time some downloaded, hard copy or electronic material will be retained as City records of specific events.
11. All internal requests for CCTV footage, or viewing, must be made, and recorded using the City's approved report operating systems (Pathway).
12. Contact and exchange of information between the City of Belmont and WA Police will be conducted in accordance with the current Memorandum of Understanding (MOU).
12. Requests to access or to view live CCTV or captured images can only be undertaken under the supervision of City's Authorised Personnel (Examples of this would be to, review, monitor or verify City of Belmont maintenance services and public works).
13. Access to CCTV will remain with the City's Authorised Personnel only.
14. The City 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 solely to the interests of the City of Belmont or operational needs of the WA Police.
15. The City's CCTV system and analytics software will only be accessed by Authorised Personnel. Original recordings or data will not be released unless requested under a search warrant, court summons, by a recognised State or Federal law enforcement agency, Freedom of Information release or upon approval for release by the City's Chief Executive Officer.
16. The City may use footage in the investigation of breaches of its Local Laws or other relevant legislation.
17. Metadata from analytics software can be used to provide demographic information to assist in the efficient use and management of the City's facilities.
18. The facial recognition capability of analytics software will not be activated or used by the City.

Refer to CP59 - Closed Circuit Television (CCTV) Video Analytics Policy in the City's Policy Manual.

### **3.5 Code of Conduct**

Any staff member or contractor, including authorised personnel as defined within this manual who have access to view live or playback CCTV footage, or access to the City's back-end CCTV systems, are required review and then sign the City's CCTV Code of Conduct (Annexure 1)

These processes have been adopted to ensure the highest of integrity, standard and honesty are undertaken when accessing the City's CCTV systems

Any staff member or contractor, including authorised personnel as defined within this manual who breach the requirements of the Code of Conduct, may be subject to disciplinary action, up to and including dismissal as employee or contractor of the City and or criminal proceedings.

### **3.6 Confidentiality**

Any staff member or contractor, including authorised personnel as defined within this manual are to ensure information viewed, gathered by or from the City's CCTV operating systems are not viewed, disclosed, or discussed with unauthorised Personnel or associates who have no direct responsibility to the CCTV Operations.

Unless the City's CCTV Code of Conduct has been signed, and access approved, then access to and the City's CCTV system unaccompanied would not be permitted



### 3.7 Operating Conditions

Locations where CCTV may be viewed live or in the playback options, are to be in areas which are secured and isolated from public view and non-authorised personnel.

Any CCTV which is viewed live, or playback mode must be logged and any viewing or CCTV which is viewed in playback mode must not exceed the intended purposes.

Please note any City CCTV footage viewed live or in playback mode, can only be undertaken in the presence of authorised personnel, as defined in this manual

CCTV footage viewed by any non - Authorised Personnel, and whilst in the presence of an Authorised Personnel must be recorded in the City's CCTV Activity Register and signed.

CCTV Operational records (hard copy or electronic) can only be destroyed with written authorisation by the MSC, CCS or the CSCP Officers, in accordance with approved CCTV Operating Procedures and the State Records General Disposal Authorisation Policy.

The use of the CCTV **must not** be for personal benefit or gain or invade any individual or groups privacy. Cameras should only be used in accordance with Statement 3.2.

Live viewed or played back mode CCTV **must not** be recorded and **shall not** be copied by any 2<sup>nd</sup> or 3<sup>rd</sup> party or taken from Designated Surveillance Areas.

Download and use of capture CCTV footage can only be released via the approved and established CCTV request processes.

### 3.8 Reporting a Breach of the Code of Conduct

Should any reports of concern be received regarding the handling or managing of matters related to CCTV, and the incident, then that person is obliged to report the incident to MSC.

The MSC in return will refer the matter to the City's Manager People & Culture, for further investigation.

The CCTV Code of Conduct form must be signed by all authorised personnel and can be found on the City Belnet.

[CCTV Code of Conduct Form](#)

## 4.0 CCTV MANAGEMENT PRACTICES

### 4.1 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.

CCTV Management requires continued commitment for monitoring, reviewing, and auditing processes, in addition to planning and finance procedures, relating to the CCTV Operations. The City should continue to seek out areas for improvement ensuring system efficiency.

### 4.2 Key Performance Indicators

Establishing clear and concise Key Performance Indicators (KPIs) for CCTV Operations allows for the effective reporting and monitoring of system effectiveness and quickly highlights trends concerning fundamental operations, which may require early intervention or closer monitoring by Authorised Personnel.

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

1. Number of improvements and enhance the City's CCTV network.
2. Number of CCTV request from WA Police.
3. Number of CCTV requests from internal and external parties

### 4.3 Operational Objectives

Operational objectives should be based on measurable criteria, including:

- Improving community's perceptions of safety
- Expand CCTV surveillance within public open spaces, or high volume or activity areas (excluding residential areas).
- Improve community resilience towards crime and community safety
- Ongoing collaboration with key agencies and community on the contributors to crime and community safety

Assessment of the above criteria is undertaken in part through the annual Community and Business surveys.

### 4.4 Western Australian Guidelines

Western Australian guidelines (available on-line) relating to CCTV Operations should be read in association with the CCTV Management and Operations Manual and include:

- WA Police State CCTV and ANZPAA guidelines.
- WA Planning Commission Designing Out Crime Guidelines.

### 4.5 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 ([www.standards.org.au](http://www.standards.org.au)). In Australia, best practice CCTV Operation guidelines may refer to the following:

- **AS/NZS 62676.1.1:2020 Video surveillance systems for use in security applications,**  
Part 1.1: System requirements — General (IEC 62676-1-1:2013, MOD)
- **AS/NZS 62676.1.2:2020 Video surveillance systems for use in security applications,**  
Part 1.2: System requirements — Performance requirements for video transmission (IEC 62676-1-2:2013, MOD).

- **AS/NZS 62676.2.1:2020[Current] Video surveillance systems for use in security applications,**  
Part 2.1: Video transmission protocols — General requirements (IEC 62676-2- 1:2013, MOD)
- **AS/NZS IEC 62676.2.2:2020[Current] Video surveillance systems for use in security applications,**  
Part 2.2: Video transmission protocols — IP interoperability implementation based on HTTP and REST services
- **AS/NZS IEC 60839.11.2:2019 [Current] Alarm and electronic security systems,**  
Part 11.2: Electronic access control systems — Application guidelines
- **AS/NZS 62676.4:2020 [Current] Video surveillance systems for use in security applications,**  
Part 4: Application guidelines (IEC 62676-4:2014, MOD)
- **AS/NZS IEC 62676.2.31:2020 [Current] Video surveillance systems for use in security applications,**  
Part 2.31: Live streaming and control based on web services
- **AS/NZS IEC 62676.2.32:2020 [Current] Video surveillance systems for use in security applications,**  
Part 2.32: Recording control and replay based on web services
- **'AS/NZS 1158.3.1:2020 - 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.
- **AS 2201.1:2007 - Security Installations.**
- **AS/ACIF S009:2013 - Cabling Provider Rules.**
- **AS/NZS 1768:2007 - Lightning protection.**
- **ISO 31000:2019 - Risk Management (Supersedes ISO 31000:2018).**
- **HB 167: 2006 - Security Risk Management Handbook.**
- **AS 1743:2018 - Development, testing, implementation of information and safety symbols and symbolic signs.**
- **AS2416:2010 - Provides examples and the display of multiple hazard signage.**

## 4.6 Relevant Legislation

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

<b>Commonwealth</b>	
<i>Surveillance Devices Act 2004</i>	Regulates use of optical surveillance devices without warrant
<i>Privacy Act 1988</i>	Establishes and regulates privacy principles for individuals, corporate entities and personal information
<b>Western Australia</b>	
<i>Criminal Investigation Act 2006</i>	Provides powers for the investigation and prevention of offences and for related matters.

<i>Work Health and Safety Act 2020</i>	Regulates the protection of persons at or near workplaces from risks to health and safety
<i>Surveillance Devices Act 1998</i>	Regulates use, installation, and maintenance of optical surveillance devices
<i>Security and Related Activities (Control) Act 1996</i>	Regulates WA Security Providers
<i>Security and Related Activities (Control) Regulations 1997</i>	Regulates WA Security Providers

## 4.7 Accountability

The City is responsible for ensuring that CCTV Operations will be assessed and reviewed regularly 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 such as the redacting of footage provided under Freedom of Information.

Evaluation of CCTV Operations will include, as a minimum:

- a) Assessment of its impact on improving perceptions of safety and reducing 'Fear of Crime' by members of the public in the areas that have the City's CCTV in operation
- b) Compliance with the Code of Conduct, protocols, and standard operating procedures.
- c) The number of CCTV requests lodged.

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

## 4.8 Breaches of the Code of Conduct

The 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 City of Belmont or the needs of the current Community Safety Strategy 2025-2030.

Primary responsibility for ensuring the Code of Conduct is adhered to, rests with the City. This includes ensuring that breaches of the Code are investigated and remedied to the extent that breaches of the Code are within the ambit of the City of Belmont's power to remedy.

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

*Chief Executive Officer, City of Belmont, 215 Wright Street, Cloverdale WA 6105*

The City of Belmont will cooperate with the investigation of any complaint about the City of Belmont CCTV Operations conducted by WA Police, Crime and Corruption Commission or other appropriately authorised external organisation.

## 4.9 Management Framework

The City has implemented a management framework, contained within this document, that the MSC has oversight responsibilities for CCTV Operations. The MSC will maintain a management overview of CCTV Operations with reference to CCTV Policy and Procedures, comprising of:

- a) Policy Statements. 3.2
- b) Code of Conduct. - Annexure 1
- c) CCTV Management Practice - Part 4.0, This document
- d) Standard Operating Procedures- Part 5.0, This document
- a) Camera Management 4.17.1; and
- b) Crime Risk Assessments 4.17.2.

## 4.10 Community Safety and Crime Prevention Planning and CCTV Operations

The CCTV Operation is acknowledged in the City's Community Safety Strategy focusing on providing outcomes related to crimes, and other type offences committed where CCTV is located. Future deployment of the CCTV is also be determined in part based on data obtained from key agencies when considering future system designs.

The City of Belmont's Community Safety Strategy 2025-2030.

**Deliver - 1.2-** Continue to improve and enhance the City's CCTV network and coverage within the public realm based on identified need.

**Empower - 2.1** Provide crime prevention support and advice to increase home and business security

**Partner- 3.1 -** Continue working with WA Police Force to foster two-way sharing of information relating to crime and safety in the area.

## 4.11 Key Roles and Responsibilities

The responsibilities of the City's, CSCP Officers, Authorised Personnel and the WA Police are:

### 4.11.1 City of Belmont Responsibilities

The City is responsible for the following key functions:

- a) Developing a Community Safety Strategy 2025-2030 that incorporates CCTV strategies (Deliver 1.2).
- b) The Coordinator Community Safety oversees the day-to-day implementation and operations of its CCTV.
- c) Providing regular updates on the City's use of CCTV within the community and ensuring notification of CCTV systems in operation is clearly identified via signage.
- d) Financing the implementation, maintenance, and ongoing licensing needs of the CCTV systems.
- e) Ensure all CSCP officers have the skills to assist the City in the design of an appropriate CCTV monitoring system.
- f) Calling for tenders for the provision of CCTV services when required.
- g) Have an effective complaint or request handling mechanism through the City's existing processing system (Pathway).
- h) Monitoring the effectiveness of CCTV using statistical data and reported requests.
- i) Ensuring inductions are provided to new Authorised Personnel and ongoing upskilling is provided to staff involved in operating and working with the CCTV systems.
- j) Ensuring compliance with the CCTV Code of Conduct, CCTV Management Practice - Part 4.0, Protocols and CCTYV Standard Operating Procedures 5.0.
- k) Finalising specifications and Standard Operating Procedures in conjunction with contractor selected to install and operate CCTV.

### 4.11.2 WA Police Responsibilities

The WA Police will be responsible for:

- a) Providing information for and advice on community safety assessment.
- b) In consultation with the City, and in accordance with the MOU, develop and maintain the Protocols and Standard Operating Procedures between Police and the City in relation to their respective roles in accordance with the MOU.
- c) Ensuring Police officers comply with the Code of Conduct and in accordance with the MOU when viewing the CCTV footage which includes use of analytics provided by the City.
- d) Determining the appropriate level and priority of responses required to incidents identified by the CCTV cameras or Analytics, according to available resources and existing priorities.

## **4.12 CSCP Officers in Relation to CCTV Management and Operation**

The role and duties of the Community Safety and Crime Prevention Officers (CSCP) in relation to CCTV Management and Operation include:

- a) Ensuring that the Authorised Personnel perform in a manner which is consistent with the objectives of the CCTV Operations.
- b) Assisting the MSC in the preparation of budget estimates and ensuring the CCTV remains cost effective and to report any depreciation concern, or recommendations to the MSC,
- c) Ensuring compliance with any policies or related acts, for CCTV and to report any breaches identified to the MSC or relevant City of Belmont authority.
- d) Advise the MSC of any significant need for CCTV System modifications or procedures, as required.
- e) In consultation with WA Police, consider implementing or modifying the CCTV surveillance schedules based on police intelligence, and reports of peak crime times, to ensure effective strategies are in place to support CCTV Operations in reducing crime and anti-social behaviour in these or other areas.
- f) Maintain ongoing liaison with WA Police related to CCTV requests, supplied crime statistics, and potential trouble spot's locations or other relevant matters to complement Police priorities and possible CCTV expansions.
- g) Consult with business and community group representatives on their reported security concerns to consider potential CCTV placement options.
- h) Provide a proactive role in improving the effectiveness of Community Safety and Crime Prevention Planning in terms of CCTV Operations.
- i) Ongoing review of the CCTV surveillance strategies, to address problem areas throughout the City of Belmont.
- j) Regularly review the related CCTV Manual to ensure that the City's needs are being met and recommend changes as required.
- k) Maintain an awareness to any changes to CCTV technology, practices, or legislative amendments, which may affect the City's CCTV operational needs guides or manuals to ensure compliance.
- l) Maintain all the City's CCTV Registers.
- m) Ensure compliance in the handling of all recorded CCTV material which includes the supplying footage to a third party and or its disposal.
- o) Ensure appropriate restrictions are in place to limit who accesses the Designated Surveillance Areas.
- p) Ensure all requests reports and investigations related to CCTV are completed within required time frames.
- q) Ensure all Authorised Personnel are sufficiently trained in the management of CCTV Operations.
- r) Foster a high standard of public relations in support of CCTV Operations.

## **4.13 Monitoring, Review and Audit Reports and Protocols**

### **4.13.1 Monthly Monitoring and Reporting**

Data should be presented for inclusion in the monthly report to the MSC including the

1. Number of WA Police CCTV requests
2. Number of Internal CCTV requests.
3. Number of Requests to view CCTV.
4. Annual Feedback from Key stakeholders.

## 4.14 Public Awareness and Media Management

### 4.15.1 CCTV Signage

The importance of effectively placing CCTV signage in the monitored area cannot be underestimated. CCTV signage is to be placed in all locations where CCTV is in operation. This advisory signage plays a key role in CCTV Operation's effectiveness and is known to influence behaviour and perception concerns within the public space areas and are to be checked regularly for damage or theft. It is important that CCTV signage be installed and positioned in areas that allow for the best opportunity to capture user attention aimed at improving safety and crime perception concerns.

### 4.15.2 Media Management

The City holds a range of public events throughout the year and regularly releases 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 MSC in conjunction with the City's Manager PR & Stakeholder Engagement 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 3.2.

## 4.15 CCTV Operation access controls

Access to the City's CCTV system will be restricted to Authorised Personnel only and will be protected from unauthorised access.

The City of Belmont has implemented the following:

1. A procedure that clearly informs Authorised Personnel of possible disciplinary proceedings (including dismissal) if they breach any of the provisions of the Code Conduct.
2. A requirement of confidentiality which can be enforced during and after termination of employment.
3. The circumstances in which WA Police or other visitors access Designated Surveillance Operation Areas will be carefully controlled.
4. Access to the CCTV system will be limited to Authorised Personnel, or approved users.
5. A register must be kept detailing all instances of access to the CCTV system.

## 4.16 Camera Management

### 4.17.1 Camera Selection

Proposed CCTV sites should be risk assessed for environmental and lighting conditions, mounting options, the type of activity, the resolution of cameras, connectivity, and retention of recorded image rates.

The selection criteria for each camera placement and location will be documented and the effectiveness of the installation monitored on an ongoing basis. An objective measurement is the camera's purpose, to either detect, deter, recognise or identify offenders or incidents. The effectiveness of the camera should therefore be found to directly attribute to reducing community safety, or perceptions concerns, or to assist the City. This design base will allow documented design, commissioning, performance, and monitoring of each camera and subsequently, the whole system.

The location of the cameras should be clearly apparent to the public with CCTV signage in the near vicinity of each camera.

Cameras and associated hardware and applications will be replaced or upgraded as required within budgetary restraints.



#### **4.16.2 Camera Risk Assessment**

AS/NZS 31000:2018: 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.

#### **4.16.3 Control and Operation of 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 investigate 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.

#### **4.16.4 Maintaining Camera Operations**

The CCTV Operating system, must always be maintained by:

1. Scheduling regular maintenance programs to ensure the CCTV is fully functional and any defects are reported and actioned.
2. Ensuring all the cameras are recording and displaying correct dates and times with any faults being reported and actioned.
3. Ensuring any identified obstructions to the Cameras Field of Views (FOV) (foliage, umbrellas, street trees and signage) are reported and necessary treatments undertaken to remove the obstructions are actioned.
4. Ensuring a live register is maintained to record reported faults.

#### **4.16.5 CCTV Monitoring Guidelines**

CSCP Officers will regularly review incoming reports or statistics from the City of Belmont Community Watch service and WA Police to identify changing or developing crime trends or hotspot locations and provide resources to target these trends.



#### **4.16.6 Recorded Material**

The retention, treatment, retrieval and access to recorded material will be only for the purposes provided by and in accordance with the City's Code of Practice and Conduct.

Recorded material will be retained for 31 days unless required in relation to the further on an investigation of an incident, or an offence or court proceedings.

Remnant recorded material will be recorded over following 31 days.

Access to and use of recorded material and CCTV still shots will only take place:

- in compliance with the needs of police in connection with any investigation into any reported or identified offences.
- if necessary for the purpose of any legal proceedings.
- to identify community safety issues
- upon a written report of an investigation into a possible breach of the City's policies, procedures, and Local Laws.
- in the monitoring and protection of City assets
- for City educational and presentation purposes.

Recorded material and photographs must 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 not be permitted and will only be provided to WA Police in connection with the investigation of crime or in any other circumstances justified and authorised by law. Footage may be provided to the public but only with a valid FOI request or court order.

When footage is requested by way of an FOI request, it is saved and stored by the City's Authorised Personnel until the FOI process has been completed, and until any applicable decision review deadlines have passed, or until the City of Belmont considers the footage is no longer required.

Use of recorded material by the media should only occur to gain public information with respect to the identity of a person wanted in connection with an investigation and its release will be the responsibility of WA Police in consultation with the City of Belmont.

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.

#### **4.16.7 Contact with WA Police**

Contact related to CCTV Operations between City of Belmont Authorised Personnel, and the WA Police will be conducted strictly in accordance with the MOU, CCTV Code of Conduct and CCTV Management Practice.

Any change in existing arrangements for WA Police contact with and use of the CCTV Operations will amount to a major change to the CCTV Code of Practice and must be agreed to by the City of Belmont in accordance with the Code of Practice before being implemented.

Any involvement in CCTV Operations by WA Police will be documented by the City of Belmont and will be subject to review or audit.

The City will continue to provide WA Police livestream viewing access to public facing CCTV only areas.

# 5.0 CCTV STANDARD OPERATING PROCEDURES

## 5.1 Introduction

These Standard Operating Procedures (SOPs) provide an initial framework for the establishment of tailored procedures specific to the CCTV Operations implemented by the City of Belmont. The objectives of the SOPs are:

- a) To provide personnel with all the work, health, and safety environments required and operational information necessary to perform their roles and responsibilities appropriately.
- 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 City of Belmont and legislative requirements.

## 5.2 CCTV Management Spreadsheet

The City's Authorised Personnel will maintain a register for any requests for recorded material, copies of CCTV footage, identified system faults, maintenance needs, and access to Designated Surveillance Areas.

Frequent exchange of information between WA Police and the City of Belmont is to be recorded subjectively. The rating of the relationship by both stakeholders will be considered a key performance indicator.

## 5.3 Maintaining Compliance and Local Government Best Practice

### 5.3.1 Review

These procedures shall be reviewed on an ongoing basis and key performance indicators reported through the monthly report by the MSC. Improving perceptions of safety and reducing fear of crime following community consultations are reported on annually.

### 5.3.2 Audits

It is essential that the community have confidence in the City use of CCTV technology. The City of Belmont must regularly audit compliance with legislation and standards. In addition to audits, all logs of observations and activity should be regularly scrutinised by the City of Belmont.

### 5.3.3 Incident Reporting and System Analysis

All requests to view or obtained captured CCTV footage, is to be electronically recorded.

For internal staff requests this is done via the City's Pathway system,

For WA Police this should be via the WA Police using their DEMS system or an electronic email request and must include an incident report number.

All other external requests for CCTV must be in writing and must be approved by the MCS, by filling the appropriate forms before release of capture footage can be considered.

The written request should contain the:

- a) Type of incident and includes where possible,
  - i. an incident or
  - ii. reference report number.
- b) Date, time, and location of the incident.
- c) Description of the person(s) (POI) or vehicle(s) (VOI) of interest.
- d) The intent of the request, (i.e.,),
  - i. to identify a POI, VOI.
  - ii. review an incident which has occurred,
    - o For possible prosecution,
    - o civil proceedings (e.g. insurance claim)
  - I. review a City of Belmont staff matter, or,
  - II. other emergency services
- e) Requesting parties must supply there,
  - a. full name, contact details, and,
  - b. company/organisation.

### 5.3.4 Complaints Handling

Any complaints received by the City in relation to alleged breaches of the CCTV Code of Conduct will be dealt with through the City's existing complaints handling procedure.

## 5.4 Authorised Personnel – Selection and Recruitment

All Authorised Personnel assigned to surveillance operations must be authorised by the City to undertake defined roles.

All Authorised Personnel must follow these procedures.

All Authorised Personnel must sign the approved Code of Conduct at the start of their employment with the City of Belmont.

City's 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. under appropriate circumstances, the City reserves the right to terminate employment. These conditions will be detailed in all employment contracts.

The City's Authorised Personnel or CSCP Officers will ensure visitors are briefed regarding the requirements of the Code of Conduct.

The Coordinator Community Safety will provide a formal induction to new Authorised Personnel on CCTV Operations and the CCTV Management and Operations Manual.

The City's Standard Operating Procedures for live surveillance may be adapted to best reflect the requirements of the CCTV System specifications and conducted in accordance with the WA CCTV Guidelines.

The City currently provides no live CCTV surveillance services, however, should the City identify a need for this requirement, the City will do so in accordance with the WA CCTV guidelines and relevant state and federal legislative requirements.

## 5.5 Selection of Contractors and Consultants

There is a role for private sector security providers to assist the City of Belmont in the provision of CCTV Operations and related services, including CCTV design, system installation, system maintenance and independent audits and reviews.

All security providers to the City must provide appropriately qualified personnel and hold relevant licences in accordance with the *Security and Related Activities Act 1996* and current membership of a relevant Security Industry Association.

## 5.6 Surveillance Duties and Tasking

### 5.6.1 Live Surveillance Duties

Should there be a need for a City's Authorised Personnel to view live CCTV, the following procedures need to be adhered to by operator(s) viewing live surveillance:

- a) Operators must act with the utmost probity and in accordance with the Code of Conduct and relevant governing legislation.
- b) Tracking or zooming in on any member of the public shall not be done in a gratuitous or unreasonable manner. Operators should be made aware, that their camera operation may be audited and called upon to satisfy their interest in a member of the public. Members of the public going about their lawful business shall not be the subject of undue, unethical, or illegal surveillance.
- c) No cameras are to view into private premises during normal surveillance. Private premises may only come into view as part of a wide angle or long shot or as a camera is panning past them.
- d) Viewing of private premises may remain if there are reasonable grounds for so doing, (i.e., for the purpose of identifying individuals or actions when there is a reasonable cause in response to a criminal offence or situation of concern only).

At the commencement of live surveillance, operator(s) are to record the following detail on the CCTV Activity Register:

- a) Personal details
- b) Date/time of shift
- c) Designated surveillance tasks, i.e. general surveillance, targeted surveillance, area familiarisation, situational surveillance.
- d) At the completion of each live surveillance period, the operator is to record to completion date/time and a summary of incidents.

### 5.6.2 Dealing with and Responding to Incidents

The CCTV monitoring or control room should be equipped with suitable communication facilities to enable the operator to easily contact the relevant personnel. Estimate an acceptable response time for the activities being monitored and consider whether the operator should continue monitoring the subject or situation until the response arrives and has circumstances return to normal.

A list of Stakeholders and Call Out details will be compiled and maintained in the CCTV Management and Operation Spreadsheet.

In circumstances where a response to an incident or situation is necessary, consider who decides when a response is necessary and what that response should be.

For example, it might be appropriate to contact:

- a) A guard on patrol.
- b) A supervisor.
- c) The police.
- d) DFES.
- e) Ambulance or medical assistance.
- f) Utility emergency services; or

- g) Neighbouring Council officers.

In some cases, it may be appropriate to simply note the event and take no further action.

The level of Police response to incidents occurring will be determined by the WA Police and will be subject to the various priorities at the time the incident is reported. The City has no control over the priority allocated by the Police.

The City's Authorised Personnel are authorised to report relevant matters to the WA Police and other emergency services, as appropriate. A written record of any reports will be made at the time or as soon as practicable following the incident and will include details of the incident, date and time of the report and details of the Police or other public or private services. Where appropriate, the City Authorised Officers may elect to have the City Community Watch Patrol services attend the incident before making a formal report to the Police or emergency services.

All incidents requiring attendance by the Police or other emergency services will be recorded by the City's Authorised Personnel, as soon as practicable.

When an officer identifies an offence or situation of concern to which a response is required, the operator must contact the Police while ensuring that the incident is being appropriately monitored and recorded.

Where possible, the incident must continue to be monitored and recorded up to and including the completion of the response.

Whenever a response is deemed appropriate to an identified incident, the officer must record the following in the CCTV Activity Register:

- a) Type of incident (according to defined offence categories), including description (e.g. number of persons or vehicles involved);
- b) Date and time of incident; and
- c) Organisation making response (i.e. Police or City of Belmont)

An incident report must be filled out by the City's Authorised Personnel and if Police attention is required, a copy is to be provided to the Police. The incident report should record information which will assist Police in the recording of the incident.

The City's Authorised Personnel or CSCP Officers are to check all cameras daily to ensure they are operating correctly.

Checks are to be made to ensure that:

- a) Operator adjustable settings can be made appropriately, and predefined fields of view are displayed.
- b) The time and date settings are correct - it is essential that time and date settings are correct. Any inconsistencies should be documented and the equipment monitored to ensure that further drift of these settings does not occur.
- c) Recording equipment is operating correctly.
- d) The media should either be new, reformatted or erased in an approved manner in accordance with the equipment manual.
- e) Any media protection settings will not prevent recordings being made.
- f) Where possible all CCTV fixed systems should have an Uninterrupted Power Supply (UPS) system are operating to minimise outages.
- g) A scheme of checks is carried out before deployment particularly for equipment that is used less frequently.

This list is not definitive, and detailed information should be obtained from the equipment manuals.

### **5.6.3 Joint Operations with WA Police**

The WA Police and the City of Belmont have a Memorandum of Understanding (MOU).

The City acknowledges the WA Police as a key stakeholder in CCTV Operations.

Members of the WA Police may request the cooperation of the City's CCTV Operations for the purpose of surveillance relating to lawful WA Police operations and investigations.

Joint operation requests can be made by the WA Police officer responsible for coordinating the operation or investigation.

The request should detail the times and general purpose for which surveillance support is requested.

The City may decline to provide cooperation in accordance with the Code of Conduct and Code of Practice.

The City's Authorised Personnel or CSCP officers may withdraw cooperation at any time during the operation in accordance with the Code of Conduct and Code of Practice.

### **5.6.4 WA Police Contacts and State CCTV Register**

For day-to-day purposes, the City of Belmont'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 officer(s), will liaise with the City Authorised Personnel or CSCP officers regarding 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 the MOU 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 authorisation being given by the City's Authorised Personnel or CSCP officers. Police Officers may direct the operation of cameras.

The City's CCTV System will be registered with the WA State CCTV Register. If sought by Police and viable, a remote-control facility at the Police Operations Centre may be allowed. The WA Police must advise the City's CSCP Officers should they wish to access the City's CCTV System and may direct cameras during a live incident, provided the actions requested comply with the 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 (name and regimental number and location) making the request, including details authorising, time and date of the request and reasons for the request. Bien put forward.

### **5.6.5 Transferring Operating Control of Cameras to Police**

City's Authorised Personnel or CSCP officers must only transfer control of cameras to Police personnel when so requested by Police for operational purposes. In such cases, the officer must record the following in the CCTV Activity Register:

- a) The name of the requesting Police officer (name and regimental number and location).
- b) The reason given for the request for transfer of operating control; and
- c) The date, time and length of transfer control.

## 5.7 Camera Operation

### 5.7.1 Control and Operation of the Cameras

The City's CCTV will only be operated by Authorised Personnel. All authorised personnel will act with the utmost probity.

Use of the City's CCTV systems will be in accordance with the key objectives of the Management and Operation Manual, and statutory legislation in place as established, and shall comply with the City's Code of Conduct.

The City's CCTV Cameras will not be used to overlook into private property issues without cause. Contained within the Management and Operation Manual are procedures adopted to ensure restraints upon the use of cameras in connection with private premises.

All Authorised Personnel will be subject.

1. To supervisory procedures to ensure compliance with this aspect of the Code.
2. Are aware that recordings are subject to routine audit and that they may be required to justify their interest in a member of the public or premises.

The City's Authorised Personnel or CSCP officers, in consultation with Police, will determine the level of incidents to be reported to the Police. It is recognised that the decision as to what level of response is deployed is a matter entirely for the Police. The City of Belmont will liaise regularly with the Police on this subject.

A record will be maintained by the City's Authorised Personnel or CSCP officers of all monitored incidents.

Incidents will be recorded as part of the means of establishing effective evaluation and targeting of key objectives.

Incidents should be reviewed to guide:

- Monitoring criteria and schedules.
- Risk assessment; and
- Target offence reduction objectives.

Cameras should only be installed in areas which have been subject to the design of the public space,

- Crime Prevention Through Environmental Design (CPTED) Audit,
- Lighting Audit and a Crime Risk Assessment.
- Camera positioning designed to provide sufficient fields of view of the public space and
- Capabilities to provide identification, recognition, or detection footage.

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

The list of cameras and locations is to be maintained in the CCTV Management Spreadsheet.



## 5.8 CCTV System Expansion and Upgrades

### 5.8.1 Extension of the System

Where an agreement is reached to extend the CCTV System or coverage, or undertake and upgrade to the system the City agrees on the following actions:

1. The MSC must agree on an identified location or extensions requested and that the intent of the installation or upgrade will achieve the primary aims in addressing the associated issues.
2. Takes into consideration the resource implications, and the commitment levels of each stakeholder.
3. That established specifications and protocols are in place for establishing the system and ongoing management and maintenance requirements of that system are always considered.
4. That the system and any upgrades align with the City's Management and Operational manual
5. That all stakeholders agree to and comply with the responsibilities and requirements contained within the CCTV Management and Operations Manual and acknowledging the requirement for all parties to comply with the provisions of the Code of Conduct, including the enforcement of sanctions detailed within the Code.

Prior to any extension or upgrade of the System being approved the following actions will be completed:

1. The MSC will conduct a needs analysis assessment and prioritisation of risk management objectives.
2. Consultation can be undertaken amongst stakeholders where required.
3. Where cameras are to be installed, and or a major software upgrade is proposed, the City of Belmont will consult with all affected parties as appropriate.

## 5.9 Troubleshooting, Faults and Maintenance

All faults and maintenance activities are recorded Refer to the CCTV System's Operation and Technical Manual for troubleshooting and common problems.

### 5.10 Data Storage

Refer to the Milestone CCTV Operation and Technical Manual for storage configuration and commissioning.

Footage must be downloaded using the Milestone CCTV program in the "Database" file format. A copy will also be stored on the secure CCTV server. The "Database" format cannot be altered once created.

AVI copies can be created but only as a working copy, and only for evidentiary purposes.

If copied into DVD-R, format it is not possible to overwrite or altered.

The software required for viewing is provided on the DVD-R when it is created.

Any requests for CCTV footage will be kept on the WA Police Footage Request Log.

Provisions are also being made to allow for back up servers to be placed at an alternate City facility to maintain continuity of captured footage as part of it risk management process.

### 5.11 Data Access



### 5.11.1 Access to Designated Surveillance Operations Areas

Only Authorised Personnel are permitted to access the CCTV system.

Visitors to the Section must be authorised by a City of Belmont Authorised or CSCP officer and a record made of the purpose of the visit in the CCTV Activity Register.

Authorised Personnel and or visitors must wear an approved identification, or visitors card whilst in the CCTV section and must be accompanied by one of the CSCP Officers.

## 5.12 Continuity of Evidence

Evidence, in terms of a still image or captured CCTV footage, is the presentation of visual facts about an offence, or an individual that the prosecution presents to the court in support of their case.

The image can be presented either as hard copy or on a screen. It is possible to make a 'bit-for-bit' 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, as this is all determined to be documentary evidence. 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 server.

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, such things as changing to the clock on a CCTV system will affect the image authenticity but not affect the image integrity. Robust audit trails are required to maintain image authenticity.

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

- a) Details of the case.
- b) 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.
- c) Identity of the capture operative, including third parties and image retrieval officers, where applicable.
- d) Details of exhibits and disclosure officer(s).
- e) Description of the images captured.
- f) Details of retrieval or seizure process and point of transfer, if applicable.
- g) Creation and definition of the Master copy and associated metadata.
- h) Storage of the Master copy.
- i) Any access to the Master copy.
- j) Viewing of the footage, including a record of any associated viewing logs.
- k) Details and reasons for any selective capture.
- l) Electronic history log of processing applications.
- m) Any copying required for ensuring longevity of the data.
- n) Cross References on the Master and Working Copies, if required.
- o) Disposal details and retention time periods.

## 5.13 Viewing of Recorded Material

WA Police officers may request to view recorded material relating to an incident or investigation. Such requests must be in writing and must specify the officers name and include the date, time and location of the incident and the related report number linked to that incident.

Requests made by any internal staff, must be done via the City's internal operating system (Pathway) and must be in relation to a reported incident, and the request must be lodged by the Coordinator or Manager of that department or section and recorded in the City's incident report system.

Requests made by any external parties other than WA Police, for which the City has an established MOU with, must be made via a FOI request or subpoenaed.

Each FOI request will be assessed in accordance with the *Freedom of Information Act 1992*, to determine whether footage can be viewed or released.

However, where such external requests are being made, (not court related), then a written application form needs to be completed (External CCTV request form) by the requesting party, and the completed form needs to be sent to the City's Authorised or CSCP officers for further consideration and assessment. The MSC or CEO would be the final determinant in such an application.

Please note, any request, by any internal or external parties other than the WA Police, to view or use captured CCTV footage, which is part of an ongoing Police investigation, is to be refused, and the requesting party should be directed to contact the investigation officer within the WA Police.

Requests by Police must be made via email, and or the WA Police DEMS system to the City's Authorised Personal or CSCP officers.

All written requests to view recorded material must be responded to as soon as reasonably practicable or otherwise within five (5) working days. Written Police requests are to be dealt with as a priority.

### 5.13.1 Copying of Recorded Material

Only the City's Authorised Personnel or CSCP officers can make a copy of original material where a recorded incident is the subject of an investigation, prosecution or legal proceeding.

Copies of the recorded material are to be marked with the incident / case report number and a description of the incident and the requesting officer's name.

Certified copies of recorded material may only be released to the WA Police in relation to a recorded incident under an MOU agreement, or any other nominated party as approved when written permission to do so is provided by the City's Chief Executive Officer, or his nominated delegated officer.

### 5.13.2 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, court summons or by a recognised legal instrument; and

Original or copied recordings or still photographs, will not be released to any media organisation, journalist or other individual or group without submitting a valid FOI request and following the approval of such a release by the City's Chief Executive Officer.

### **5.13.3 Video Images**

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

- a) An easily read text file stating any requirements for special software or instructions for replay.
- b) All associated metadata (time and date should be bound to the relevant images); and
- c) Licence-free software enabling the sequences to be viewed correctly.

### **5.13.4 Master Copy Safeguards**

The integrity of images needs to be protected at the earliest stages as this reduces the opportunities for challenges in court.

The City stores all its Master copies in a secure electronic format.

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

### **5.13.5 Encryption**

The image file is encrypted so that the file cannot be altered, which maintains its integrity when presented as evidence in court.

### **5.13.6 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.

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.

### **5.13.7 Define Master and Procedure 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; and
- d) Never used, except to make further copies together with appropriate audit trail, or by order of the court to verify integrity.

### **5.13.8 Produce Working Copies**

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 City of Belmont. Issues of quality control, security and resource management must be considered.

### **5.13.9 Recording of Images**

CCTV images may only be recorded by the City.

All information recorded, collected and collated by means of CCTV Operations shall remain the sole property of the City.

Any incident recorded and selected for review shall be noted in the CCTV Activity Register including date, time, and type of incident.

The date, time and category of incident and related report numbers, shall be noted on the recorded medium and electronic file name.

All recorded material shall be kept in secured storage, including electronically, under the control of the City.

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 recorded in Pathway and or ECM.

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

The City's Authorised Personnel or CSCP officers shall view the CCTV Activity Register and reports will be submitted monthly, or as otherwise directed.

## **5.14 Operation Redundancy and Disaster Recovery**

The City of Belmont has redundant power supplies, UPS protection, redundant hard drives in the storage array, and secure external hard drives, stored at an alternate site for the recovery of data following power outages, system faults and other impediments to operations.