



Queensland State Archives

Managing Closed Circuit Television  
(CCTV) Records  
Guideline for Queensland Public Authorities

October 2010

## Document details

<b>Security Classification</b>	PUBLIC
<b>Date of review of security classification</b>	October 2010
<b>Authority</b>	Queensland State Archives
<b>Author</b>	Queensland State Archives
<b>Document Status</b>	Final Version
<b>Version</b>	Version 1.0

## Contact for enquiries

All enquiries regarding this document should be directed in the first instance to:

Manager, Policy and Research  
Queensland State Archives  
07 3131 7777  
[info@archives.qld.gov.au](mailto:info@archives.qld.gov.au)

## Copyright

*Managing Closed Circuit Television (CCTV) Records*

Copyright © The State of Queensland (Department of Public Works) 2010

## Licence



*Managing Closed Circuit Television (CCTV) Records* by Queensland State Archives is licensed under a Creative Commons Attribution 2.5 Australia Licence. To view a copy of this licence, please visit <http://creativecommons.org/licenses/by/2.5/au/>.

## Information security

This document has been security classified using the Queensland Government Information Security Classification Framework (QGISCF) as PUBLIC and will be managed according to the requirements of the QGISCF.

## TABLE OF CONTENTS

<b>1.</b>	<b>Introduction.....</b>	<b>5</b>
	<b>1.1 Purpose.....</b>	<b>5</b>
	<b>1.2 Audience.....</b>	<b>6</b>
	<b>1.3 Authority.....</b>	<b>6</b>
	<b>1.4 Scope.....</b>	<b>6</b>
	<b>1.5 Using this Guideline.....</b>	<b>6</b>
	<b>1.6 Definitions.....</b>	<b>7</b>
	<b>1.7 Acknowledgements.....</b>	<b>7</b>
<b>2.</b>	<b>Legislative and Regulatory Requirements.....</b>	<b>8</b>
	<b>2.1 Visual Surveillance Context.....</b>	<b>8</b>
	<b>2.2 Public Records Act 2002.....</b>	<b>8</b>
	<b>2.3 Information Privacy Act 2009.....</b>	<b>9</b>
	<b>2.4 Right to Information Act 2009.....</b>	<b>9</b>
	<b>2.5 Legislative Context for Surveillance.....</b>	<b>9</b>
	<b>2.6 Information Standard 40: Recordkeeping.....</b>	<b>10</b>
	2.6.1 Principle 7: Full and Accurate Records.....	11
	<b>2.7 Information Standard 31: Retention and Disposal of Public Records.....</b>	<b>12</b>
	<b>2.8 Additional Relevant Information Standards.....</b>	<b>12</b>
<b>3.</b>	<b>CCTV Organisational Framework.....</b>	<b>13</b>
	<b>3.1 Defining the Surveillance Function.....</b>	<b>15</b>
	<b>3.2 Identifying Operational Issues.....</b>	<b>17</b>
	<b>3.3 Specifying System Requirements.....</b>	<b>18</b>
	<b>3.4 Establishing an Appropriate Management Framework.....</b>	<b>19</b>
<b>4.</b>	<b>Recordkeeping Processes for CCTV Records.....</b>	<b>21</b>
	<b>4.1 Create and Capture.....</b>	<b>22</b>
	4.1.1 Lawful Purpose.....	22
	4.1.2 Collection Notices.....	24
	4.1.3 Creating CCTV Records that are Fit for Purpose.....	25
	4.1.4 CCTV Recorders.....	26
	4.1.5 Capture and Storage in a Recordkeeping System.....	26
	4.1.6 Evidential Audit Trail: Primary, Original, and Working Images.....	26
	4.1.7 Analogue versus Digital Recording.....	27
	4.1.8 Field of View.....	28
	4.1.9 Frame Rate.....	28
	4.1.10 Image Resolution.....	29
	4.1.11 Video Compression and File Formats.....	29
	4.1.12 Recordkeeping Metadata.....	32

<b>4.2 Use</b> .....	<b>34</b>
4.2.1 <i>Use of Personal Information</i> .....	34
4.2.2 <i>Third Party Handling of CCTV Records</i> .....	35
<b>4.3 Storage</b> .....	<b>37</b>
4.3.1 <i>Security of Storage</i> .....	37
4.3.2 <i>Encryption</i> .....	37
4.3.3 <i>Preservation</i> .....	38
4.3.4 <i>Recorded Materials Register</i> .....	41
4.3.5 <i>Storage Media</i> .....	41
4.3.6 <i>WORM Media versus Secure Servers</i> .....	42
4.3.7 <i>Re-Useable Media</i> .....	43
4.3.8 <i>Storage Capacity</i> .....	43
<b>4.4 Retrieval</b> .....	<b>45</b>
4.4.1 <i>Media Retrieval</i> .....	45
4.4.2 <i>Native File Formats</i> .....	45
4.4.3 <i>Disclosure of Personal Information for the Protection of an Individual or the Public</i> ..	46
4.4.4 <i>Disclosure of Personal Information for Law Enforcement</i> .....	47
4.4.5 <i>Disclosure of Personal Information for Other Purposes and to Other Entities</i> .....	48
<b>4.5 Disposal</b> .....	<b>49</b>
4.5.1 <i>Retention and Disposal</i> .....	49
4.5.2 <i>Documenting Disposal of Public Records</i> .....	50
<b>Appendix A: CCTV Checklist</b> .....	<b>52</b>
<b>Appendix B: Glossary</b> .....	<b>55</b>
<b>Appendix C: Australian Standards</b> .....	<b>58</b>
<b>Appendix D: Codes of Practice</b> .....	<b>59</b>
<b>Appendix E: International Standardisation Initiatives</b> .....	<b>61</b>
<b>Appendix F: Australian Research into CCTV</b> .....	<b>62</b>
<b>Appendix G: Comparison of Video File Formats</b> .....	<b>63</b>
<b>Appendix H: Logs</b> .....	<b>65</b>
<b>Appendix I: Calculation of Storage Requirements</b> .....	<b>67</b>

# 1. Introduction

Closed circuit television (CCTV) has been increasingly deployed across Queensland public authorities for a variety of visual surveillance purposes. These purposes span incident monitoring, detection and deterrence, contributing to the safety of the public, personnel and property. The use of CCTV extends to operational areas such as traffic monitoring on roads, rail and at sea, and the provision of evidence in Queensland courts.

Effectively managing CCTV records as public records may present significant challenges. Issues which may need to be addressed by public authorities include the proliferation of proprietary visual surveillance systems and encodings, overcoming poor picture quality owing to the lack of operational standards, the divergence in business processes to manage the records, and a lack of recognition of the total cost of ownership in managing records throughout their lifecycle.

## 1.1 Purpose

Appropriately designed and implemented visual surveillance systems will capture surveillance images that are, and will continue to be, fit for their intended purpose.

The purpose of this Guideline is to assist public authorities to meet their information management and recordkeeping obligations under the *Public Records Act 2002* with respect to practices surrounding visual surveillance systems. It will assist public authorities with the implementation of CCTV surveillance systems which produce images sufficient for functional purposes, including law enforcement, while protecting the privacy of individuals.

Recordkeeping cannot be seen in isolation from the technical requirements which are necessary to capture CCTV records. Consequently, this Guideline outlines the key records management processes to be considered at different stages of the surveillance operation and makes recommendations on core technical elements of the design, implementation, maintenance and management of visual surveillance systems.

Adherence to this Guideline will assist public authorities in the management of CCTV records, resulting in the following benefits:

- Compliance with the *Public Records Act 2002*
- Creation of 'full and accurate' public records in compliance with *Information Standard 40: Recordkeeping*
- Consistent data quality
- Continuity of business processes
- Accessibility of public records and efficiency of storage
- Integrity, with public records being fit for forensic purposes and presentation in a court of law, if required
- Appropriate handling of personal information in compliance with the *Information Privacy Act 2009*.

## **1.2 Audience**

The intended audience for this Guideline includes staff responsible for records and information management within Queensland public authorities, including Chief Information Officers, in addition to heads of security operations, business managers responsible for planning and implementing CCTV, and ICT staff responsible for the maintenance of records created by CCTV systems.

## **1.3 Authority**

Queensland State Archives is responsible for the provision of policy advice relating to a wide range of strategic information management and recordkeeping issues for Queensland public authorities. This Guideline forms part of a wider recordkeeping policy framework.

The State Archivist has issued this Guideline in accordance with section 25(1)(f) of the *Public Records Act 2002*, which enables the Archivist to make policy, standards, and guidelines about the making, keeping, preserving, managing and disposing of public records.

## **1.4 Scope**

This Guideline is intended for Queensland public authorities, as defined in Schedule 2 of the *Public Records Act 2002*, and is customised to the Queensland legislative environment. While certain recordkeeping principles will have universal application, other Australian and international jurisdictions choosing to use this Guideline are advised to seek legal advice as to the operation of their legislative instruments with regard to surveillance.

This Guideline does not apply to covert surveillance conducted under statutory authority or search warrant.

## **1.5 Using this Guideline**

This Guideline consists of three key components. The first component of this Guideline outlines the legislative and regulatory requirements relating to the management of CCTV records as public records. The second component discusses the CCTV organisational framework, designed to help public authorities specify their visual surveillance operations. The third component provides an in-depth discussion of the recordkeeping processes for CCTV records, including outlining the key technical requirements to be considered for visual surveillance technologies. This section covers the lifecycle of CCTV records, from creation through to disposal. A summary of the key recordkeeping requirements is presented as a checklist at the conclusion of each phase of the lifecycle.

Appendix A contains a complete checklist of the key recordkeeping considerations for CCTV records. This checklist is designed to be used as a tool to assess existing CCTV systems against the key recordkeeping considerations of this Guideline, or to be used for the design and implementation of new systems in compliance with the requirements of this Guideline.

## **1.6 Definitions**

A Glossary providing clarification and definitions of terms relating to the operation of CCTV used in this document is included as Appendix B.

Records and information management-specific terms are defined in Queensland State Archives' *Glossary of Archival and Recordkeeping Terms* available on Queensland State Archives' website.<sup>1</sup>

## **1.7 Acknowledgements**

Queensland State Archives (QSA) conducted a questionnaire in 2009 about the use of CCTV records within the Queensland public sector. In developing this Guideline, QSA acknowledges the contributions of 70 public authorities including Government Departments, Local Governments, Government Owned Corporations, Statutory Entities and Universities.

In addition, the preparation of this Guideline has been greatly assisted by in-depth discussions and/or site visits with the following:

- Crime and Misconduct Commission, Queensland
- Office of the Information Commissioner, Queensland
- Port of Brisbane Corporation
- Queensland Rail CCTV Analysis Unit
- State Government Protective Security Service
- Queensland Police Service, and
- South Australian Police.

This Guideline has drawn substantially from the extensive work undertaken by the UK Home Office Scientific Development Branch (HOSDB)<sup>2</sup> and the Senior Managers of Australian and New Zealand Forensic Laboratories (SMANZFL) Electronic Evidence Specialist Advisory Group.<sup>3</sup>

The development of this Guideline has been supported by the Queensland Government ICT Innovation Fund.<sup>4</sup>

---

<sup>1</sup> [www.archives.qld.gov.au/downloads/GlossaryOfArchivalRKTterms.pdf](http://www.archives.qld.gov.au/downloads/GlossaryOfArchivalRKTterms.pdf)

<sup>2</sup> [www.homeoffice.gov.uk/science-research/hosdb/](http://www.homeoffice.gov.uk/science-research/hosdb/)

<sup>3</sup> [www.nifs.com.au/SMANZFL/SMANZFL.html](http://www.nifs.com.au/SMANZFL/SMANZFL.html)

<sup>4</sup> <http://ggcio.govnet.qld.gov.au/govnet/projectsandservices/funding/Pages/index.aspx>

## 2. Legislative and Regulatory Requirements

**Public authorities must meet legislative and regulatory requirements relating to the management of CCTV recordings as public records.**

### 2.1 Visual Surveillance Context

Visual surveillance recordings used by public authorities to monitor business transactions may constitute public records. Consequently, public authorities must meet all legislative and regulatory requirements relating to the management of CCTV recordings as public records.

The legislative context for surveillance in Queensland is detailed below<sup>5</sup>. Public authorities implementing new visual surveillance systems or reviewing existing systems may wish to assure themselves that all CCTV recordings captured are managed appropriately with regard to legislative requirements.

The CCTV checklist provided in Appendix A of this document comprises a summary of the key recordkeeping considerations identified throughout this Guideline to assist public authorities in either their implementation of CCTV or in their evaluation of existing CCTV processes against recordkeeping and legislative requirements.

Also, the following appendices provide information regarding the broader visual surveillance arena:

- Appendix C provides information about the four Australian Standards relating to the management, operation, and technical specifications of CCTV
- Appendix D describes existing Codes of Practice with regard to the use of CCTV footage in Australia
- Appendix E summarises international standardisation initiatives for networked CCTV interoperability, and
- Appendix F details selected Australian research into CCTV.

### 2.2 Public Records Act 2002

Recordkeeping in the Queensland public sector is governed by the *Public Records Act 2002*, which covers all public records irrespective of the technology or medium used to generate, capture, manage, preserve and access those records. All public records, including electronic records, are subject to legislation and to legal processes such as discovery and subpoenas.

As public records, CCTV recordings made by public authorities are subject to the *Public Records Act 2002* and associated recordkeeping Information Standards, *Information Standard 40: Recordkeeping* and *Information Standard 31: Retention and Disposal of Public Records*.

---

<sup>5</sup> This Guideline acknowledges that there may be other legislative requirements specific to individual public authority's records management obligations. This Guideline provides a summary of the records management obligations of Queensland public sector authorities.



## 2.3 Information Privacy Act 2009

Queensland's *Information Privacy Act 2009*<sup>6</sup> provides rules for how agencies must handle personal information. These rules include the Information Privacy Principles and the National Privacy Principles. As the National Privacy Principles apply only to Queensland Health, and are substantially similar to the Information Privacy Principles, except in regard to collection of documents and the definition of personal information, this guide makes reference only to the Information Privacy Principles. The requirements of a number of these Information Privacy Principles have been integrated into this Guideline as they are of particular relevance to the creation, capture, use and retrieval of visual surveillance records. Special consideration would be given to Queensland Health records given its reliance on the National Privacy Principles and the additional confidentiality obligations under the *Health Services Act 1991*.

## 2.4 Right to Information Act 2009

The primary objective of Queensland's *Right to Information Act 2009*<sup>7</sup> is to give a right of access to information in the government's possession or under the government's control unless, on balance, it is contrary to the public interest to give the access. Records captured from CCTV systems may form part of information discovery requests.

## 2.5 Legislative Context for Surveillance

Legislation changes frequently. It is the agency's responsibility to identify any legislation in addition to the *Public Records Act 2002*, *Information Privacy Act 2009* and the *Right to Information Act 2009* that may apply to the records captured in the agency's CCTV operation.<sup>8 9</sup>

In Queensland, specific aspects of surveillance covered by legislative instruments include, but are not limited to, those detailed below:

Legislation	Purpose
<b><i>Crime and Misconduct Act 2001</i></b>	Section 121 of the <i>Crime and Misconduct Act 2001</i> describes the application process for obtaining surveillance warrants. Section 128 describes the powers bestowed to commissioned officers under these surveillance warrants.
<b><i>Liquor Act 1992</i></b>	Division 6 of the <i>Liquor Act 1992</i> contains provisions relating to liquor licensing in the Brisbane City Council Area; specifically, section 142AH details conditions relating to CCTV equipment in licensed venues.

<sup>6</sup> <http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/I/InfoPrivA09.pdf>

<sup>7</sup> <http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/R/RightInfoA09.pdf>

<sup>8</sup> The Australian Customs and Border Protection Service site provides an overview of other Australian jurisdictions' legislation applicable to CCTV at [www.customs.gov.au/site/page5979.asp](http://www.customs.gov.au/site/page5979.asp)

<sup>9</sup> For a comparative study of European and United Kingdom legislative frameworks, see 'The Legal Regulation of CCTV in Europe' by Marianne L. Gras, *Surveillance & Society CCTV Special* (eds. Norris, McCahill and Wood) 2 (2/3): 216-229 (2004) at [www.surveillance-and-society.org/cctv.htm](http://www.surveillance-and-society.org/cctv.htm)

Legislation	Purpose
<b>Security Providers Act 1993</b>	The <i>Security Providers Act 1993</i> defines who is a security provider, bodyguard, crowd controller, private investigator, security adviser, security equipment installer, security officer, and security firm. It outlines the terms and conditions of licences and temporary permits for installation of security equipment.
<b>State Buildings Protective Security Act 1983</b>	This legislation establishes the State Government Protective Security Service, charged with providing services for the security of state buildings. It encompasses the appointment of protective security officers, and establishes standards for their fitness and propriety.
<b>Transport Infrastructure Act 1994</b>	Chapter 8, Part 3 of the <i>Transport Infrastructure Act 1994</i> specifies the functions and powers of Port Authorities in Queensland. Section 275 (1) (d) specifies that a function of Port Authorities Security is to keep appropriate levels of safety and security in the provision and operation of the Ports' facilities and services.
<b>Transport Operations (Passenger Transport) Regulation 2005</b>	Part 6, Division 4 of the <i>Transport Operations (Passenger Transport) Regulation 2005</i> details the requirements for taxi security camera systems in Queensland. It encompasses the use of, and safeguards for, image recordings taken from taxis, ensuring images can be admissible as evidence (e.g. where requested for law enforcement purposes).

Also, CCTV systems and recordings are referenced by relevant Australian Standards <sup>10</sup> and, in some instances, by Codes of Practice. <sup>11</sup>

## 2.6 Information Standard 40: Recordkeeping

This Guideline seeks to assist public authorities in their compliance with the principles of *Information Standard 40: Recordkeeping* (IS40) which applies to records in all formats. The recordkeeping requirements outlined in this Guideline, and summarised in Appendix A, adhere to the minimum mandatory requirements of IS40.

*Information Standard 40: Recordkeeping* is the umbrella recordkeeping policy for Queensland public authorities as defined in Schedule 2 of the *Public Records Act 2002*.<sup>12</sup> As it applies to records in all formats, CCTV recordings must be managed according to its principles.

*Information Standard 40: Recordkeeping* details seven mandatory principles public authorities are subject to. These principles are summarised in Table 1 on the following page.

<sup>10</sup> Appendix C provides information about the four Australian Standards relating to CCTV which are available at [www.saiglobal.com/shop/script/Details.asp?DocN=AS229907590845](http://www.saiglobal.com/shop/script/Details.asp?DocN=AS229907590845)

<sup>11</sup> Appendix D describes existing Codes of Practice regarding the use of CCTV footage in Australia.

<sup>12</sup> [www.archives.qld.gov.au/downloads/QGEAInformationStandard40v2.0.0.pdf](http://www.archives.qld.gov.au/downloads/QGEAInformationStandard40v2.0.0.pdf)

**Table 1: Mandatory Principles of Information Standard 40: Recordkeeping**

<b>Principle</b>	<b>Requirement</b>
Principle 1:	Public authority recordkeeping must be <b>compliant and accountable</b>
Principle 2:	Recordkeeping must be <b>monitored and audited</b> for compliance
Principle 3:	Recordkeeping activity must be <b>assigned and implemented</b>
Principle 4:	Recordkeeping must be <b>managed</b>
Principle 5:	Recordkeeping systems must be <b>reliable and secure</b>
Principle 6:	Recordkeeping must be <b>systematic and comprehensive</b>
Principle 7:	<b>Full and accurate records</b> must be made and kept for as long as they are required for business, legislative, accountability and cultural purposes.

### **2.6.1 Principle 7: Full and Accurate Records**

Principle 7 of *Information Standard 40: Recordkeeping* details the *Public Records Act 2002* requirement that Queensland public authorities make and keep ‘full and accurate’ records of their activities. The characteristics of full and accurate records are detailed in Table 2 below.

**Table 2: Characteristics of Full and Accurate Records**

<b>Attribute</b>	<b>Requirement</b>
<b>Adequate:</b>	Records must be fit for the purposes for which they are created and kept. They should provide adequate evidence of an agency’s conduct of a business activity to be able to account for that conduct. Records that document more important or higher risk transactions or processes need to be more detailed than records which document low risk activities.
<b>Complete:</b>	To be complete, records should contain not only content, but also the structural and contextual information necessary to document and make sense of the business transaction. It is therefore necessary to maintain adequate recordkeeping metadata relating to the record, to demonstrate that it is a true and accurate representation of the transaction, activity or facts.
<b>Meaningful:</b>	Records must be able to be understood within the context of the processes and business for which they are created and in which they are used.
<b>Accurate:</b>	Records must correctly reflect what was communicated, decided or done (or not done). That is, the record’s contents, context and structure can be trusted as true and accurate representation of the transactions, activities or facts to which it attests and can be relied upon in the course of subsequent transactions or activities.
<b>Authentic:</b>	An authentic record is a record that can be proven and trusted to be what it purports to be. It must have been created, used, transmitted or retained by the person who claims to have done these actions.
<b>Inviolable:</b>	To be regarded as inviolable, a record must be securely maintained to prevent unauthorised access, alteration, removal or destruction. The internal and external processes to which a record has been subject should be traceable.

Attribute	Requirement
<b>Accessible:</b>	Records must remain accessible and available to people both inside and outside the agency, in accordance with security, privacy and legislative requirements, for the designated period for which they must be retained. To be accessible, records must be maintained so that they can be quickly and easily identified, viewed and retrieved when required.
<b>Useable:</b>	Useable records are those that can be viewed and remain fully functional. Records must be kept in a format that allows their continued use.

Management of CCTV records should follow appropriate recordkeeping processes throughout their lifecycle to ensure that they continue to maintain the above characteristics.

Section 4 of this Guideline details key recordkeeping processes for CCTV records.

## **2.7 Information Standard 31: Retention and Disposal of Public Records**

Records should be created, captured, and retained in an accessible and useable format to appropriately document an authority's essential business activities. A record's evidential integrity should be preserved for as long as it is required to support the agency's business and to fulfil its legal obligations.

*Information Standard 31: Retention and Disposal of Public Records* relates specifically to the appraisal, retention and disposal of public records. The *Public Records Act 2002* prohibits the disposal of public records without the permission of the State Archivist. This permission is usually given through authorised Retention and Disposal Schedules, as detailed in section 4.5.1 *Retention and Disposal*.

## **2.8 Additional Relevant Information Standards**

Other relevant Information Standards which public authorities should consider in developing any policy related to management of information include *Information Standard 18: Information Security (IS18)*; *Information Standard 25: Intellectual Property (IS25)*; and *Information Standard 34: Metadata (IS34)*.

### 3. CCTV Organisational Framework

**Public authorities should provide an appropriate organisational framework that supports the management of CCTV records.**

To establish a visual surveillance operation which is compliant with legislative and regulatory requirements surrounding recordkeeping, it is important to:

1. Define the surveillance function
2. Identify operational issues
3. Specify system requirements
4. Establish an appropriate management framework.

The following flow chart may assist public authorities in their establishment of an appropriate organisational framework to support the management of CCTV records. It will support the creation of visual surveillance records that are full and accurate, as required by Principle 7 of *Information Standard 40*, and fit for purpose, whether operational or evidentiary.

Examples of the steps entailed in each of the four points above are outlined in Figure 1 on the following page. A brief description of key aspects will follow. Further supporting detail can be obtained in the UK Home Office Scientific Developments Branch's *CCTV Operational Requirements Manual 2009*.<sup>13</sup>

---

<sup>13</sup> Available at [http://www.nactso.gov.uk/SiteCollectionDocuments/ManagingTheRisk/28\\_09\\_CCTV\\_OR\\_Manual2835.pdf](http://www.nactso.gov.uk/SiteCollectionDocuments/ManagingTheRisk/28_09_CCTV_OR_Manual2835.pdf)

Figure 1: Establishing an Appropriate Organisational Framework for CCTV<sup>14</sup>

1. Define the Surveillance Function						
Location	→	Activity	→	Purpose of Observation	→	Target Speed
Car Park Reception Point of Sale		Theft Vandalism Public Safety		Identify Recognise Monitor Detect		Stationary Walking Variable
2. Identify Operational Issues						
Who Monitors	→	When Monitored	→	Where Monitored	→	Response
Trained Staff Police		24/7 Office Hours As Needs Basis		Locally Remotely Mobile Platform		Contact Decision Maker Emergency Services Continue Monitoring
3. Specify System Requirements						
Alert Function	→	Displays	→	Recording	→	Export/Archive
Visual Audible Integrated System		Type Number Size		Retention Period Image Quality Frame Rate Metadata		Video Export Facilities 3 <sup>rd</sup> Party Access Replay Software
4. Establish a Management Framework						
Standards & Constraints	→	Legislation	→	Maintenance	→	Resources
Recordkeeping & Security Standards Regulations Licensing		<i>Public Records Act (2002)</i> <i>Information Privacy Act (2009)</i> Other legislation relevant to your CCTV operation		Cleaning Repairs Upgrades Warranties Product Life-cycle		Staff Training Accommodation Consumables

<sup>14</sup> This specification is adapted, with permission, from the UK Home Office Scientific Developments Branch *CCTV Operational Requirements Manual 2009* available at [http://www.nactso.gov.uk/SiteCollectionDocuments/ManagingTheRisk/28\\_09\\_CCTV\\_OR\\_Manual2835.pdf](http://www.nactso.gov.uk/SiteCollectionDocuments/ManagingTheRisk/28_09_CCTV_OR_Manual2835.pdf)

### **3.1 Defining the Surveillance Function**

It is regularly noted that where CCTV is deployed for the deterrence and detection of crime, CCTV systems form only part of the security solution for any organisation, that is, cameras should be deployed in conjunction with crime prevention measures such as access control, and physical security implementations.

To help define the surveillance function, public authorities should consider the following questions with respect to each activity:

- Where on the premises needs to be monitored?
- Which potential threat or activity needs to be monitored?
- How much detail is needed in the picture?
- How fast will the target be moving?

When defining the purpose of the CCTV surveillance function, it is suggested that the design and use of CCTV systems could be addressed in a process similar to that described in the Tasmanian Crime Prevention & Community Safety Council *Policing Requirements for Closed Circuit Television*.<sup>15</sup> The brochure discusses the attributes of a functional system, installation, set-up, system maintenance and data management. With regard to camera locations and purpose, Figure 2 on the following page shows the differences between images fulfilling different purposes for installation.

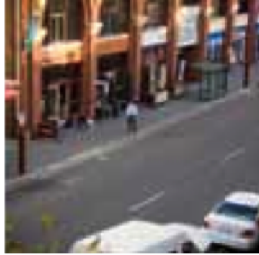
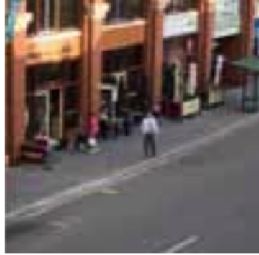
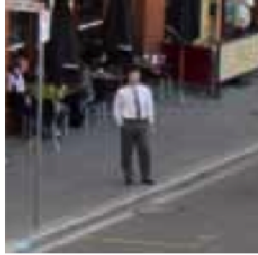

When planning a CCTV installation, an agency needs to demonstrate a clear and lawful business case for its use. The essential feature of any visual surveillance system is that it is designed to meet operational objectives, and that its use complies with legislative requirements.

---

<sup>15</sup> [http://www.police.tas.gov.au/uploads/file/Pamphlets/Closed\\_Circuit\\_Television\\_brochure.pdf](http://www.police.tas.gov.au/uploads/file/Pamphlets/Closed_Circuit_Television_brochure.pdf)

**Figure 2: Comparison of CCTV Image Displays for Varying Purposes**

Image used with the permission of Tasmania Police<sup>16</sup>

			
<b>OBSERVE</b>	<b>DETECT</b>	<b>RECOGNISE</b>	<b>IDENTIFY</b>
<p>This is where a person or vehicle (target) occupies 5 percent of the monitor's viewing height.</p> <p>Cameras located to observe and enable the viewer to know someone was there. The time and date stamp shows what time they were there. The image size will be too small for identification but will place a person or vehicle at the scene when considered with other images - ie: recognise and identify.</p>	<p>A person or vehicle will occupy 10 percent of the monitor's viewing height.</p> <p>At this size, the target's image will be adequate for detection using video motion detection, if installed on the system, but would be too small to identify the person for evidence purposes. If a system is monitored it will provide enough detail to indicate the person is doing something suspicious.</p>	<p>A person or vehicle will occupy 50 percent of the monitor's viewing height.</p> <p>At this field of view, the target's image can be recognised if they are already known to staff. They would not be accurately identified if they are unknown. However, the person could be recognised as the same person in different camera shots.</p>	<p>At 120 percent of the monitor's viewing height, images are of suitable quality to enable identification of individuals and provide distinguishing features of vehicle number plates. Police will have the greatest chance of enlarging the images and capturing vital details.</p>

In addition to the information described above in the Tasmanian Crime Prevention & Community Safety Council *Policing Requirements for Closed Circuit Television*, the COAG CCTV Code of Practice provides detailed recommended CCTV performance criteria and parameters for each of the operational objectives of *Observation, Detection, Recognition and Identification*<sup>17</sup>.

<sup>16</sup> [http://www.police.tas.gov.au/uploads/file/Pamphlets/Closed\\_Circuit\\_Television\\_brochure.pdf](http://www.police.tas.gov.au/uploads/file/Pamphlets/Closed_Circuit_Television_brochure.pdf)

<sup>17</sup> COAG Working Group. A national approach to closed circuit television: national code of practice for CCTV systems for mass passenger transport sector for counter-terrorism. 14 July 2006. [http://www.coag.gov.au/coag\\_meeting\\_outcomes/2006-07-14/docs/cctv\\_code\\_practice.pdf](http://www.coag.gov.au/coag_meeting_outcomes/2006-07-14/docs/cctv_code_practice.pdf)



### 3.2 Identifying Operational Issues

Operational issues will vary widely dependent on the scale of the visual surveillance operation.

As a starting point for the identification of operational issues, public authorities should consider the following questions with respect to each activity:

- How will CCTV be monitored (i.e. actively, passively or by recording)?<sup>18</sup>
- Who will be responsible for the monitoring of CCTV screens?
- Who will be responsible for the management of the CCTV records?
- Which hours during the day, and which days in the week might live monitoring be required?
- Where is the CCTV control room located? Where no control room or monitoring exists, how will CCTV footage be obtained?
- What happens when an event occurs?

*Information Standard 40: Recordkeeping* provides the basis for public authorities to manage their rights and responsibilities relating to the making and keeping of public records. Recordkeeping activities must be assigned and implemented through responsible management by individuals and systems. In defining the essential business functions of recordkeeping, public authorities must:

- Formally assign responsibility for recordkeeping activities to those conducting Government business
- Communicate roles and responsibilities for records management across the organisation.

Principle 4 of *Information Standard 40* states that recordkeeping must be administered by appropriately skilled staff. At a minimum, public authorities must assign responsibility for recordkeeping to an appropriately skilled manager or senior administrative officer.

The rights and responsibilities associated with the different roles performed within the CCTV system – owners, managers, supervisor, operators and contractors – are detailed in Part 1 of the Australian CCTV Standard, AS 4806.1–2006. The standard also outlines training requirements, noting that there should be a formal plan that addresses these.<sup>19</sup>

Queensland's *Security Providers Act 1993* and *Security Providers Amendment Act 2007* define the roles and legal responsibilities of security providers, advisers, equipment installers, and officers. The legislation outlines terms and conditions of licences and temporary permits for those who work with CCTV operations.

Further detail relating to the operation of control rooms can be found in Part 1 of the Australian CCTV Standard, AS 4806.1-2006.

---

<sup>18</sup> [www.coag.gov.au/coag\\_meeting\\_outcomes/2006-07-14/docs/cctv\\_code\\_practice.rtf](http://www.coag.gov.au/coag_meeting_outcomes/2006-07-14/docs/cctv_code_practice.rtf) provides further information about the various monitoring methods.

<sup>19</sup> Appendix C provides further information about the four Australian Standards relating to CCTV.

### 3.3 Specifying System Requirements

Once the surveillance function has been clearly defined and operational issues and constraints have been identified, the following questions should be raised with respect to each activity to obtain a starting position on the system elements and settings for CCTV installations required.

- What action should the system take when an event is detected?
- How will the images be viewed?
- How long must the video be retained on the system before being overwritten?
- What image quality is required on the recorded image compared with the live image?
- What frame rate is required for the recorded video?
- What metadata should be recorded with the video?
- How will data be exported from the system to create a record for appropriate retention?
- Who will require access to the data (e.g. police etc.)?
- How will they replay the video (e.g. is special software required)?

The recording and export functions identified at the stage of defining system requirements are of particular importance for the creation of full and accurate records. Specific details surrounding these requirements are outlined in section *4.1 Create and Capture*.

'A CCTV system is by definition a television system that transmits images in a 'closed loop'. Images are only available to people directly connected to the transmission system or given access rights to a closed user group within an information and communications technology network'.<sup>20</sup>

The quality of the records generated by CCTV systems depends on the combined operation of the following components:

- Cameras and lenses, appropriately positioned, calibrated, and housed to capture the activities of the agency
- Lighting
- Digital recorders with adequate storage space to retain records for the required period
- Monitors
- Compression algorithms to ensure evidentiary quality, and
- Mechanisms and procedures to capture and extract evidence with appropriately labelled storage media.

CCTV system elements should not be capable of being adjusted or removed other than by documented processes.

---

<sup>20</sup> [http://www.coag.gov.au/coag\\_meeting\\_outcomes/2006-07-14/docs/cctv\\_code\\_practice.pdf](http://www.coag.gov.au/coag_meeting_outcomes/2006-07-14/docs/cctv_code_practice.pdf)

The CCTV system should be installed and configured according to the manufacturer's specifications and agency's operational procedures to ensure that images produced by the system are of sufficient quality to observe, detect, recognise, or identify people and objects as required. A site plan should document the location and field of view of each camera in the facility, as determined during system design.<sup>21</sup> Consideration should be given to the physical conditions in which the cameras operate, and the resources required for system operation and maintenance.

Initial and routine checks of the agency's CCTV operation should ensure that:

- The field of view of each camera is correctly adjusted and focus is maintained
- The system's time and date settings are correct (i.e. the time/date generator displays correctly and is synchronised to the exact time/date on all equipment)
- Sufficient storage media is available to retain records for the required periods
- Storage media are regularly checked for faults
- Media protection settings will not prevent recordings being made
- Redundancy is built into the system, with adequate spare media and battery backup available.<sup>22</sup>

### **3.4 Establishing an Appropriate Management Framework**

Part 1 of the Australian CCTV Standard, AS4806.1–2006 states:

It should be the responsibility of all parties connected with a CCTV system to maintain a continuous review of its integrity, security, procedural efficiency and methods of operation in respect of the gathering, retention and release of data.

The following questions may assist public authorities to establish appropriate management frameworks for visual surveillance systems:

- Which licensing regulations apply to the CCTV system?
- What laws apply to the storage of and access to information?
- What regular maintenance is required?
- Who is responsible for ongoing maintenance tasks?
- What are the resources required to operate and maintain the system and to create and maintain records?

According to the Principle 1 of *Information Standard 40*, public authorities must implement a strategic approach to recordkeeping that is endorsed by the agency's Chief Executive. Public authorities must comply with public records legislation and other legal and administrative requirements for managing records within the areas in which they operate. Establishing an appropriate management framework requires the identification of appropriate legislative requirements and standards. It is also important that resources be identified to support the appropriate management of public records, and that systems are regularly maintained and audited for compliance.

---

<sup>21</sup> Please refer to Section 4 of this Guideline for a discussion of technical specifications

<sup>22</sup> As per SMANZFL (2004) *Australasian Guidelines for Digital Imaging Processes*  
[www.nifs.com.au/2004%20Digital%20Imaging%20Guidelines.pdf](http://www.nifs.com.au/2004%20Digital%20Imaging%20Guidelines.pdf)

In line with Principle 2 of *Information Standard 40: Recordkeeping*, systems generating and managing records should be monitored and audited for compliance. The operation of all CCTV equipment and systems should therefore be verified before use, and monitored regularly. System evaluations should be documented, with modifications to hardware and software being noted in a log.

An appropriate maintenance schedule should be outlined by the agency to regularly check that all system elements are operating according to specification. To ensure continued quality of recording, system maintenance should be performed by approved technicians, in accordance with manufacturer recommendations. Details of maintenance should be documented in a log, commencing from the date of purchase. Appendix H contains an example which public authorities may choose to use as the basis for their system maintenance log.

Test recordings should be made during maintenance to compare captured images to the original recordings. These may be used to ascertain that the system has not degraded or suffered damage from environmental or human factors. These recordings should be stored in a recordkeeping system alongside the records to which they relate.<sup>23</sup>

Detail regarding preventative maintenance is contained in section 7 of Part 2 of Australian CCTV Standard, AS4806.2-2006.<sup>24</sup>

---

<sup>23</sup> Recordkeeping system (definition) 'The interaction of the technology, people, principles, methods, processes and information systems which captures, manages and provides access to records through time.' Adapted by Queensland State Archives from AS ISO 15489, Part 1, Clause 3.17  
See [www.archives.qld.gov.au/downloads/GlossaryOfArchivalRKTerms.pdf](http://www.archives.qld.gov.au/downloads/GlossaryOfArchivalRKTerms.pdf)

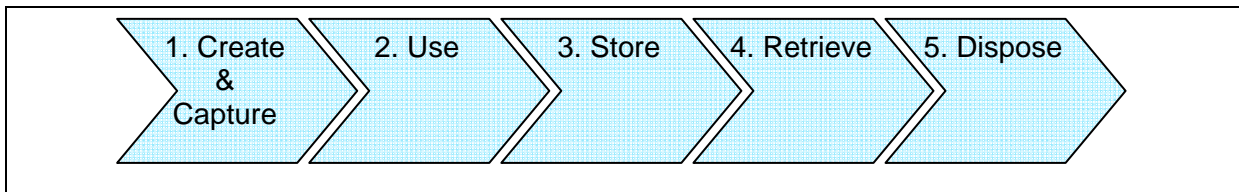
<sup>24</sup> Appendix C provides further information about the four Australian Standards relating to CCTV.

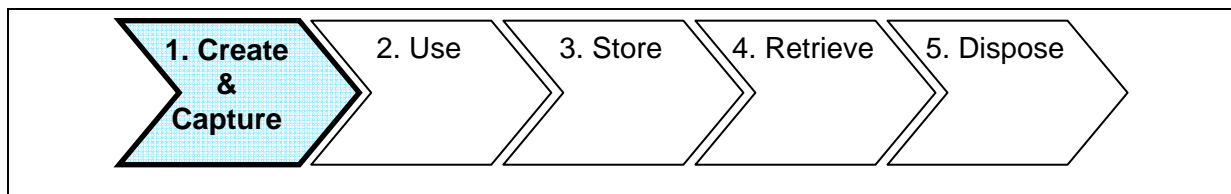
## 4. Recordkeeping Processes for CCTV Records

**Public authorities should follow appropriate recordkeeping processes in the creation, use, storage, retrieval, and disposal of CCTV records. It should be ensured that CCTV records are fit for purpose, in accordance with operational and forensic requirements where they may be used in evidence.**

The management of CCTV records should follow appropriate recordkeeping processes, as detailed throughout this section and illustrated in Figure 3 below. These processes support recordkeeping that is systematic and comprehensive, as required by Principle 6 of *Information Standard 40: Recordkeeping*, and facilitate the creation of full and accurate records and their appropriate retention for business, legislative, accountability and cultural purposes, as required by Principle 7.

**Figure 3: Recordkeeping Processes for CCTV Records**





#### **4.1 Create and Capture**

As required by *Information Standard 40: Recordkeeping*, CCTV records should be created and captured to be 'full and accurate' public records. Refer to section 2.6.1 to review the characteristics of full and accurate records.

##### **4.1.1 Lawful Purpose**

In capturing personal information via CCTV, the agency must comply with the relevant Information Privacy Principles set out in the *Information Privacy Act 2009*.<sup>25</sup>

The Office of the Information Commissioner has released *Information Privacy Act 2009 Guidelines* 'intended to assist agencies and members of the public to understand the privacy principles and the privacy rights and obligations contained in the *Information Privacy Act 2009*'.<sup>26</sup>

It is recommended that agencies consult the above document together with this Guideline (*Managing Closed Circuit Television (CCTV) Records*), as this Guideline contains only summary information on selected aspects of the Information Privacy Principles most relevant to the collection and management of visual surveillance records.

#### **Information Privacy Principles 1 – 3: Collection of Personal Information**

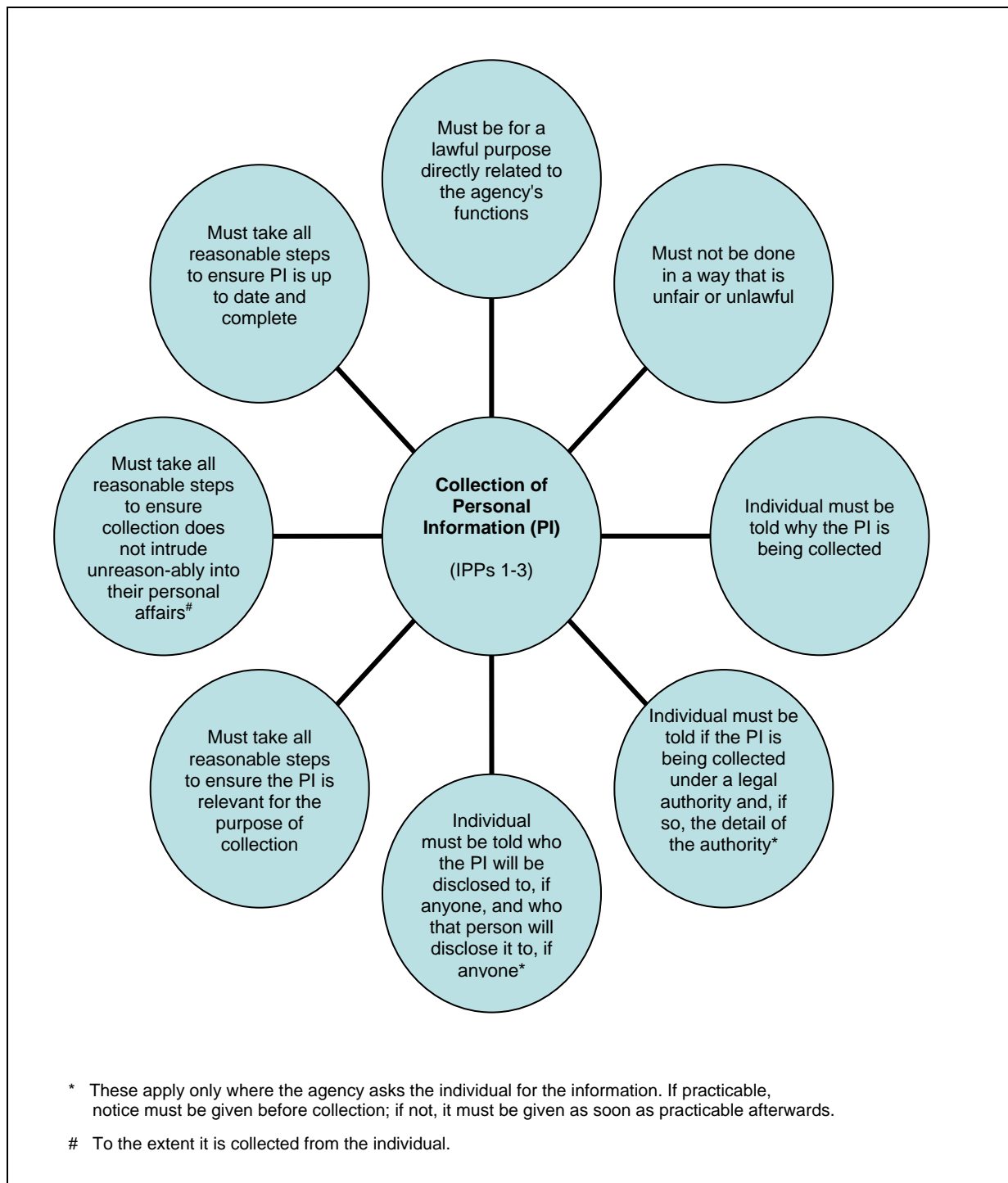
Information Privacy Principles 1 – 3 relate to the collection of personal information by an agency. Figure 4 on the following page summarises the aspects of these three Information Privacy Principles.

<sup>25</sup> [www.legislation.qld.gov.au/LEGISLTN/CURRENT/I/InfoPrivA09.pdf](http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/I/InfoPrivA09.pdf)

<sup>26</sup> [www.oic.qld.gov.au/files/IPAGuidelines/Privacy%20Guideline%20%28complete%29%20-%2030-06-09.pdf](http://www.oic.qld.gov.au/files/IPAGuidelines/Privacy%20Guideline%20%28complete%29%20-%2030-06-09.pdf)

**Figure 4: Summary of Information Privacy Principles 1-3 – Collection**

Image used with the permission of the Office of the Information Commissioner, Queensland



Closed Circuit Television recordings will contain personal information if the identity of the individual captured is apparent or can be reasonably ascertained. If so, any information concerning that individual (e.g. that they are in the vicinity of the camera at that particular time) constitutes that individual's personal information. The design and use of CCTV systems (section 3.1 of this Guideline) will determine the extent of personal information collected. For example, CCTV systems established to observe will not contain personal information, as it would be unlikely that an individual could be identified. Alternatively, CCTV

systems installed to identify will contain personal information, and the agency must comply with the relevant Information Privacy Principles set out in the *Information Privacy Act 2009*.<sup>27</sup>

#### **4.1.2 Collection Notices**

Where CCTV systems are in operation, a Collection Notice must be displayed to allow individuals to consider whether they wish to proceed knowing that they may be recorded and how their image may be used.

While not required to carry standardised wording, CCTV Collection Notices must comply with the requirements of **Information Privacy Principle 2** of the *Information Privacy Act 2009*<sup>28</sup>, ensuring that the individual being filmed is aware of the purpose of collection, any legal requirements for collection, and the possibility that the footage may be disclosed, or passed to another agency.

An agency must tell people it collects personal information and describe:

- Why the information is being collected
- Details of any law that allows or requires the collection of personal information
- Details of any person or body to whom the agency usually gives the information
- If any person or body to whom the agency regularly gives information in turn regularly gives it to any other person or body and the agency is aware of this, details of the other person or body.

A sample Collection Notice is provided in Figure 5 below.

**Figure 5: Example Collection Notice**

**These premises are protected by Closed Circuit Television**

Images are recorded by the Department of Keeping People Safe for the purposes of crime prevention and public safety, in accordance with the *Keeping People Safe Act (2020)*.

Images may be provided to the State Police Service.

For further information, please contact John Smith, Manager, Security Operations, on (07) 3000 1111.

<sup>27</sup> [www.legislation.qld.gov.au/LEGISLTN/CURRENT/I/InfoPrivA09.pdf](http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/I/InfoPrivA09.pdf)

<sup>28</sup> [www.legislation.qld.gov.au/LEGISLTN/CURRENT/I/InfoPrivA09.pdf](http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/I/InfoPrivA09.pdf)



### 4.1.3 Creating CCTV Records that are Fit for Purpose

This Guideline highlights the importance of maintaining image quality which is fit for purpose, whether that be evidentiary or operational.

Attention should be paid to the following four factors, identified by the UK Home Office Scientific Development Branch *CCTV Operational Requirements Manual 2009*, which are key in ensuring CCTV image quality and in generating records that are fit for purpose:

1. **Clarity** – Is the picture sharp enough, and is there any lens distortion? Ensure that the lens or lens/camera combination is of sufficient quality for operational requirements.
2. **Detail** – Is there enough detail to identify objects? Ensure that detail is not compromised in the attempt to capture too much of the scene (via large field of view, section 4.1.8).
3. **Colour** – Is colour necessary? Natural? If accurate colour reproduction is required, ensure that lighting is of sufficient quality to illuminate the scene.
4. **Artefacts** – Are there errors in the image? Do they obscure critical information? Depending on the artefact, either the amount of compression needs to be reduced, or camera/lighting placement needs to be addressed.<sup>29</sup>

To guide users and installers in the appropriate design of a CCTV system, Part 2 of the Australian Standard on CCTV, AS4806.2–2006, offers technical advice on:

- Camera and lens selection criteria
- Recommended object sizes
- Ancillary equipment
- Evaluation of scene and illumination
- Selection of the video transmission system
- System diagnostics
- Control centre configuration
- System test specification
- Export and playback of video footage and images
- Time and date integrity.

The Standard also provides a framework for objectively evaluating the performance of an installed system.

Further discussion of technical consideration can be found in the UK Home Office Scientific Development Branch *CCTV Operational Requirements Manual 2009*.<sup>25</sup>

---

<sup>29</sup> Available at

[http://www.nactso.gov.uk/SiteCollectionDocuments/ManagingTheRisk/28\\_09\\_CCTV\\_OR\\_Manual2835.pdf](http://www.nactso.gov.uk/SiteCollectionDocuments/ManagingTheRisk/28_09_CCTV_OR_Manual2835.pdf)

#### **4.1.4 CCTV Recorders**

The majority of contemporary CCTV systems use Digital Video Recorders (DVRs), where images are typically recorded onto a hard disk drive, as in modern computers. DVRs have the ability to set image quality and frame rate, which are key determinants of storage requirements, as shown in Appendix I. DVRs have limited storage capacity on board, which often means that images are overwritten as space is used. Equally, adjusting the image retention period so that storage is maximised may result in lower quality images.

CCTV system requirements should specify the required recorded image quality and frame rate for each camera. Attention should also be paid to compression algorithms, which are covered in section 4.1.11 *Video Compression and File Formats*.

#### **4.1.5 Capture and Storage in a Recordkeeping System**

In accordance with Principle 4 of *Information Standard 40*, recordkeeping must be managed through an identifiable recordkeeping program that includes records in all formats, and be administered by appropriately skilled staff. Public authorities must implement an identifiable records management program with documented policies, procedures, and business rules. A record's capture and storage within a suitably designed and implemented recordkeeping system will support its continuing authenticity, integrity, reliability, and usability.

It is advisable for public authorities to manage records associated with visual surveillance by capturing them as electronic objects within a recordkeeping system, such as an Electronic Document and Records Management System (eDRMS) or other business system with recordkeeping functionality. Alternatively, records associated with visual surveillance should be stored securely, with appropriate controls to ensure the attributes of full and accurate records are retained, with metadata captured into a recordkeeping system.

These recordkeeping systems should have accurately documented policies, assigned responsibilities and formal methodologies for their management.

#### **4.1.6 Evidential Audit Trail: Primary, Original, and Working Images**

Agencies collecting images for security purposes should safeguard the integrity of the surveillance record from the time of its creation. This is necessary should the CCTV footage need to be presented in court where its accuracy must be established.

The procedures outlined in the Senior Managers of Australian and New Zealand Forensic Laboratories (SMANZFL) *Australasian Guidelines for Digital Imaging Processes* make a distinction between Primary, Original, and Working Images for this purpose, as follows:

**Primary Image:** The first instance in which an image is recorded onto any media that is a separate, identifiable object or objects.

**Original Image:** Exact binary copy of the Primary Image. There can be a number of Original Images. While the file name can be changed, the actual image data must remain exact.

**Working Image:** A copy of the Original or Primary Image. This may involve applying processes that change file format or Original Image data in any way (including compression, enhancement, filtering, cropping, etc.).<sup>30</sup>

**The Original Image should not be subjected to processes that cause permanent alteration. Where any type of enhancement is desired, a Working Image must be made.**

In the course of an agency's operations, Primary Images are generally transferred onto secure servers or other appropriate archival media from the recording device, thereby becoming Original Images. As an exact binary copy of the Primary Image, the Original Image will now be considered the 'master,' and an official public record, sentenced according to the *General Retention and Disposal Schedule for Administrative Records*<sup>31</sup> or the agency's core business Retention and Disposal Schedule.

When no longer required for the agency's business processes, Primary Images are then able to be appropriately disposed of in accordance with the relevant Retention and Disposal Schedule. See section 4.5.1 *Retention and Disposal* for further details.

Once an image has been defined as an Original Image, its integrity should be maintained. Section 4.3.5 *Storage Media* recommends that agencies avoid storing CCTV in systems where the native format is a proprietary, non-standard format, or one which is not widely used. If it may be necessary to keep footage for a long time, it is recommended that that equipment is selected where the native format is a widely used standard (e.g. MPEG-4).

If an Original Image is to be used in evidence, it must be shown to be identical to the Primary Image, with notes made as to the process of copying the image file from a memory card to a hard disk drive. In addition, details should be made of any person who has accessed the Original Image in a manner that could affect the integrity of the image.

To establish appropriate audit trails, records should be created by those involved in CCTV image capture and handling processes to verify the origin, authenticity, and integrity of the image. Details regarding the downloading of the Primary Image, the creation, use and storage of the Original Image(s), and adjustments leading to Working Images should be noted. Any adjustments must be repeatable – an appropriately trained technician should be able to recreate the Working Image from the Primary Image if necessary. Disposal actions should also be recorded, in compliance with *Information Standard 31: Retention and Disposal of Public Records*, as addressed in section 4.5.1 *Retention and Disposal*.

#### **4.1.7 Analogue versus Digital Recording**

The transition from analogue to digital recording has had a significant impact on the functionality of CCTV systems. In researching this Guideline, responses to Queensland State Archives' CCTV questionnaire indicated that the majority of CCTV installations in Queensland now use digital recording facilities. Tape based analogue recording systems are becoming obsolete technology. It is unlikely that the technology will be further developed, and consequently the number of manufacturers of players and media will fall. Selecting analogue technology for new CCTV installations may expose an organisation to a risk of not being able to access the records over a lengthy period of time.

In comparison with tape-based analogue systems, digital operations offer:

---

<sup>30</sup> [www.nifs.com.au/2004%20Digital%20Imaging%20Guidelines.pdf](http://www.nifs.com.au/2004%20Digital%20Imaging%20Guidelines.pdf)

<sup>31</sup> [www.archives.qld.gov.au/downloads/GeneralDisposalSchedule.pdf](http://www.archives.qld.gov.au/downloads/GeneralDisposalSchedule.pdf)

- Higher image quality
- Ability to embed metadata
- Increased storage options
- Greater ease of image retrieval and duplication of data.

It is important to design, install and maintain systems to ensure both operational efficiency and effectiveness. The reality of many digital systems is that:

- Lossy compression compromises image quality
- Metadata is often unstructured and varies between manufacturers
- Systems may be designed to reduce storage requirements, rather than taking into account the purpose for which they have been installed
- Processes for exporting video are complex and may be specific to each manufacturer.

By developing and implementing a management framework which covers the CCTV system processes described in this Guideline, Queensland's public authorities should be able to overcome these issues.

#### **4.1.8 Field of View**

Field of View (FoV), or angle of view, is a measure of the extent of a given scene captured by the camera. A camera's FoV is determined by its lens configuration, sensor size, and where the camera is positioned in relation to the scene. Fixed lenses have set fields of view, while cameras with varifocal or zoom lenses have adjustable fields of view. In general, the larger the FoV, such as seen in wide-angle lenses, the smaller the target object. The smaller the sensor, the narrower the FoV.

When determining the FoV required of a camera, it is important to avoid areas such as shadows and blind spots. FoV should be restricted to the purpose of the surveillance; attention should also be given to areas in which a person's privacy may be breached. Camera placement should be based on achieving an optimum view; the choice of location should not be dictated by ease of installation.

The Internet offers a variety of CCTV lens calculator tools to determine the combination of sensors and lenses appropriate to a given scene. Input values are typically object distance (anticipated distance from camera to target) and the horizontal or vertical view required.

#### **4.1.9 Frame Rate**

Frame rate refers to the speed at which a video system records unique consecutive images, and is typically measured in frames per second (fps). The higher the frame rate, the higher the quality of the recording. To achieve recording with real-time attributes, where the viewer sees the motion smoothly, frame rate is set to 25 fps (PAL) or 30 fps (NTSC). Many CCTV systems are constrained by bandwidth, and operate in time-lapse mode of 6–12 fps, or as little as 1 fps. Recent research into crime detection recommends a minimum of 8 fps.<sup>32</sup>

---

<sup>32</sup> Keval, H., & Sasse, M.A. (2008). To Catch a Thief – You Need at Least 8 Frames Per Second: The Impact of Frame Rates on User Performance in a CCTV Detection Task. *Proceedings of the 16<sup>th</sup> ACM International Conference on Multimedia*, 941-944.

The Department of Transport and Main Roads' *Recommended Specifications for Closed Circuit Television (CCTV) Fitted in Queensland Buses* suggests that 6 fps be recorded in normal mode, and 25 fps in alarm or alert mode.<sup>33</sup>

As with other parameters, the CCTV frame rate settings should be adjusted to meet operational requirements – if the scene is complex, or the target of high speed, then a high frame rate is advised. For simpler operations, a lower frame rate may suffice.

#### **4.1.10 Image Resolution**

Image resolution describes the detail and clarity of an image, and is therefore a primary indicator of the quality of that image. Resolution is a measure of the number of lines or pixels in an image file. Resolution is dependent upon the quality of the CCTV camera and lens, shutter speeds, allocation of bandwidth, compression algorithms used in recording, and the quality of display monitors. With higher resolution comes the requirement for higher storage capacity, as the amount of data contained in an image increases. Higher resolution cameras will also require proportionally brighter light sources. The resolution chosen for a scene depends on the operational objective of the installation – higher resolutions will be required for higher risk areas.

#### **4.1.11 Video Compression and File Formats**

The current constraints of processing power and storage capacity mean that video files are stored in a reduced, or compressed, form. Compression can also effectively reduce the bandwidth required to transmit video.

Video compression algorithms reduce the amount of data stored in an image by altering:

- The number of pixels in the image or resolution – spatial compression
- The interval between the images or frame rate – temporal compression
- The amount and efficiency of the data storage – data compression.

Spatial compression operates on a single image, rather than a series of images, removing data that is not required to describe the image. Adjustments to spatial compression, i.e. resolution, are usually found in high-end cameras, where various formats can be chosen.

Temporal compression, or interframe compression, compares one frame in the video to the previous, and stores the differences. If little changes between successive frames, little storage space is required. This method allows for the prediction of frames.

Data compression falls into two categories: lossy and lossless. While lossless algorithms, which preserve the image 'as is,' may appear preferable, they consume significantly larger amounts of space than lossy algorithms, in which some of the original image data is discarded. Compression techniques attempt to achieve the preservation of the most significant areas of an image to strike an optimum balance between fidelity and storage requirements. Operators must be aware that the more compression applied, the smaller the file size, but the larger the loss of image quality.

A significant issue encountered with digital CCTV to date has been that there is no universal standard for the compression of video images, with manufacturers employing a variety of

---

<sup>33</sup> [http://www.tmr.qld.gov.au/~media/travel-and-transport/public-transport/pdf\\_pt405\\_recommended\\_specifications\\_for\\_cctv\\_0408.pdf](http://www.tmr.qld.gov.au/~media/travel-and-transport/public-transport/pdf_pt405_recommended_specifications_for_cctv_0408.pdf)








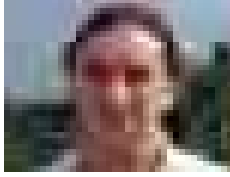



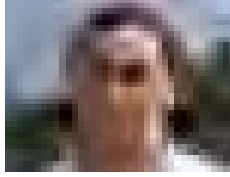


open, proprietary and mixed compression formats. Compression formats for the transmission and storage of still and moving images include: MPEG-1, MPEG-2, MPEG-4, JPEG, M-JPEG, JPEG-2000, H.263, and H.264. These are tabulated in Appendix G.

At present, the MPEG-4 (Part 10) compression algorithm, known as H.264, offers the best video quality for most CCTV scenarios. This standard is more efficient than its predecessors, and is designed to deliver high quality video for both high and low resolutions and bandwidths.

Figure 6 on the following page illustrates the effects of compression on image quality using two current compression techniques: wavelet and DCT (Discrete Cosine Transform). Wavelet compression is gaining in popularity given that its artefacts, typically fuzziness and a diffusion of the image, are less obvious to the human eye than the 'blockiness' produced under DCT.

**Figure 6: Effects of Compression on Image Quality**

Image used with the permission of the UK Home Office<sup>34</sup>

DCT Compression		Wavelet Compression
 <p>Blocking is visible in the sky and colour changes exist on the boundaries</p>  <p>Very clear blocking and slight ambiguity with some of the characters</p>  <p>Blocking and blurred detail is visible in both the sky and trees</p>	<p style="text-align: center;"><b>Live View Image (High Resolution)</b></p>  <p>Above, the car's number plate is clearly visible and the model's features can be easily described. Below however some of the characters on the number plate have become ambiguous and the model's features are much harder to discern.</p> <p>The difference between these two images is the resolution. Above the image resolution is typical for a live viewed image whereas below, the resolution has been reduced as often occurs when the image is recorded. Image compression technology, as shown in the side panels, may further reduce the recorded picture quality.</p>	 <p>Image is generally smeared with a loss of detail throughout</p>  <p>Good retention of character definition and image shape</p>  <p>Image is smeared with very little detail in both sky and trees</p>
   <p>Low resolution images and heavy DCT compression provides images of very little use Significant blocking and very little detail remain in the image</p>	<p style="text-align: center;"><b>Recorded Image (Low Resolution)</b></p> 	   <p>Low resolution images and heavy Wavelet compression provides images of little use Extensive blurring ensures little detail remains</p>

<sup>34</sup>[http://www.nactso.gov.uk/SiteCollectionDocuments/ManagingTheRisk/28\\_09\\_CCTV\\_OR\\_Manual2835.pdf](http://www.nactso.gov.uk/SiteCollectionDocuments/ManagingTheRisk/28_09_CCTV_OR_Manual2835.pdf)

#### 4.1.12 Recordkeeping Metadata

To facilitate the ongoing management and retrieval of visual surveillance records, Queensland public authorities must adhere to at least the minimum mandatory requirements of *Queensland Recordkeeping Metadata Standard and Guideline (QRKMS)*<sup>35</sup>, as specified in Principle 7 of *Information Standard 40: Recordkeeping*. Appendix B of the Standard specifies the minimum mandatory elements required to enable appropriate recordkeeping.

The UK Home Office Scientific Development Branch (HOSDB) report on the *Storage, Replay and Disposal of Digital Evidential Images* notes that surveillance systems should automatically generate the time and date of image capture; the camera number and location and the software version.<sup>36</sup>

The report recommends that all such metadata be retained and managed in a way that ensures its reliable association with the relevant image, taking into account the complexities of proprietary formats.

During installation, unique references should be allocated for all equipment. It is also recommended that the correct time, date, and camera number and location should be automatically embedded on all CCTV recordings and be able to be read when the image is played back on a different system without interfering with the view of the target area. Recordings should be able to be selected by any camera, or selection of cameras and for the required time period.

Digital Video Recorders typically allow the CCTV operator to search for events by time, date, and camera.

In addition, the HOSDB *Digital Imaging Procedure* notes that removable media storing CCTV records, such as CD/DVDs, should be marked with the following metadata:

- The image sequence/s clearly identified
- A text file stating any special hardware or software requirements for replay
- All associated metadata (time and date should be bound to the relevant images).<sup>37</sup>

To facilitate current and future use of the recordings within the context of the records' creation, other items which may be included are:

- Text data about the originating camera or system
- Audit trails
- Authentication or verification software
- A short test sequence to confirm that the recorded image sequences are being replayed correctly.

The HOSDB *Digital Imaging Procedure* additionally notes that making analogue VHS recordings from digital files will often cause the loss of metadata and therefore care should be taken during this process.

---

<sup>35</sup> [www.archives.qld.gov.au/downloads/QRKMS.pdf](http://www.archives.qld.gov.au/downloads/QRKMS.pdf)

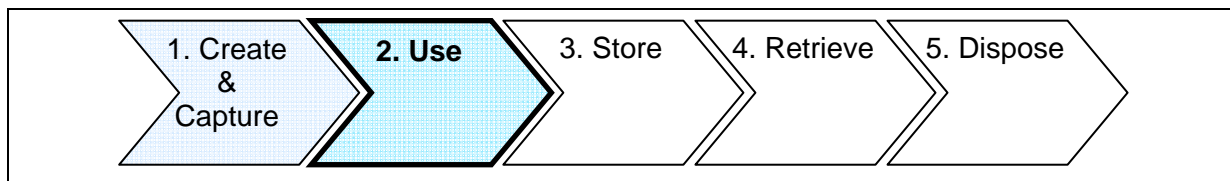
<sup>36</sup> Home Office Scientific Development Branch 2007, *Digital Imaging Procedure* (no. 53/07).

<sup>37</sup> [http://tna.europarchive.org/20100413151426/http://scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/DIP\\_2.1\\_16-Apr-08\\_v2.3\\_\(Web\)2835.pdf?view=Binary](http://tna.europarchive.org/20100413151426/http://scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/DIP_2.1_16-Apr-08_v2.3_(Web)2835.pdf?view=Binary)



<b>Create &amp; Capture – Key Recordkeeping Considerations</b>	
The agency's surveillance operation is lawful and directly related to the agency's function.	<input type="checkbox"/>
CCTV images produced by the system are fit for purpose – to observe, detect, recognise, or identify people or objects as appropriate.	<input type="checkbox"/>
The agency's collection of personal information is in accordance with Information Privacy Principles 1 – 3.	<input type="checkbox"/>
CCTV collection notices are prominently displayed, detailing the purpose of the surveillance, the authority under which the records are created, and parties to whom the surveillance record may be given.	<input type="checkbox"/>
The CCTV system has been installed and configured according to the manufacturer's specification and agency's operational requirements.	<input type="checkbox"/>
CCTV records captured into and managed by recordkeeping systems are accessible and meaningful, and are maintained with appropriate controls to ensure the attributes of full and accurate records are retained.	<input type="checkbox"/>
Original Images are preserved as exact copies of the Primary Image, with appropriate audit trails being maintained. Working Images are created where appropriate.	<input type="checkbox"/>
Mandatory recordkeeping metadata <sup>38</sup> associated with the CCTV records is captured into an identified recordkeeping system to ensure ongoing accessibility.	<input type="checkbox"/>

<sup>38</sup> [www.archives.qld.gov.au/downloads/QRKMS.pdf](http://www.archives.qld.gov.au/downloads/QRKMS.pdf)



## **4.2 Use**

The use of surveillance records should be controlled and auditable. Business processes should be in place requiring surveillance system operators to record system actions and events appropriately.

Documentation systems should be in place to officially note actions affecting the system. Section 9.2 of the Australian CCTV Standard AS4806.1–2006 provides detailed guidance on the range of system actions which should be logged or registered.<sup>39</sup>

Appendix H provides a number of generic example logs including the following:

- CCTV Incident Log
- CCTV Maintenance Log / Fault Reports Log
- CCTV Viewing Log
- Issued Copy of Image Log
- Daily CCTV System Check Log (Operators Log).

Regular checks and audits should be conducted to ensure that documentation systems are functioning effectively.

To preserve inviolate and authentic records, it is recommended logs should either be bound books with printed, numbered pages to prevent page removal and/or replacement or electronic databases which show sequential entries that are secured in append-only files so that these cannot be overwritten. Documentation should be carried out at the time of the incident and not retrospectively.

### **4.2.1 Use of Personal Information**

Use of personal information is governed by the *Information Privacy Act 2009* through Information Privacy Principles 8 and 9 detailed in Figure 7 on the following page relating to ensuring the accuracy of personal information and using it only for relevant purposes. Use is also governed by Information Privacy Principle 10, which outlines when personal information may be used, and is addressed in sections 4.4.3 through 4.4.5 of this Guideline. When an agency intends to use surveillance records containing personal information, it must comply with these Information Privacy Principles.

---

<sup>39</sup> Available from [www.saiglobal.com/shop/script/Details.asp?DocN=AS229907590845](http://www.saiglobal.com/shop/script/Details.asp?DocN=AS229907590845)

**Figure 7: Information Privacy Principles 8 and 9<sup>40</sup>**

**Information Privacy Principle 8**

**– Checking of accuracy etc. of personal information before use by agency**

Before an agency uses personal information contained in a document under its control, the agency must take all reasonable steps to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, complete and up to date.

**Information Privacy Principle 9**

**– Use of personal information only for relevant purpose**

- (1) This section applies if an agency having control of a document containing personal information proposes to use the information for a particular purpose.
- (2) The agency must use only the parts of the personal information that are directly relevant to fulfilling the particular purpose.

#### **4.2.2 Third Party Handling of CCTV Records**

Agencies conduct business and deliver services in a variety of ways, including by outsourcing and through partnerships. For example, monitoring of surveillance systems may have been outsourced to a commercial provider. If appropriate action is not taken in these situations public records may be at risk of unlawful disposal, undermining accountability and efficiency.

In situations using outsourcing, including shared service arrangements, agencies should refer to Queensland State Archives' *Custody and Ownership Guideline*. A public authority can be responsible for records that are not in its physical custody or for records that have been created by another entity. In any outsourcing of government services (including those related to CCTV), the responsible public authority must make adequate arrangements for the safekeeping, proper preservation and return of records not in its physical custody.

The QSA *Custody and Ownership Guideline* addresses the issue of a public authority's responsibility for public records when those records may not be in its possession, ensuring that they are fulfilling their responsibilities for managing public records in accordance with the *Public Records Act 2002*.<sup>41</sup>

The provision of CCTV footage and associated recordkeeping requirements of the footage must be clearly communicated to partners and/or providers and formalised in written agreements (e.g. Operating Level Agreements/Memorandum of Understanding) between the agency and the third party. These agreements should address the intended and permissible use of imagery, and information security and privacy controls and accountabilities. Any written agreements must detail specific requirements relating to the management of public records during the period of the agreement.

Where a third party is used to capture CCTV records, the 'point of transfer' at which the responsibility for handling of third party images is transferred to the public authority (i.e.

<sup>40</sup> [www.legislation.qld.gov.au/LEGISLTN/CURRENT/I/InfoPrivA09.pdf](http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/I/InfoPrivA09.pdf)

<sup>41</sup> [www.archives.qld.gov.au/downloads/Guideline\\_Custody\\_and\\_Ownership.pdf](http://www.archives.qld.gov.au/downloads/Guideline_Custody_and_Ownership.pdf)

Primary, Original or Working Copy) must be established. The 'point of transfer' will depend on the nature of the CCTV records being transferred, the recording format and equipment used by the third party. Both third parties and public authorities have responsibilities to ensure continuity of CCTV audit trails are maintained up to, and following the 'point of transfer'.

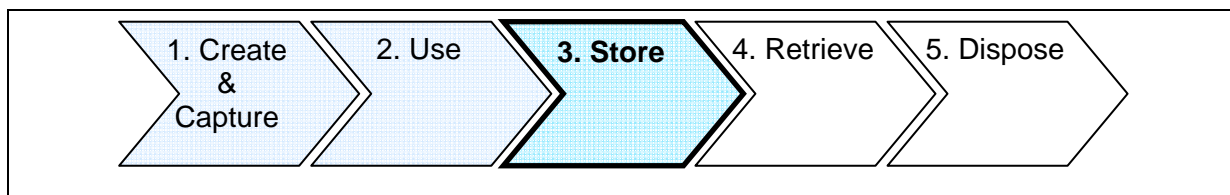
Additionally, system configurations need to provide adequate security and privacy safeguards. Remote connections through the CCTV network to workstations *outside* controlled areas should be secured by firewall or similar at both ends (the CCTV network and the remote site). Cameras connected over wireless links should transmit, and be controlled by, encrypted data to prevent interceptions; for example, secured either over the viewing application, or in the networking on the data stream itself.

Methods for exchanging CCTV records between public authorities and/or third parties must be compliant with legal and legislative requirements, and consistent with the *Queensland Government Authentication Framework*<sup>42</sup>, and the classification schemes and controls defined in the *Queensland Government Information Security Classification Framework*<sup>43</sup>.

<b>Use – Key Recordkeeping Considerations</b>	
Use of surveillance records is controlled and auditable through the maintenance of logs and registers.	<input type="checkbox"/>
A maintenance schedule has been specified to ensure the ongoing operation of CCTV equipment.	<input type="checkbox"/>
Use of personal information is in accordance with Information Privacy Principles 8 and 9: CCTV records are accurate, up-to-date, and complete.	<input type="checkbox"/>
Third party handling responsibilities for CCTV records are documented in accordance with <i>Custody and Ownership Guideline</i> , and security controls implemented which are consistent with the <i>Queensland Government Authentication Framework</i> and the <i>Queensland Government Information Security Classification Framework</i> .	<input type="checkbox"/>

<sup>42</sup><http://www.qgcio.qld.gov.au/SiteCollectionDocuments/Architecture%20and%20Standards/QGAF%201.0.1.doc>

<sup>43</sup><http://www.qgcio.qld.gov.au/SiteCollectionDocuments/Architecture%20and%20Standards/QGISCF%20v1.0.1.doc>



## 4.3 Storage

### 4.3.1 Security of Storage

Principle 5 of *Information Standard 40* states that all systems that are used to create and maintain records must work reliably and be secure to ensure that records are credible and authoritative, regardless of format. Public records should additionally be secured in accordance with *Information Standard 18: Information Security (IS18)*.<sup>44</sup> Public authorities required to comply with IS18 must also look at the *Queensland Government Authentication Framework*<sup>45</sup> (which guides agencies in the determination of authentication requirements for services), and the *Queensland Government Information Security Classification Framework*<sup>46</sup> (which provides a standard process to allow agencies to evaluate their information assets and determine the appropriate level of security classification that should be applied). Public authorities not bound by the requirements of IS18 should refer to the frameworks as a useful source of advice. At a minimum, public authorities must implement recordkeeping systems which are secure from unauthorised access, damage and misuse. The classification and protective control applied to CCTV records must be commensurate with their value, importance and sensitivity.

It is essential that the integrity of the agency's CCTV records be maintained through these protocols. Particular protocols should be developed for recorded material requested by the police and/or which contains a known incident. Controlled access to the secured media should be strictly maintained (see section 4.2.2 for further details relating to third party handling of CCTV records).

The Australian Customs website *Managing Risks to CCTV Data and Systems* outlines several ways in which security of CCTV footage can be compromised.<sup>47</sup> These range from intentional physical security risks, such as tampering, to natural disasters and network failures. The site recommends implementing information management policies surrounding the collection and storage of CCTV footage, investing in offsite backup systems and redundant arrays (RAID), and improving physical control measures such as resilient camera housings to reduce risk.

### 4.3.2 Encryption

Encryption techniques may be used to increase the security of electronic documents during transmission, ensuring the confidentiality of the record and limiting access to its content.

<sup>44</sup> [www.ggcio.qld.gov.au/ggcio/architectureandstandards/informationstandards/current/Pages/Information%20Security.aspx](http://www.ggcio.qld.gov.au/ggcio/architectureandstandards/informationstandards/current/Pages/Information%20Security.aspx)

<sup>45</sup> <http://www.ggcio.qld.gov.au/SiteCollectionDocuments/Architecture%20and%20Standards/QGAF%201.0.1.doc>

<sup>46</sup> <http://www.ggcio.qld.gov.au/SiteCollectionDocuments/Architecture%20and%20Standards/QGISCF%20v1.0.1.doc>

<sup>47</sup> [www.customs.gov.au/site/page5990.asp](http://www.customs.gov.au/site/page5990.asp)

Where an agency transmits an encrypted file, documentation should be maintained to establish the reliability and integrity of the encryption technologies used. The system should show that files can be accurately decrypted without error.

Loss of the ability to decrypt an encrypted record may equate to destruction of the record. For storage and preservation purposes, it is critical that the record be stored as an unencrypted file. Encrypted files may become inaccessible over time if the private key required for decryption is lost. There should also be a policy in place for managing incidents in which an encryption key has been lost or the security of an encryption key has been compromised.

It is therefore recommended that surveillance records be decrypted and stored in a recordkeeping system with suitable security controls. Where encryption is applied to files stored on a secure server, relevant encryption keys will need to be managed over time to ensure that records remain accessible throughout their lifecycle. As with physical keys, encryption keys should be available only to personnel with appropriate authorisations. These measures will support the security of surveillance records.

Additionally, it is important to store the CCTV record's metadata, audit logs and associated information required to establish the evidentiary audit trail and to provide contextual information in a secure manner.

#### **4.3.3 Preservation**

To maximise the longevity of storage media, the UK Home Office's *Digital Imaging Procedure* notes that disks and drives should be stored in a clean, dry environment, and protected from strong magnetic fields, UV exposure, and chemical contamination.<sup>48</sup> Media should be appropriately handled, with all attempts made not to scratch CD/DVDs.

The retention of records in electronic formats may involve the migration to new file formats, to ensure these records remain accessible over time.

Information Privacy Principle 4 of the *Information Privacy Act 2009* relates to the storage and security of personal information.<sup>49</sup> Where personal information is contained within stored surveillance records, agencies must comply with this Information Privacy Principle and ensure that the personal information is adequately preserved and safeguarded for the life of the record.

Figure 8 on the following page and Table 3 on page 40 summarise the requirements of Information Privacy Principle 4.

The *Information Privacy Act 2009 Guidelines* released by the Office of the Information Commissioner, Queensland, provide further guidance on the storage and security of personal information.<sup>50</sup>

---

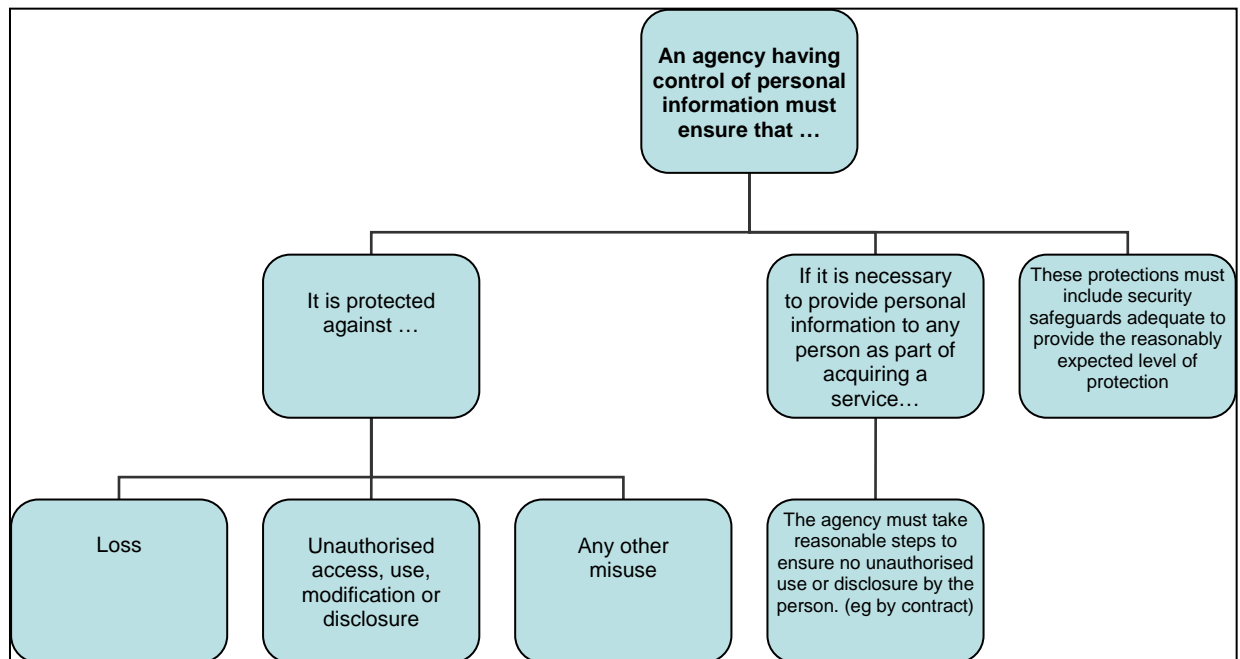
<sup>48</sup> [http://tna.europarchive.org/20100413151426/http://scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/DIP\\_2.1\\_16-Apr-08\\_v2.3\\_\(Web\)2835.pdf?view=Binary](http://tna.europarchive.org/20100413151426/http://scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/DIP_2.1_16-Apr-08_v2.3_(Web)2835.pdf?view=Binary)

<sup>49</sup> [www.legislation.qld.gov.au/LEGISLTN/CURRENT/I/InfoPrivA09.pdf](http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/I/InfoPrivA09.pdf)

<sup>50</sup> [www.oic.qld.gov.au/files/IPAGuidelines/Privacy%20Guideline%20%28complete%29%20-%2030-06-09.pdf](http://www.oic.qld.gov.au/files/IPAGuidelines/Privacy%20Guideline%20%28complete%29%20-%2030-06-09.pdf)

**Figure 8: Summary of Information Privacy Principle 4 – Storage and Security of Documents**

Image used with the permission of the Office of the Information Commissioner, Queensland



**Table 3: Security Considerations – Storage and Security of Documents**

Used with the permission of the Office of the Information Commissioner, Queensland

The safeguards must apply equally to personal information held in paper form, electronically, as film, photographs, audio or video recording or any other media.

Techniques for securing personal information include securing physical access to personal information, using audit logs to detect security breaches, securing/encrypting portable electronic storage, securing data during and after transmission.

The primary safeguard in protecting documents containing personal information is to limit access only to those who need to access it in order to do their jobs.

The security measures that an agency takes to protect documents containing personal information should be proportionate and appropriate to the possible risk of a security breach and the level of harm that could result from a breach.

Practices that may lead to breaches of security include:

- leaving files containing personal information unattended at a public counter
- not disposing of records in a secure manner
- inadequate controls regarding which staff can access information; for example, inadequate user ID and password control on a database
- storing sensitive data on a laptop computer that is taken 'off-site' and not stored securely
- emailing confidential information
- neglecting to include audit capabilities or audit trails in databases.

Queensland Government *Information Standard 18, Information Security (IS18)* requires all departments and agencies to:

- establish an appropriate information security culture within the department
- satisfy the 10 mandatory information security principles set out in IS18
- implement security measures beyond the minimum requirements commensurate with the information's value, business significance and sensitivity
- adhere to all legal and legislative requirements.



#### **4.3.4 Recorded Materials Register**

Section 8.4 of Part 1 of the Australian CCTV Standard, AS4806.1–2006 states that agencies should maintain a register documenting the life of the CCTV system's recorded removable media from the time of purchase until destruction. The recorded materials register should include details of any presentation of media at court as an exhibit. As such, the register will provide a key component of the CCTV system's audit trail. It should also enable evaluation of the CCTV installation, by documenting how recordings have been used, and, in particular, statistics of what has been requested for court proceedings.

The Australian CCTV Standard states that the recorded materials register should include the following elements:

- Unique storage media reference number
- Storage media type and batch number
- Details of purchase: from whom purchased and delivery date
- Time/date/person placing storage media in store
- Time/date/person removing from secure storage for use
- Time/date/person returning storage media to secure storage after use
- Remarks column to cover additional points (e.g. erase/destroy/handed over to police/removed from recording machine)
- Time/date/person responsible for any subsequent removal of the storage media
- Time and date of delivery to the police, identifying the police officer concerned
- Time/date/person responsible for erasure and/or destruction.

This information may already exist within logs, metadata and other recorded documentation within an agency's recordkeeping system, rather than in the form of a discrete register.

#### **4.3.5 Storage Media**

CCTV systems must be equipped with appropriate export and archiving facilities for retention of CCTV records in compliance with *Information Standard 31: Retention and Disposal of Public Records*. Original Images must be copied from the recording drive to a storage medium, as detailed below. Where possible, it is recommended that agencies avoid storing records in a proprietary, non-standard format. Technology that is only available from one vendor is at a high risk of becoming orphan technology if the vendor makes a commercial decision to cease support (or simply goes out of business). The inability to obtain readers or media can easily cause the effective loss of the records. In the instance where exported video has a proprietary, non-standard format, the equipment manufacturer must provide additional software to make the images playable on standard equipment.

When assessing storage options, considerations should be made to the quality, durability, permanence, and reliability of media. Where the length of the required minimum retention period warrants, archive-quality materials should be chosen to safeguard the longevity of the records.

Digital storage media options include the following:

- Magnetic tape
- WORM (Write-Once, Read-Many) media

- Re-useable, removable, non-tape media, such as memory cards
- Network servers with disk-based storage.

#### **4.3.6 WORM Media versus Secure Servers**

Many organisations have determined that Write-Once Read-Many (WORM) media represents the most secure and cost effective long-term storage solution for CCTV records. WORM technologies are currently found in the form of optical discs such as CDs and DVDs, magnetic disks, and tape. Given that WORM media is inherently non-editable, it brings the protection that data cannot be altered, over-written or corrupted. The one-time nature of WORM media means that it is often admitted as evidence in court.

Several issues exist, however, in relation to the management of WORM media. A CD, for example, is more easily able to be destroyed, damaged, or removed from its environment, being easily transportable, than records stored on servers where audit trails are automatically generated. Additionally, once it has been noticed that the media has failed it is often too late to retrieve required data. In terms of preservation, it is now thought that CD/DVDs may be at risk of end-of-life and obsolescence within 10 to 20 years. The drives required to read media can also become obsolete before the actual media itself reaches expiry. Therefore the media will need to be refreshed regularly to avoid obsolescence. To be able to reliably locate records stored on external media it is important to retain appropriate indexes of records through full and accurate metadata.

Appropriate recordkeeping practices should be developed to ensure that the media bearing CCTV images and associated metadata does not degrade and that the media can be replayed in the future. Use of rewritable media such as CD-RW/DVD-RW is not recommended, as it has a much shorter life expectancy compared to WORM media, and is susceptible to loss or alteration of content as a result of the rewriting.

Regardless of media used, regular auditing should be undertaken to ensure early detection of media decay. To achieve optimum outcomes, it is recommended that the National Archives of Australia's handling guidelines for optical disks be followed.<sup>51</sup>

The storage capacity of media should also be taken into account. Where it becomes necessary to store records of incidents for long-term operational requirements, it may be impractical to transfer the entirety of the records to WORM media, as it may take a considerable time to copy, and require many discs. Where single images and short video excerpts are required, CD/DVDs will often be fit for purpose.

In contrast, a secure server with attached disk storage offers a central, searchable, metadata-rich repository from which authorised persons can stream CCTV video and take frame grabs. Secure servers have the advantage that data can be migrated automatically and with no loss within a RAID system (Redundant Array of Independent Disks).

Systems which allow the protection of identified sequences from being overwritten offer additional protection for the security of public records. This includes disk-based systems which provide a form of WORM functionality. Additionally, RAID storage allows images to be distributed across multiple hard disk drives, to protect against the failure of a single drive. Disk-based RAID systems also regularly conduct integrity checking and can perform repairs from the Parity Disk where data integrity is compromised. If the drive is not repairable it is

---

<sup>51</sup> [http://www.naa.gov.au/images/optical%20discs\\_tcm2-5470.pdf](http://www.naa.gov.au/images/optical%20discs_tcm2-5470.pdf)

replaced from a 'hot spare'<sup>52</sup> pool in the array with no data loss. This feature is present in standard RAID arrays and in WORM disk-based storage. In contrast, the WORM devices outlined above have minimal/no data recovery capability if they are damaged.

The SMANZFL *Australasian Guidelines for Digital Imaging Processes* recommend: 'Generally CD-R, DVD-R, digital tapes, etc., are designed for short-to-medium term storage periods. To ensure the integrity of the data the files need to be transferred to new media regularly, or transferred to professionally managed data management archive systems.' (p. 43).

#### **4.3.7 Re-Useable Media**

Removable media should be indelibly marked with a unique reference number, ideally on the medium itself. As described in the *SWGIT Best Practices for Forensic Video Analysis*, notations should be made in the clear inner ring of the CD/DVD as no data is recorded in that area.<sup>53</sup> Media should be stored according to the manufacturer's specifications. Serial numbers should be documented, and media should be stored in date order where appropriate.

As is well recognised, it is important that users:

- Do not scratch the label side of the disk
- Do not use a pen, pencil, or other sharp writing instrument to write on the disk. If a disk must be labelled, a non-solvent based felt-tip permanent marker designed for optical media is recommended
- Do not use inkjet printing on disks intended for long term archiving<sup>54</sup>
- Do not use adhesive labels (or try to peel off or reposition already applied labels e.g. non-acidic labels)<sup>55</sup>

The marking of re-useable media is additionally noted in the metadata section of this Guideline.

#### **4.3.8 Storage Capacity**

CCTV image quality should be determined by operational and evidentiary requirements, rather than to minimise storage capacity.

The storage requirements of a specific CCTV system should be determined during the design phase to make sure that the system writes to media of sufficient size.

The Australian Customs CCTV Advisory Service provides the following step-by-step guide to assist the end user when determining storage capacity:

- Determine the numbers of cameras
- Determine the frame rate (frames per second) at which each camera will record

---

<sup>52</sup> A hot spare is a slice (not a volume) that is functional and available, but not in use. A hot spare is reserved, meaning that it stands ready to substitute for a failed slice in a submirror or RAID 5 volume. A hot spare pool is a collection of slices (hot spares).

<sup>53</sup> [www.theiai.org/guidelines/swgit/guidelines/section\\_7\\_v1-0.pdf](http://www.theiai.org/guidelines/swgit/guidelines/section_7_v1-0.pdf)

<sup>54</sup> ISO 18921:2008

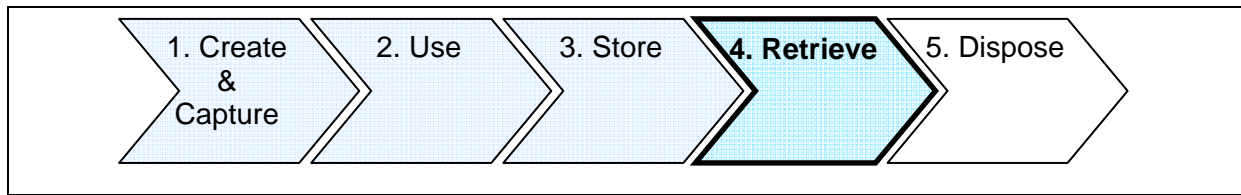
<sup>55</sup> [http://www.naa.gov.au/images/optical%20discs\\_tcm2-5470.pdf](http://www.naa.gov.au/images/optical%20discs_tcm2-5470.pdf)

- Determine the average size (in kilobytes) each compressed frame of video will take up on the hard disk after the compression ratio has been applied
- Approximate the activity (in percentage) time each camera will be recording at the above frame rate, and
- Determine the duration (in days) that video from each camera will be retained.<sup>56</sup>

An equation to determine the CCTV system's required storage capacity is located in Appendix I.

<b>Storage – Key Recordkeeping Considerations</b>	
A reliable system and documented processes are in place to ensure CCTV records remain secure from unauthorised access, damage and misuse, in accordance with <i>Information Standard 18: Information Security</i> .	<input type="checkbox"/>
Documented processes exist for encrypting and decrypting CCTV records to ensure their ongoing accessibility and security in transit.	<input type="checkbox"/>
Media containing stored CCTV records are appropriately handled, and are stored in a clean, dry area, and are protected from strong magnetic fields, UV exposure, and chemical contamination.	<input type="checkbox"/>
Storage of surveillance records is in accordance with Information Privacy Principle 4.	<input type="checkbox"/>
A recorded materials register is maintained to keep track of removable media if all relevant metadata is not captured in a recordkeeping system.	<input type="checkbox"/>
Media decay is monitored, and migration to new file formats over time to ensure accessibility is considered.	<input type="checkbox"/>
Storage media is selected and implemented to ensure ongoing availability and longevity of CCTV records, taking into consideration retention periods; protection requirements and storage capacity requirements.	<input type="checkbox"/>

<sup>56</sup> [www.customs.gov.au/site/page5974.asp](http://www.customs.gov.au/site/page5974.asp)



## **4.4 Retrieval**

### **4.4.1 Media Retrieval**

Where possible, a set time should be established to load and unload (or backup and download) storage media from the CCTV recorder. The retrieval of media should be conducted at the most operationally convenient time, with regard to the least likelihood of incidents, as stated in section 8.4.3 of Part 1 of the Australian CCTV Standard, AS4806.1–2006.

Where media is released for evidential purposes, replacement storage media should be inserted immediately, and notes made to this effect in the recorded materials register.

A CCTV download register should be maintained and kept securely by the operator. This register should note all recordings of which copies have been made, specifying:

- Details of the recording copied: date, times, cameras, and the copy format
- The reason the recording was copied
- The name and signature of the person making the copy
- Date and time the copy was made
- The recipient of the recording
- Date and time of receipt.

### **4.4.2 Native File Formats**

Section 4.1.6 *Evidential Audit Trail: Primary, Original, and Working Images* described the distinction between Primary, Original, and Working Images. To preserve the integrity of the CCTV record, the Primary Image should be exported in its native file format. No additional compression should be applied during this process.<sup>57</sup> This allows the Original Image to become the master, being a bit-for-bit identical copy of the Primary Image.

In the case where proprietary hardware or software is required for video replay, and where this may not provide the required functionality to enable editing or processing, a format conversion will be required. This process needs to be audited to ensure that it has been carried out soundly.

---

<sup>57</sup> UK Home Office Scientific Development Branch (2008) *Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems* (66/08) at [http://tna.europarchive.org/20100413151426/http://scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/66-08\\_Retrieval\\_of\\_Video\\_Ev12835.pdf?view=Binary](http://tna.europarchive.org/20100413151426/http://scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/66-08_Retrieval_of_Video_Ev12835.pdf?view=Binary)

#### 4.4.3 Disclosure of Personal Information for the Protection of an Individual or the Public

Use and disclosure of personal information is governed by the *Information Privacy Act 2009* through Information Privacy Principles 10 and 11 relating to limits on use of personal information and limits on disclosure. When an agency intends to use or disclose surveillance records containing personal information, it must comply with these Information Privacy Principles. The *Information Privacy Act 2009 Guidelines* released by the Office of the Information Commissioner provide further guidance on the disclosure of personal information.<sup>58</sup>

Figure 9 summarises the requirements of Information Privacy Principles 10 and 11 associated with the protection of an individual or the public when using or disclosing personal information.

**Figure 9: Summary of Information Privacy Principles 10(1)(b) and 11(1)(c)  
– Use or Disclosure Necessary for the Protection of an Individual or the Public**

Image used with the permission of the Office of the Information Commissioner, Queensland



<sup>58</sup> [www.oic.qld.gov.au/files/IPAGuidelines/Privacy%20Guideline%20%28complete%29%20-%2030-06-09.pdf](http://www.oic.qld.gov.au/files/IPAGuidelines/Privacy%20Guideline%20%28complete%29%20-%2030-06-09.pdf)

#### 4.4.4 Disclosure of Personal Information for Law Enforcement

It may become necessary for agencies to disclose visual surveillance records to the Queensland Police or other law enforcement bodies in the course of their business or, if they are law enforcement bodies, to use visual surveillance records for law enforcement purposes.

Use of personal information in this regard is covered by section 1(d) of Information Privacy Principle 10 which requires the agency to be satisfied on reasonable grounds that the use will contribute to the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of law imposing penalties or sanctions, or seriously improper conduct. Section 1(e) of Information Privacy Principle 11 deals with disclosure to law enforcement bodies to assist with their law enforcement functions. If an agency discloses personal information under IPP 10(1)(d) or IPP 11 (1)(e), the agency must include with the document a note of the disclosure.

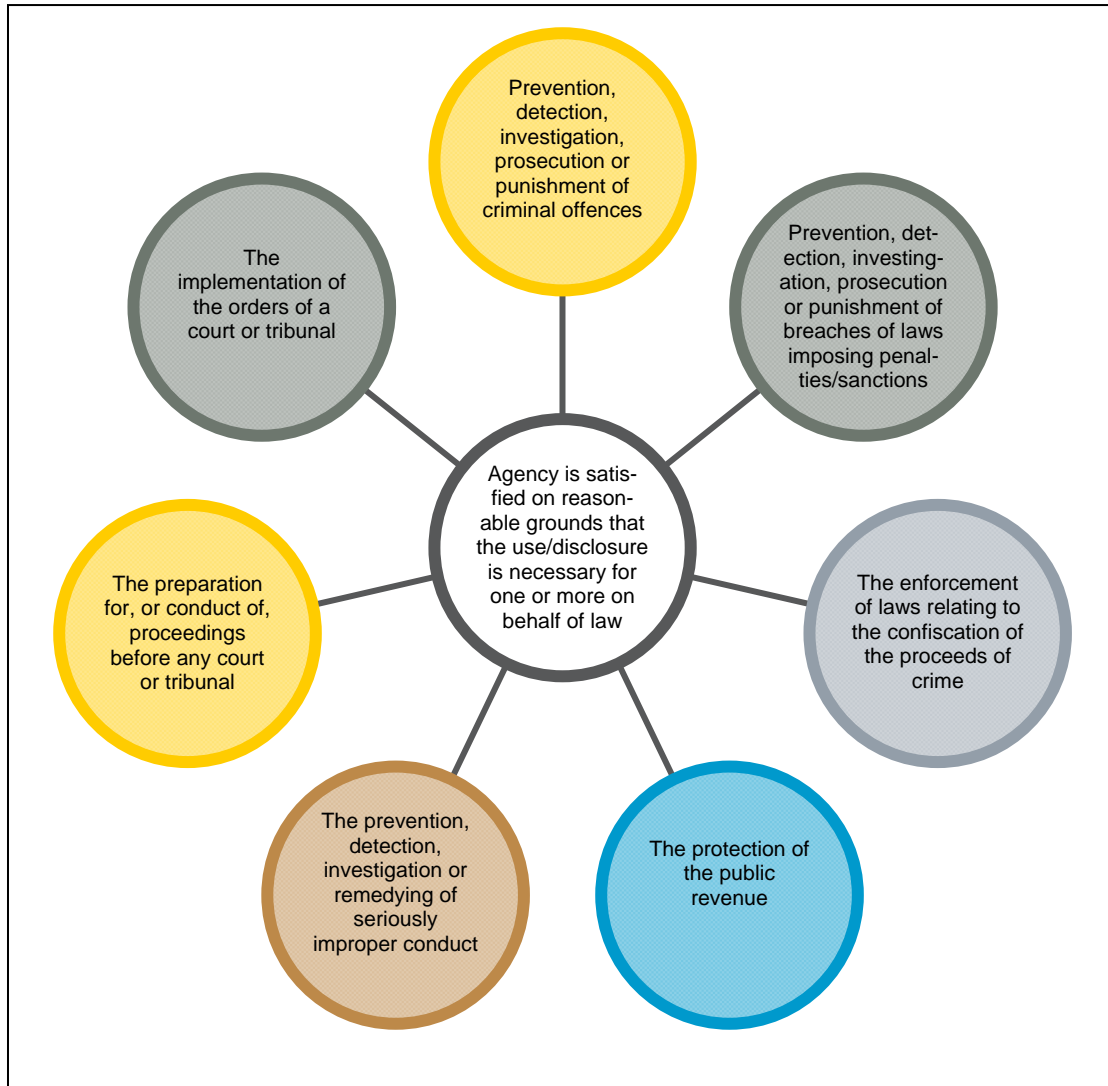
Figure 10 on the following page summarises the requirements of Information Privacy Principles 10 and 11 associated with the use and disclosure of personal information for law enforcement.

Under the *Information Privacy Act 2009*, **law enforcement agency** means—

- a) the Queensland Police Service under the *Police Service Administration Act 1990*; or
- b) the Crime and Misconduct Commission under the *Crime and Misconduct Act 2001*; or
- c) the community safety department; or
- d) any other agency, to the extent it has responsibility for—
  - i. the performance of functions or activities directed to the prevention, detection, investigation, prosecution or punishment of offences and other breaches of laws for which penalties or sanctions may be imposed; or
  - ii. the management of property seized or restrained under a law relating to the confiscation of the proceeds of crime; or
  - iii. the enforcement of a law, or of an order made under a law, relating to the confiscation of the proceeds of crime; or
  - iv. the execution or implementation of an order or decision made by a court.

**Figure 10: Summary of Information Privacy Principles 10(1)(d) and 11(1)(e)  
– Use or Disclosure Necessary for Law Enforcement Activities/Action**

Image used with the permission of the Office of the Information Commissioner, Queensland

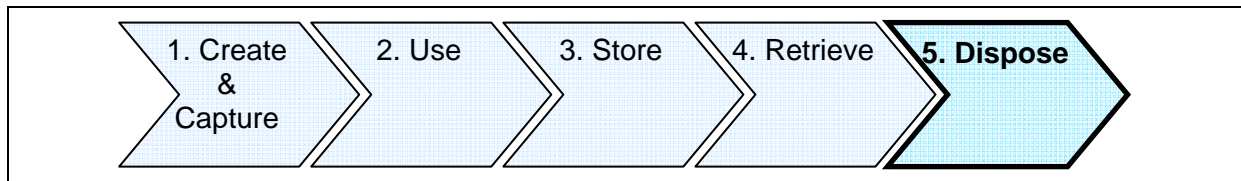


**4.4.5 Disclosure of Personal Information for Other Purposes and to Other Entities**

Information disclosed to further third parties for purposes other than those listed above must be authorised under another law, done with the express or implied agreement of the individual or where the individual was made aware of the disclosure through advice/notification to this extent. Refer to section 4.1.2 *Collection Notices* to review the requirement that individuals be informed in situations where they may be recorded.

<b>Retrieval – Key Recordkeeping Considerations</b>	
A CCTV download register is maintained noting the details of records retrieved.	<input type="checkbox"/>
Where required, format conversion processes are audited to ensure that the process has been carried out soundly.	<input type="checkbox"/>
Disclosure of personal information contained within the CCTV records is in accordance with Information Privacy Principles 10 and 11).	<input type="checkbox"/>





## 4.5 Disposal

Under the *Public Records Act 2002*, disposal of a record includes:

- (a) destroying or damaging the record, or part of it; or
- (b) abandoning, transferring, donating, giving away or selling the record, or part of it.<sup>59</sup>

Note that, in the case of electronic records including digital CCTV records, disposal may also include deleting a record or failing to take the necessary steps to ensure a record's readability/useability over time.

Under section 13 of the *Public Records Act 2002*, the disposal of public records must be authorised by the State Archivist. Such authorisation is generally given in the form of a Retention and Disposal Schedule.

### 4.5.1 Retention and Disposal

*Information Standard 31: Retention and Disposal of Public Records* requires Queensland public authorities to ensure that records are appraised and retained according to accountability, legal, administrative, financial, research and community requirements and expectations.<sup>60</sup> Records of continuing value need to be identified and retained in a useable form for a minimum period as specified in an approved Retention and Disposal Schedule.

The two mandatory principles of *Information Standard 31* are:

1. Public authorities must ensure public records are retained for as long as they are required.
2. The disposal of public records must be authorised by the State Archivist.

Surveillance records associated with the security of premises can be disposed of<sup>61</sup> in accordance with the *General Retention and Disposal Schedule for Administrative Records* (GRDS) which authorises the disposal of common administrative records for all Queensland public authorities.<sup>62</sup>

<sup>59</sup> [www.legislation.qld.gov.au/LEGISLTN/CURRENT/P/PublicRecA02.pdf](http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/P/PublicRecA02.pdf)

<sup>60</sup> [www.qgcio.qld.gov.au/SiteCollectionDocuments/Architecture%20and%20Standards/Information%20Standards/Current/is31\\_print.pdf](http://www.qgcio.qld.gov.au/SiteCollectionDocuments/Architecture%20and%20Standards/Information%20Standards/Current/is31_print.pdf)

<sup>61</sup> The Queensland Government Information Security Classification Framework (QGISCF) details appropriate methods for destroying records beyond any possible reconstruction and provides guidance on media which cannot be sanitised and should be destroyed if they contain or may have contained classified information.  
[www.qgcio.qld.gov.au/SiteCollectionDocuments/Architecture%20and%20Standards/QGISCF%20v1.0.1.doc](http://www.qgcio.qld.gov.au/SiteCollectionDocuments/Architecture%20and%20Standards/QGISCF%20v1.0.1.doc)

<sup>62</sup> [www.archives.qld.gov.au/downloads/GeneralDisposalSchedule.pdf](http://www.archives.qld.gov.au/downloads/GeneralDisposalSchedule.pdf)

Agencies using the GRDS to dispose of surveillance records that are not required for investigations will need to establish business processes to determine when the disposal trigger of 'no further administrative use' can be applied.

If the use of surveillance relates to the core business activities of the public authority, these records should be included in a sector or agency-specific Retention and Disposal Schedule approved by the State Archivist. The agency's legislative and operational requirements will be reflected in suitable retention periods for surveillance records.

For example, the COAG *CCTV Code of Practice*, a voluntary code of practice for CCTV recordings of the Mass Passenger Transport Sector for Counter-Terrorism described in Appendix D, adopts a risk-based approach (through security priorities) to determine the minimum recommended retention periods for CCTV footage<sup>63</sup>. Table 4 illustrates the COAG *CCTV Code of Practice* recommended minimum retention period associated with each security priority.

**Table 4: Recording Storage Recommendations – COAG CCTV Code of Practice<sup>64</sup>**

Security priority	Recommended minimum recording storage
Priority 1	not less than 30 days
Priority 2	not less than 15 days, but 30 days preferred
Priority 3	not less than 7 days, but 30 days preferred

When making decisions on recommended minimum retention periods, local security issues and circumstances must be taken into account, together with priorities established by Government as well as those of the individual agency. Relevant factors used to determine minimum retention periods may include consideration of how long after an incident occurs is notification typically received. Where, for example, incidents are known immediately in a control room, and the records immediately retrieved, a shorter retention period would be suitable. Conversely, where incidents may not be reported or noticed for days/weeks, or it may take a significant time for the record to be retrieved from a recorder (e.g. the recorder is mounted to a vehicle), the retention period needs to be longer. Once a suitable retention period has been established, it requires authorisation in a Retention and Disposal Schedule approved by the State Archivist.

Recordings required for evidentiary purposes which form part of the records of an investigation or criminal or court proceedings should be managed and disposed of in accordance with the retention requirements of the investigation or court records. This includes both Original and Working Images, associated metadata and logs.

Agencies requiring further advice on the retention and disposal of records should contact Queensland State Archives' Agency Services unit.

#### **4.5.2 Documenting Disposal of Public Records**

Disposal of visual surveillance records which are public records (Original Images and Working Images) must be in accordance with the principles of *Information Standard 31: Retention and Disposal of Public Records*. Public authorities must document the disposal of

<sup>63</sup> [www.coag.gov.au/coag\\_meeting\\_outcomes/2006-07-14/docs/cctv\\_code\\_practice.rtf](http://www.coag.gov.au/coag_meeting_outcomes/2006-07-14/docs/cctv_code_practice.rtf)  
<sup>64</sup> [www.coag.gov.au/coag\\_meeting\\_outcomes/2006-07-14/docs/cctv\\_code\\_practice.rtf](http://www.coag.gov.au/coag_meeting_outcomes/2006-07-14/docs/cctv_code_practice.rtf)

public records. This documentation must be retained permanently in accordance with the requirements of the GRDS. Automatic disposal of Primary Images (via overwriting) must be in accordance with documented business processes established to determine when the disposal trigger of 'no further administrative use' can be applied.

Appendix D of the *Queensland Recordkeeping Metadata Standard and Guideline* details the minimum metadata which must be retained after the destruction of a public record. At a minimum, this includes the following:

- Unique record identifier
- Record title
- Record creation date/time
- Queensland Disposal Authority Number (QDAN), version number and reference number under which the records are disposed
- Disposal sentence (e.g. Retain for 7 years after last action)
- Date of disposal
- Authorising officer
- The manner of destruction of the records, and
- Who destroyed the records.<sup>65</sup>

This may be kept as a disposal log by the CCTV operator.

<b>Disposal - Key Recordkeeping Considerations</b>	
CCTV records are retained appropriately and disposed of lawfully, in accordance with <i>Information Standard 31: Retention and Disposal of Public Records</i> .	<input type="checkbox"/>
CCTV records are retained for at least the specified minimum retention period, in accordance with the <i>General Retention and Disposal Schedule for Administrative Records</i> or relevant sector- or agency-specific Retention and Disposal Schedule.	<input type="checkbox"/>
Documented business processes are in place which establish when the disposal trigger of 'no further administrative use' can be applied.	<input type="checkbox"/>
Disposal of public records is conducted appropriately and documentation regarding disposal of public records is captured and retained permanently.	<input type="checkbox"/>

<sup>65</sup> [www.archives.qld.gov.au/downloads/QRKMS.pdf](http://www.archives.qld.gov.au/downloads/QRKMS.pdf)

## Appendix A: CCTV Checklist

The following checklist is a summary of the recordkeeping considerations documented throughout this Guideline, and is designed to assist public authorities to implement and support CCTV systems and management frameworks which generate full and accurate records (i.e. records which are adequate, complete, meaningful, authentic, inviolate, accessible, and useable). Agencies may wish to use this checklist as a starting document to modify and expand in line with the operational requirements of the agency.

<b>General</b>	
<p>The CCTV organisational framework (see section 3) has been followed to:</p> <ul style="list-style-type: none"> <li>• Define the surveillance function</li> <li>• Identify operational issues</li> <li>• Specify system requirements</li> <li>• Establish a management framework.</li> </ul>	<input type="checkbox"/>
<b>Create &amp; Capture</b>	
The agency's surveillance operation is lawful and directly related to the agency's function (see section 4.1.1).	<input type="checkbox"/>
The agency's collection of personal information is in accordance with Information Privacy Principles 1 – 3 (see section 4.1.1).	<input type="checkbox"/>
CCTV collection notices are prominently displayed, detailing the purpose of the surveillance, the authority under which the records are created, and parties to whom the surveillance record may be given (see section 4.1.2).	<input type="checkbox"/>
The CCTV system has been installed and configured according to the manufacturer's specification and agency's operational requirements (see sections 4.1.3 – 4.1.12).	<input type="checkbox"/>
CCTV images produced by the system are fit for purpose – to observe, detect, recognise, or identify people or objects as appropriate (see section 4.1.3).	<input type="checkbox"/>
CCTV records captured into and managed by recordkeeping systems are accessible and meaningful, and are maintained with appropriate controls to ensure the attributes of full and accurate records are retained (see section 4.1.5).	<input type="checkbox"/>
<p>Original Images are preserved as exact copies of the Primary Image, with appropriate audit trails being maintained (see section 4.1.6).</p> <p>Working Images are created where appropriate (see section 4.1.6).</p>	<input type="checkbox"/>
Mandatory recordkeeping metadata <sup>66</sup> associated with the CCTV records is captured into an identified recordkeeping system to ensure ongoing accessibility (see section 4.1.12).	<input type="checkbox"/>

<sup>66</sup> [www.archives.qld.gov.au/downloads/QRKMS.pdf](http://www.archives.qld.gov.au/downloads/QRKMS.pdf)

<b>Use</b>	
Staff are appropriately trained and behave in accordance with identified roles (see section 3.2).	<input type="checkbox"/>
Use of surveillance records is controlled and auditable through the maintenance of logs and registers (see section 4.2).	<input type="checkbox"/>
A maintenance schedule has been specified to ensure the ongoing operation of CCTV equipment (see sections 3.4 and 4.2).	<input type="checkbox"/>
Use of personal information is in accordance with Information Privacy Principles 8 and 9: CCTV records are accurate, up-to-date, and complete (see section 4.2.1).	<input type="checkbox"/>
Third party handling responsibilities for CCTV records are documented in accordance with Custody and Ownership Guideline, and security controls implemented which are consistent with the Queensland Government Authentication Framework and the Queensland Government Information Security Classification Framework (see sections 4.2.2 and 4.3.1).	<input type="checkbox"/>
<b>Store</b>	
A reliable system and documented processes are in place to ensure CCTV records remain secure from unauthorised access, damage and misuse, in accordance with <i>Information Standard 18: Information Security</i> (see section 4.3.1).	<input type="checkbox"/>
Documented processes exist for encrypting and decrypting CCTV records to ensure their ongoing accessibility and security in transit (see section 4.3.2).	<input type="checkbox"/>
CCTV records are stored in a clean, dry area, and are protected from strong magnetic fields (see section 4.3.3).	<input type="checkbox"/>
Media containing stored CCTV records are appropriately handled, and are stored in a clean, dry area, and are protected from strong magnetic fields, UV exposure, and chemical contamination (see section 4.3.3).	<input type="checkbox"/>
Storage of surveillance records is in accordance with Information Privacy Principle 4 (see section 4.3.3).	<input type="checkbox"/>
A recorded materials register is maintained to keep track of removable media if all relevant metadata is not captured in a recordkeeping system (see section 4.3.4).	<input type="checkbox"/>
Media decay is monitored, and migration to new file formats over time to ensure accessibility is considered (see section 4.3.6).	<input type="checkbox"/>
Storage media is selected and implemented to ensure ongoing availability and longevity of CCTV records, taking into consideration retention periods; protection requirements and storage capacity requirements (see sections 4.3.5 to 4.3.8).	<input type="checkbox"/>

<b>Retrieve</b>	
A CCTV download register is maintained noting the details of records retrieved (see section 4.4.1).	<input type="checkbox"/>
Where required, format conversion processes are audited to ensure that the process has been carried out soundly (see section 4.4.2).	<input type="checkbox"/>
Disclosure of personal information contained within the CCTV records is in accordance with Information Privacy Principles 10 and 11 (see sections 4.4.3 and 4.4.4).	<input type="checkbox"/>
<b>Dispose</b>	
CCTV records are retained appropriately and disposed of lawfully, in accordance with <i>Information Standard 31: Retention and Disposal of Public Records</i> (see section 4.5.1).	<input type="checkbox"/>
CCTV records are retained for at least the specified minimum retention period, in accordance with the <i>General Retention and Disposal Schedule for Administrative Records</i> or relevant sector- or agency-specific Retention and Disposal Schedule (see section 4.5.1).	<input type="checkbox"/>
Documented business processes are in place which establish when the disposal trigger of 'no further administrative use' can be applied (see section 4.5.1).	<input type="checkbox"/>
Disposal of public records is conducted appropriately and documentation regarding disposal of public records is captured and retained permanently (see section 4.5.2).	<input type="checkbox"/>

## Appendix B: Glossary

The Glossary below provides clarification and definitions of the terms relating to the operation of CCTV used in this document.

Records and information management-specific terms are defined in Queensland State Archives' *Glossary of Archival and Recordkeeping Terms* available on Queensland State Archives' website at: [www.archives.qld.gov.au/downloads/GlossaryOfArchivalRKTerms.pdf](http://www.archives.qld.gov.au/downloads/GlossaryOfArchivalRKTerms.pdf).

<b>- A -</b>	
Access Control	A system for restricting access to a particular resource, such as physical property or a data set. Access control mechanisms grant and revoke privileges based on established rules.
Active System Monitoring	Trained personnel use cameras actively to conduct surveillance of areas in support of law enforcement or security officers on the ground. Similarly, use of CCTV systems by transport control personnel to manage signals or controls to balance passenger and vehicle flows.
Analogue Signal	A signal which conveys data in continuously varying quantities, as opposed to discrete values as in digital signals.
Artefact	Undesirable elements or errors in a video image. Artefacts may occur naturally or may be introduced through compression.
<b>- B -</b>	
Bit Rate	The number of bits (units of information) used for compressing video per second, or transmitted per unit of time. As such, it is a measure of image quality. With a higher bit rate, more information can be carried.
<b>- C -</b>	
CCTV – Closed Circuit Television	A video system which is monitored in a closed environment, as opposed to public broadcast. CCTV transmits signals in analogue or digital form over a closed circuit via an electrical conducting cable, fibre-optic cable, or wireless connection. A standard CCTV system includes a camera or series of cameras for capturing video, transmitters and receivers to transfer video from the source to where it is recorded, a recording system for video playback and extraction, and a monitor for observation.
Compression Method	The process of encoding data by using fewer bits, either to save storage or to use less bandwidth in transmission. Video compression is either lossy, in which data is lost, or lossless, which will provide a bit-for-bit match with the original.
<b>- D -</b>	
Digital Signal	A signal in which information is conveyed in discrete states, as opposed to analogue signals, which are continuously varying. A video signal will comprise bits of binary data (1s and 0s).
Digital Video Recorder – DVR	A device that is capable of capturing one or more video input signals in a digital format to a disk drive or other digital storage device. DVRs have now largely replaced VCR recorders in CCTV installations.
<b>- E -</b>	
Encryption	A technique used to secure information transmitted over a communication channel to prevent all parties other than authorised receivers from interpreting the message. Encryption relies on the rearrangement of the bit stream of an encoded signal to make the information unrecognisable without a decryption key.
<b>- F -</b>	
Field of View – FoV	Also known as Angle of View. The extent of image that can be seen through a given lens. Described in terms of diagonal, horizontal, or vertical degrees.

Fixed Lens	A fixed focus lens has a set focal length and field of view that cannot be changed, as opposed to a varifocal lens.
Focal Length	A property of a lens, expressed in millimetres, which is defined by the distance between the optical centre of a lens and the principal convergent focus point.
Frame	The frame is the total area occupied by the television picture. A full frame of video is two image fields interlaced together. A frame within NTSC is composed of 525 lines, whereas PAL frames are composed of 625 lines.
Frames per second – FPS	The number of full video frames displayed or recorded in one second. In NTSC format, 30 frames are displayed for one second of real-time video. In PAL format, 25 frames represent real-time recording.
- I -	
Image Analysis	The application of digital processing techniques to extract information from images. Image analysis is used in number plate recognition (NPR) technologies and for facial/iris recognition.
- J -	
JPEG – Joint Photographic Experts Group	JPEG is a lossy compression format commonly used for image data.
- L -	
Lens	An optical device which focuses light onto an image sensor to create a visible image. Lenses are typically made of optical-grade glass and have curved surfaces to converge or diverge transmitted light from an object.
Lossless Compression	Any compression technique where smaller file sizes are achieved without the loss of Original Image data values. The image can be retrieved in its original form.
Lossy Compression	Any compression technique where image data is irretrievably lost in the compression process. The effects of the compression may or may not be visible, but the original data cannot be restored.
- M -	
MPEG – Motion Picture Experts Group	A ubiquitous lossy standard for compressing video image data.
- N -	
NTSC – National Television Systems Committee	The National Television Systems Committee (NTSC) formulated television standards for colour television used in the USA, Japan, South Korea, Taiwan, Burma and some Pacific island nations. The colour broadcasting standard was developed in 1953. An NTSC video frame comprises two interlaced fields transmitted at 60 cycles per second (60Hz). One frame comprises 525 scan lines.
- P -	
Passive Monitoring	Employee monitoring of a small number of television screens showing a selection of available CCTV footage (in conjunction with, or incidental to, other duties).
PAL – Phase Alternate Line	PAL is the colour encoding standard for television in Australia, Great Britain and the majority of Europe. The PAL composite video signal is composed of luminance (light) and chrominance (colour) signals. A PAL video frame comprises two interlaced fields transmitted at 50 cycles per second (50Hz). One frame comprises 625 scan lines.



- R -	
RAID – Redundant Arrays of Independent Disks	A number of hard disk drives connected into one mass storage device, used for the storage and retrieval of digital video images, among other data.
Recording Monitoring	CCTV systems may record images whether they are monitored or not. Such records may be accessed and used for intelligence, investigative or evidentiary purposes.
Resolution	The measure of the ability of an imaging system to reproduce detail, seen in how clear and sharp a video image will be displayed. The greater the number of pixels, the higher the resolution.
- S -	
Scene Illumination	The average light level of an identified area, usually measured for the human visible spectrum. Illumination is measured in lux.
- T -	
Time Lapse	Video cassette recorders have traditionally employed time lapse recording to allow extended periods of time to be captured on a single video tape. This technique employs frequent tape pauses. The longer the recording time, the fewer images captured per second. Time lapse VCRs often had external alarm triggers, and the capacity to mark the video signal with time and date stamps.
- V -	
Varifocal Lens	A lens with an adjustable focal length, able to provide wider viewing angles or narrower telephoto fields of view. Varifocal lenses, also known as zoom lenses, provide flexibility to CCTV operations.
VCR – Video Cassette Recorder	An analogue device capable of accepting video and audio signals which are recorded onto a magnetic tape, typically VHS. Tapes are able to be played back using the same device. Surveillance VCRs offer time lapse recording.
VHS	A standard size for VCR cassette tapes.
Video Analytics	Software that monitors real-time video for specific applications, such as facial recognition, left objects (e.g. abandoned bags) and crowd control.
Video Motion Detection	An advanced software feature which detects motion in a camera's field of view and commences recording. Video motion detection is a feature of many digital video recorders. Specific areas can be identified in the camera's field of view for attention.
- W -	
Wavelet	A mathematical function used in signal processing and video image compression.
WORM – Write Once, Read Many	WORM, Write-Once, Read-Many, is a storage technology that allows data to be written permanently to an optical medium, preventing alteration or erasure. WORM devices are typically used for archival or judicial purposes.

## Appendix C: Australian Standards

A suite of four Australian Standards providing guidance on the management, operation, and technical specifications of CCTV was developed in response to end-user and industry requests.

The Standards are available for purchase in .pdf or hard copy format from [www.saiglobal.com/shop/script/Details.asp?DocN=AS229907590845](http://www.saiglobal.com/shop/script/Details.asp?DocN=AS229907590845).

<b>Australian Standard</b>	<b>Operation</b>
<b>AS 4806.1–2006:</b> <b><i>Closed Circuit Television (CCTV): Management and operation</i></b>	This Standard provides recommendations as to the operation and management of CCTV within a controlled environment, where data that may be offered as evidence is received, stored, reviewed or analysed. The Standard is applicable to CCTV systems in public places, systems that overlook public places, and those where camera views adjoin a public place. The Standard provides good practice guidelines for all other Australian CCTV systems. Clauses on the management of visual surveillance data are applicable to the storage of recorded images.
<b>AS 4806.2–2006:</b> <b><i>Closed Circuit Television (CCTV): Application guidelines</i></b>	This Standard provides a technical specification for Australian CCTV operations and the means by which a system may be objectively evaluated. It considers system design criteria, installation requirements, commissioning and handover, preventative maintenance and objective test planning (OTP). The Standard also notes State-based requirements for licensed operation and notification.
<b>AS4806.3–2006:</b> <b><i>Closed Circuit Television (CCTV): PAL signal timings and levels</i></b>	This Standard provides specifications for Phase Alternating Line (PAL) CCTV signal timings and levels. These recommendations are based on the Australian Communications and Media Authority Technical Planning Guidelines.
<b>AS4806.4–2006:</b> <b><i>Closed Circuit Television (CCTV): Remote video</i></b>	This Standard outlines recommendations and requirements for the design, installation, commissioning, operation and remote monitoring of CCTV surveillance systems, detector-activated alarm verification CCTV systems, and interactive video management CCTV systems. It details the responsibilities of system owners, and expected service levels.

## Appendix D: Codes of Practice

Several codes of practice currently exist with regard to the use of CCTV footage in Australia. These typically outline:

1. General rationale for the introduction of CCTV and background to the installation of the program
2. Technical specifications of the cameras and their locations
3. Ownership and management of the system
4. Objectives of the system
5. Accountability and complaints procedures
6. Management of the control room, and
7. Retention of and access to recorded images.<sup>67</sup>

### ***Council of Australian Governments' CCTV Code of Practice***

The Australian Federal Government proposed a series of security counter-measures to protect mass transport in response to the London Underground bombings of 7 July 2005. The Council of Australian Governments (COAG) endorsed 'A National Approach to Closed Circuit Television' at the 27 September 2005 Special Meeting on Counter-Terrorism, noting that Australian jurisdictions operated extensive CCTV networks across transport, public spaces, and major facilities.<sup>68</sup> Each jurisdiction was required to review the functionality, location, coverage, and operation of mass passenger transport CCTV systems.

The resultant voluntary Code of Practice was passed on 14 July 2006, establishing a policy framework, objectives, protocols and minimum requirements for the use of CCTV systems to enhance counter-terrorism arrangements, acknowledging associated risks.<sup>69</sup>

### ***Department of Transport and Main Roads (Queensland) Portfolio Code of Practice for CCTV***

The *Transport Portfolio Code of Practice for Closed Circuit Television Systems* has been developed by the Department of Transport and Main Roads (Queensland) for the installation and operation of CCTV in the State's buses and taxis.<sup>70</sup> It specifies 10 principles for the operation of CCTV:

- Principle 1 Purpose
- Principle 2 Public Interest
- Principle 3 Responsibilities and Accountabilities
- Principle 4 Recorded Imagery
- Principle 5 Responsibility to Ensure CCTV System is Maintained and Operational
- Principle 6 Contact with Police
- Principle 7 Duty of Care
- Principle 8 Breaches of this Code
- Principle 9 Security of CCTV Equipment and Recorded Images
- Principle 10 Control Rooms

---

<sup>67</sup> Wilson, D., & Sutton, A. (2003). Open-Street CCTV in Australia. *Trends & Issues*, 271, Australian Institute of Criminology compares five codes of practice from Sydney, Lismore, Canberra, Bendigo, and Perth.

<sup>68</sup> [www.immi.gov.au/media/publications/multicultural/pdf\\_doc/coag270905.pdf](http://www.immi.gov.au/media/publications/multicultural/pdf_doc/coag270905.pdf)

<sup>69</sup> [www.coag.gov.au/coag\\_meeting\\_outcomes/2006-07-14/docs/cctv\\_code\\_practice.rtf](http://www.coag.gov.au/coag_meeting_outcomes/2006-07-14/docs/cctv_code_practice.rtf)

<sup>70</sup> [http://www.tmr.qld.gov.au/~media/about-us/corporate-information/publications/cctv-code-of-practice/code\\_ccvt\\_feb\\_2007.pdf](http://www.tmr.qld.gov.au/~media/about-us/corporate-information/publications/cctv-code-of-practice/code_ccvt_feb_2007.pdf)

These principles have been adopted in *A Recommended Code of Practice for the Use of Closed Circuit Television (CCTV) by Operators of Passenger Transport Services and Infrastructure*.<sup>71</sup>

Specifications from the *Transport Operations (Passenger Transport) Regulation 2005* have been included in the Department of Transport and Main Roads (Queensland) Code of Practice for operation of surveillance cameras.<sup>72</sup>

---

<sup>71</sup>[http://www.tmr.qld.gov.au/~media/travel-and-transport/public-transport/pdf\\_pt404\\_code\\_of\\_practice\\_for\\_cctv\\_0308.pdf](http://www.tmr.qld.gov.au/~media/travel-and-transport/public-transport/pdf_pt404_code_of_practice_for_cctv_0308.pdf)

<sup>72</sup>[www.legislation.qld.gov.au/LEGISLTN/SLS/2005/05SL329.pdf](http://www.legislation.qld.gov.au/LEGISLTN/SLS/2005/05SL329.pdf)

## Appendix E: International Standardisation Initiatives

The Australian Customs and Border Protection Service reports on the latest efforts to develop an international standard for networked CCTV interoperability, to resolve the divergence in the industry in terms of hardware and software implementation. They note:

A standard is needed, not simply for signal format compatibility, but also to allow components from different manufacturers to exchange audio data, metadata, video analytical data as well as component capability information.

...

A single industry standard should bring considerable benefits to end users in terms of greater choice of equipment, greater flexibility, easier integration of systems and lower lifecycle cost.<sup>73</sup>

In early 2008, three leading global manufacturers formed the Open Network Video Interface Forum (ONVIF) ([www.onvif.org/](http://www.onvif.org/)) to work towards a new standard for networked CCTV interoperability. The ONVIF has made considerable progress and some parts of the new standard are available for comments. Another group of manufacturers, called the Physical Security Interoperability Alliance (PSIA) ([www.psialliance.org/](http://www.psialliance.org/)) has also developed and released some specifications, claiming its standard to be superior.

Data exchanged in network transactions can encompass details of video format (JPEG, MPEG-4, H.264), metadata (time, date, location), video analytical data, initialisation and control data, and security protocols.

Australian Customs CCTV Advisory Service regards the benefits accruing from the adoption of a video interface standard as follows:

- New users and system designers will have the ability to mix and match from a range of vendors, thus assembling a system that most closely meets their needs;
- Greater choice for end users when selecting replacement video components because there will be no need to limit the selection to the brand of the system they own (provided it is compatible with the standard);
- Longer effective system life, hence lower lifecycle cost, as it will not be necessary to replace an entire system if a manufacturer discontinues production of a key component;
- The prospect of sharing video feeds between different jurisdictions and organisations, with minimal hardware compatibility issues;
- Simpler installation and commissioning of systems;
- Reduced need for special software patches or other development costs when designing special purpose systems;
- Simpler, more uniform operating procedures because of a common configuration language;
- Greater variety in the products on the market, because smaller manufacturers will be able to produce compatible products.

Both the ONVIF and PSIA standards are set to be voluntary.

---

<sup>73</sup> [www.customs.gov.au/site/page5967.asp](http://www.customs.gov.au/site/page5967.asp)

## Appendix F: Australian Research into CCTV

The Report to the Criminology Research Council of Australia in April 2003, *Open-Street CCTV in Australia: A comparative study of establishment and operation*, by Dean Wilson and Adam Sutton, presented the first comprehensive overview of the operation of CCTV in Australia's public spaces.<sup>74</sup> According to this research, at that point in time, 33 systems were operated by local governments in Australia, with 10 in Queensland.<sup>75</sup> Wilson and Sutton called for a consistent approach to the study and regulation of CCTV in the country.

There is a need for legislation to regulate open-street CCTV schemes, and bring some coherence to their manner of operation and mechanisms of accountability. Well thought out legislation, guidelines and codes of practice would increase public confidence that CCTV systems were appropriately controlled, administered and accountable. (Abstract)

### Select Bibliography of Australian CCTV Research

Brew, N. (2005). An overview of the effectiveness of closed circuit television (CCTV) surveillance. Parliament of Australia Department of Parliamentary Services Research Note 14. Retrieved August 6, 2009, from [www.aph.gov.au/library/pubs/RN/2005-06/06rn14.pdf](http://www.aph.gov.au/library/pubs/RN/2005-06/06rn14.pdf).

Brooks, D.J. (2008). *Public street CCTV: A psychometric study of social risk*. Saarbrücken: VDM Verlag.

Wells, H., Allard, T., & Wilson, P. (2006). Crime and CCTV in Australia: Understanding the Relationship. *Humanities & Social Sciences papers*. Centre for Applied Psychology and Criminology: Bond University. Retrieved August 6, 2009, from [http://epublications.bond.edu.au/hss\\_pubs/70/](http://epublications.bond.edu.au/hss_pubs/70/).

Wilson, D., & Sutton, A. (2003). Open-Street CCTV in Australia. *Trends & Issues*, 271, Australian Institute of Criminology.

Wilson, D., & Sutton, A. (2004). Open-Street CCTV in Australia: The Politics of Resistance and Expansion. *Surveillance & Society*, 2(2/3), 310-322. Retrieved August 6, 2009, from [www.surveillance-and-society.org/articles2\(2\)/australia.pdf](http://www.surveillance-and-society.org/articles2(2)/australia.pdf).

Wilson, P., & Wells, H. (2007). What do the watchers watch? An Australian case study of CCTV monitoring. *Humanities & Social Sciences papers*. Faculty of Humanities and Social Sciences: Bond University. Retrieved August 6, 2009, from [http://epublications.bond.edu.au/cgi/viewcontent.cgi?article=1265&context=hss\\_pubs](http://epublications.bond.edu.au/cgi/viewcontent.cgi?article=1265&context=hss_pubs)

---

<sup>74</sup> [www.criminologyresearchcouncil.gov.au/reports/200102-26.pdf](http://www.criminologyresearchcouncil.gov.au/reports/200102-26.pdf)

<sup>75</sup> Town-centre schemes operated in Brisbane, Cairns, Gatton, Gold Coast, Ipswich, Logan, Rockhampton, Toowoomba, Townsville, and Warwick.

## Appendix G: Comparison of Video File Formats

A significant issue encountered with digital CCTV to date has been that there is no universal standard for the compression of video images, with manufacturers employing a variety of open, proprietary, and mixed compression formats.

Table 5 below provides a comparison of various compression formats for the transmission and storage of still and moving images.

**Table 5: Comparison of Video File Formats**

Compression (Technique)	Bit Rate	Resolution	Frame Rate (fps)	Strengths	Weaknesses	Applications
JPEG (DCT)	8Mbps	Unspecified	0-5	As an industry standard, JPEGs can be viewed by a large range of systems.	Not suitable for motion – videos appear blocky under high compression ratios.	Storing still video frames and photographs. Very low frame-rate CCTV.
JPEG2000 (Wavelet)	30 Kbps to 7.5 Mbps	160x120 320x240	8-30	High compression artefacts – fuzzy picture – are more acceptable than blocky artefacts. Final file sizes smaller than images compressed via DCT to an equivalent quality level.	Significant lag.	Some CCTV recording.
MJPEG (DCT)	10Kbps to 3Mbps	Any size	0-30	Same advantage as JPEG, with ability to be played in rapid succession.	The popularity of MJPEG has meant the acceptance of lower frame rates in security applications.	Common in CCTV due to simplicity. IP Networks.

Compression (Technique)	Bit Rate	Resolution	Frame Rate (fps)	Strengths	Weaknesses	Applications
Motion JPEG2000 (Wavelet)	30Kbps to 70Mbps	Any size	0-30	Motion JPEG 2000 is a flexible format, permitting a wide variety of usages, such as editing, display, interchange, and streaming.	Large image sizes	High resolution CCTV.
MPEG-1 (DCT)	1.5Mbps	352x288 (PAL) 352x240 (NTSC)	Up to 30	VHS quality on low-cost video CDs (VCDs).	Constrained to VHS quality.	VHS quality. Low-cost video CDs (VCDs).
MPEG-2 (DCT)	2Mbps to 15Mbps	720x576 (PAL) 720x480 (NTSC)	24-30	Broadcast quality.	Bandwidth intensive at 2 – 15 Mbps per camera.	Broadcast quality video, HDTV, DVDs, high-fidelity stereo audio.
MPEG-4 PART 2 (DCT and Wavelet)	10Kbps to 10Mbps	640x480 to 4096x2048	1-60	Efficient at high frame rates.	Limited performance at low frame rates or high scene activity. When bit rate limited, video artefacts – speckling, blocky quality.	Streaming video via Internet, CCTV when a high frame rate is used, or when scene activity is low to medium.
H.263 (DCT)	30 Kbps to 64 Kbps	128x96 to 704x480	10-15	Optimised for low data transfer rates.	Low performance when higher bandwidths are available.	Connections via modem and analogue telephone lines. Video streaming teleconference.
H.264/MPEG-4 PART 10 (DCT)	64 Kbps to 240 Mbps	4096x2048	0-30	Near broadcast quality. Compression more efficient than MPEG-4 Part 2.	Need for high power processing hardware. Higher lag times.	High-speed video. HD DVDs, HDTV and Pay TV.
MPEG-7	-	-	-			Multi-media content. Smart cards. Not yet in security applications.



## Appendix H: Logs

The following registers should be completed within the Control Room of a CCTV operation:

- Visitors Log
- CCTV Incident Log
- CCTV Maintenance Log / Fault Reports Log
- CCTV Viewing Log
- Issued Copy of Image Log
- Daily CCTV System Check Log (Operators Log)

Example templates for these registers are provided below:

### Visitors Log

Date	Arrival	Departure	Surname	Init.	Organisation	Position	Signature	Signed In By

### CCTV Incident Log

Date:	Time:	Location:
Incident Type:		
Recording Number:		Live Incident Recording: YES/NO
Name of Person Reporting:		Employer:
Description of Incident:		
Response to Incident:		
If Police required, time requested:		Time of Police arrival:
Name(s) of attending Police Officer(s):		Registered Number(s):
If medical assistance required, time requested:		Time of medical assistance arrival:
Name(s) of attending Medical Officer(s):		
Name of Monitoring Room Officer:		Signature:

### CCTV Maintenance Log / Fault Reports Log

Date:	Time:	Engineer:
Reason: Regular Maintenance / Call Out		
Maintenance Details:		
Outcome:		

### Viewing Log of CCTV Images

Date of Viewing	Time of Viewing	Tape/CD/DVD Identifier	Operator

Name(s) of Person Viewing	Organisational Details

Reason For Viewing
Outcome If Any

### Issued Copy of Image Log

Reason for Provision: Legal Proceedings/Subject Access/Other			
Date of Creation	Time of Creation	Operator	Tape/CD/DVD Identifier
Crime/Incident No			
Police Officer/Third Party Name			
Contact Details			
Signature of Third Party	Date of Destruction or Return	Signature of Manager	

### Daily CCTV System Check Log

Building/Dept/Unit:				

Date	Time	Operator	Date/Time Stamp Checked	Cameras & Recording Quality Checked

## Appendix I: Calculation of Storage Requirements

The following equation allows an agency to calculate the total amount of storage required for a particular CCTV operation, as provided by the Australian Customs CCTV Advisory Service:

- Determine the numbers of cameras ( $N_c$ );
- Determine the frame rate (frames per second) at which each camera will be recorded at ( $R_f$ );
- Determine the average size (in kilobytes) that each compressed frame of video will take up on the hard disk ( $S_f$ ) after the compression ratio has been applied;
- Approximate the activity (in percentage) time each camera will be recording at the above frame rate ( $A$ ); and
- Determine the duration (in days) that video from each camera will be retained ( $D$ ).<sup>76</sup>

Once these values are determined, the following formula can be used to determine the HDD capacity:

$$\text{Capacity(Gigabytes)} = \frac{N_c \times R_f \times S_f \times A \times (3600 \times 24 \times D)}{1000000}$$

A CCTV system's storage capacity is thus dependent on several factors:

- Image size;
- Frames per second;
- Number of cameras;
- Operational hours;
- Required retention period.

Typical values for these variables are:

- Frame size: 5kB – 50kB
- Frames per second: 1 – 30
- Number of cameras: 1 – 16
- Operational hours: 1 – 24
- Retention period: 24 hours – 31 days.

This equation is applicable to scenarios where all closed circuit cameras produce images of the same size and frame rate over the same operational period. In more complex systems, storage requirements can be calculated for each camera, and totalled to provide the overall system requirements.

---

<sup>76</sup> [www.customs.gov.au/site/page5974.asp](http://www.customs.gov.au/site/page5974.asp)

A further equation is provided by the UK Home Office Scientific Development Branch in the *CCTV Operational Requirements Manual 2009*,<sup>77</sup> as follows:

$$\frac{\text{Image size} \times \text{frames per second} \times \text{no. cameras} \times \text{operational hours} \times 3600 \times \text{retention period}}{1,000,000}$$

Image size is calculated in kilobytes

Operational hours are calculated over a 24-hour period

3600 converts seconds to hours

1,000,000 converts kilobytes to gigabytes

### Example 1

A CCTV system is being designed for a custody suite that is required to capture high-quality images of 20kB per frame. 12fps per camera are being generated and there are 8 cameras in the system. Each camera is recorded for 24 hours per day, and the retention period is 31 days. The storage capacity is given by:

$$\left( \frac{20 \times 12 \times 8 \times 24 \times 3,600}{1,000,000} \right) \times 31 = 5142 \text{ (GB)}$$

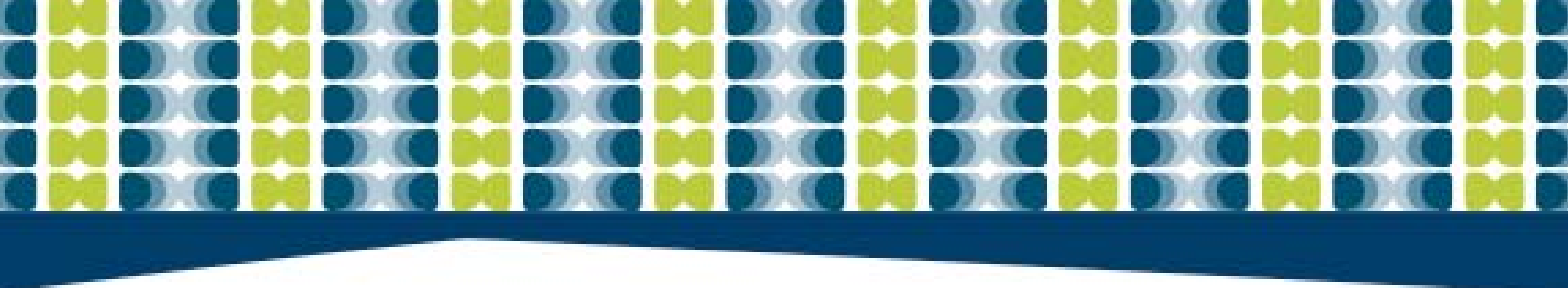
### Example 2

A retail outlet is installing a small CCTV system to monitor the access points (windows and doors) whilst the shop is closed. The image frame size has been set to a 'medium' value (10kB), and the resultant image checked for suitability. The recorder will be triggered by motion detection and IR sensors and the average frame rate has been calculated at 2fps for all the cameras. 6 camera locations have been identified to offer maximum coverage, and all the cameras will only be recording for the hours the venue is closed from 7pm to 7am. As the reason for the system is to provide evidence after a break-in the retention time has again been set to 31 days. The storage requirement is given by:

$$\left( \frac{10 \times 2 \times 6 \times 12 \times 3,600}{1,000,000} \right) \times 31 = 160 \text{ GB}$$

<sup>77</sup> Available at

[http://tna.europarchive.org/20100413151426/http://scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/28\\_09\\_CCTV\\_OR\\_Manual2835.pdf?view=Binary](http://tna.europarchive.org/20100413151426/http://scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/28_09_CCTV_OR_Manual2835.pdf?view=Binary)



---

For more detailed guidance on the management of public records visit the Queensland State Archives website at [www.archives.qld.gov.au](http://www.archives.qld.gov.au) or contact us on: Telephone: (07) 3131 7777 or Email: [info@archives.qld.gov.au](mailto:info@archives.qld.gov.au)