

# Closed circuit television system policy and procedure

## 1. Policy statement

This policy sets out a framework for the management of the Level 18, 53 Albert Street, Brisbane, closed circuit television system (CCTV) used by the Office of the Queensland Ombudsman (the Office). All CCTV cameras are installed to surveil public areas as part of a security system to act as a deterrent to unwanted behaviour of persons, as an aid to the monitoring of people, events or activities, and to assist in timely and effective response to incidents and to gather evidentiary material.

This policy and procedure provides information in relation to the operation of CCTV in the Office.

## 2. Principles

The operation of the CCTV system will be:

- in accordance with Australian legislative requirements and applicable laws
- operated ethically with due regard to the privacy and civil liberties of members of the public and employees
- operated, maintained and monitored in accordance with this policy and guideline for the ethical use of the CCTV system.

## 3. Application/scope

This policy applies to all permanent and temporary employees of the Office as well as contractors, employment agency staff, sub-contractors, clients, work experience students and volunteers (who are defined as workers in the *Work Health and Safety Act 2011*) while working in the Office.

It specifically places requirements on management, certain employees and/or other persons (e.g. contractors) providing security services to, or on behalf of the Office. Authorised officers will abide by the guideline for the ethical use of the CCTV system (see Appendix A).

## 4. CCTV system ownership and control

The Queensland Ombudsman is designated as having overall responsibility for the formulation and implementation of the policies, purpose and control of the CCTV system, as it operates on level 18 of 53 Albert Street.

The level 18 CCTV cameras form part of a CCTV system which is used by, and covers, levels 17 to 22. The main service components including software and hard drives are located in the secure Level 17 data centre.

Responsibility for managing and maintaining the system has been transferred to the Department of Energy and Public Works, on behalf of all tenants using levels 17 to 22. Each tenant is however responsible for their own system (including policy and procedures) and liaising with the Building Security Co-ordinator in relation to system issues.

The CCTV system is also connected to, and displayed at, the Building Security Coordinator (BSC) security station in the ground floor foyer. The building owner is responsible for CCTV in the entry of the building and external perimeter. A CCTV camera also operates in the Level 17 Data Centre.

The BSC is subject to the Queensland Police Protective Service (QPPS)'s policies and procedures, including the operation of CCTV equipment and the management, retention and disposal of records.

## **5. Procedures**

### **5.1 CCTV acquisition**

The Office will procure any new CCTV cameras or modifications to the existing level 18 CCTV system in accordance with the Office's procurement policies. In modifying the CCTV system, the Office may consult the QPPS to obtain advice and guidance in managing the CCTV infrastructure and camera placement.

Areas to be subjected to surveillance by fixed cameras are the level 18 public reception area, lift foyer, interview rooms, and hallway and level 17 data centre. Fixed cameras are selected for defined fields of view which have a designated and defined purpose, either to detect, recognise or identify.

A risk assessment will be undertaken when installing new CCTV cameras. The risk assessment will consider each camera placement and location to ensure that the installation is effective.

No audio recording devices have been installed.

The Office will ensure that contractors hold appropriate qualifications and licences. Further, contractors will be bound by the provisions of the *Information Privacy Act 2009*.

Storage of surveillance images will be in Australia as determined by the Information Management Steering Committee.

### **5.2 CCTV maintenance**

Maintenance and support of the CCTV system is the responsibility of the Department of Energy and Public Works, which is responsible for organising a maintenance regime for the CCTV system that will ensure:

- CCTV recording equipment is in a fully functional working order
- clear, recorded vision from each camera is available at all times
- any system failures are promptly responded to..

The Intake Team is responsible for monitoring and removing obstructions (boxes, furniture) and reporting faults with the CCTV system to the CSU-IS.

In the event of CCTV system failure, (other than power) the CSU-IS will conduct a preliminary investigation to determine the cause, including where appropriate, rebooting the CCTV system. If this fails to correct the problem the matter is to be reported to Building Security who will lodge a maintenance call-out request to the contracted service provider, and who will advise agencies of the outage.

Remote connection to the CCTV system is not available.

### **5.3 Control of CCTV cameras**

Cameras will be positioned in a way that does not intrude to an unreasonable extent on the privacy of individuals. Cameras will not be positioned to look into or monitor adjacent or nearby premises or buildings, except for following (in real time) participants in a situation of concern. CCTV cameras will not be used in toilets.

Only authorised officers (CSU-IS, BSC and CCTV vendor) will have access to camera operating controls.

### **5.4 User access and security**

Access to the CCTV system and recordings are detailed in 6. Roles, responsibilities and authorisation.

Requests for access change to the CCTV system, such as creating a new user or operator and defining their role, must be submitted for approval to the Director, Corporate Services Unit (CSU) or the Chief Financial Officer.

All CCTV monitoring software must be held in a locked cupboard with the screen turned off.

Only the BSC and the CCTV vendor have access to historical CCTV footage. Other authorised employees are only able to view live CCTV footage on a limited number of screens.

Access to overt surveillance images is restricted to those authorised and to those employees authorised to monitor or operate the surveillance equipment as a normal part of their duties.

Access to covert surveillance images shall be limited to the authorised officers, the security officer/operator conducting the surveillance and the person or agency authorised in writing to conduct and/or view the surveillance footage.

Footage from the Level 18 CCTV system will not be disclosed to any agency or organisation, other than an agency with a tenancy on level 18, except in accordance with this policy.

### **5.5 Training and education**

Employees responsible for surveillance will be trained in the ethical conduct and use of CCTV surveillance systems upon induction. Reminders will be issued to officers identified in 6. Roles, responsibilities and authorisation about acting in accordance with this policy and the Guideline for the ethical use of the CCTV system (Appendix A).

Employees must sign the Guideline for the ethical use of the CCTV system (Appendix A) prior to viewing any footage.

BSC will be trained by the CCTV vendor in how to extract CCTV footage. The CCTV vendor will provide training manuals on operating the CCTV system and will be engaged as required to train new authorised officers in operating the system as per their role requirements.

### **5.6 Complaints regarding the CCTV system and its operation**

Complaints are to be handled in accordance with the Office's complaint management policies and procedures. The Director, Corporate Services Unit must be advised of any complaint relating to the operation of the CCTV system.

The Office will refer complaints regarding the BSC to the QPPS.

## 5.7 Breaches

Any misuse by an employee may amount to a breach of the Guideline for the ethical use of the CCTV system and the Office's code of conduct and disciplinary action may be taken in accordance with the Office's Discipline policy.

Breaches by the BSC will be addressed with QPPS. If the CCTV vendor acts inappropriately breaches will be managed in accordance with the contract by the Department of Energy and Public Works.

All authorised officers will be made aware that recordings are subject to routine audit and they will be required to justify their interest in a particular member of the public or other person.

## 5.8 CCTV back-up

No backup is held of CCTV footage, however recorded CCTV footage is temporarily stored for up to 90 days on the hard drive.

The only data requiring backup is relatively low in volume and its backup is managed by the vendor. This data includes:

- operating system and utility software
- system configuration data
- CCTV software.

## 5.9 Covert surveillance

In exceptional circumstances, covert surveillance may be required where there is a concern about the security of an area or there is suspected criminal activity or serious misconduct occurring.

Approval in writing shall be given by the Queensland Ombudsman prior to installation of covert CCTV systems within the workplace.

When seeking written approval to undertake covert CCTV surveillance the following information shall be provided:

- the evidence-based grounds for the request (e.g. specific person or persons may be involved in unlawful activities)
- details of any other managerial or investigative actions which have already been conducted
- who or what will be in view of the camera
- proposed dates and times of surveillance (not to be open ended).

Any written approval given will remain in force for a maximum of 30 days.

Covert surveillance targetted at employees will only occur following approval of a disciplinary investigation by the Queensland Ombudsman.

Covert primary surveillance images shall be stored securely from unauthorised access. Access should be limited and strictly controlled with access being documented in the CCTV image access register. As soon as practicable, original covert surveillance images should be copied and delivered to the Queensland Ombudsman, delegated officer or enforcement agency. The Queensland Ombudsman or delegated officer will ensure the original covert surveillance images are secured in a lockable unit in an area where access can be limited and strictly controlled.

Original covert surveillance images not containing images of an employee's involvement in misconduct or unlawful activity shall be destroyed within 31 days of the Queensland Ombudsman's written authority to do so.

Original covert surveillance images that are used as evidence in disciplinary proceedings against an employee and which form a part of their disciplinary file will be retained in accordance with the Office's recordkeeping retention and disposal schedules.

## **5.10 Access to recorded overt or covert surveillance images**

### **5.10.1 Request for recorded CCTV footage form**

Strict limitations are in place as to who can access and retain recorded CCTV images. Further details are outlined in 5.9.2 CCTV footage form approval. Footage can be obtained as follows:

- Queensland Ombudsman employees wishing to view recorded images must first gain written authorisation from an authorised officer, by completing the Request for recorded CCTV footage form (Appendix C), along with providing an encrypted USB.
- A member of the public can apply to access CCTV footage by making an Information Privacy or Right to Information request. The Right to Information Officer will liaise with an authorised officer to complete the Request for recorded CCTV footage form (Appendix C), together with providing an encrypted USB. The Right to Information Officer will liaise with the BSC to obtain a copy of the extracted CCTV footage and ensure any deidentification required occurs before providing the CCTV footage to the member of the public.
- If CCTV footage is required for court or tribunal proceedings (whether via summons, subpoena, notice to produce or otherwise) the agency must contact the General Counsel to request access to the CCTV footage, outlining the reasons why access is required. The General Counsel will manage retrieving CCTV footage in accordance with the request.

### **5.10.2 CCTV footage form approval**

CCTV footage may only be authorised for disclosure (extracted, exported and handed over), if it meets one or more of the following criteria:

- approved right to information or information privacy request
- an approved request for recorded CCTV footage from an authorised officer
- a request for recorded CCTV footage from a law enforcement agency
- for use in court or tribunal proceedings (pursuant to compulsory process for a subpoena).

In determining whether approval is to be granted to release CCTV footage, authorised officers are to be satisfied that the reasons provided by the requestor are lawful and reasonable. Consideration must always be given to protecting the rights of other persons captured on the CCTV recording.

Before an authorised officer authorises disclosure of CCTV footage, they must be satisfied that:

- the request for recorded CCTV footage form has been properly completed
- on reasonable grounds that the use/disclosure is necessary to prevent or lessen a serious threat to the health, safety, welfare or life of an individual or public health, safety or welfare

or

- on reasonable grounds that the use/disclosure is necessary for legal or law enforcement purposes:

- prevention, detection, investigation, prosecution or punishment of criminal offence, breaches of laws imposing penalties/sanctions
  - the enforcement of laws relating to the confiscation of the proceeds of crime
  - the protection of the public revenue
  - the prevention, detection, investigation or remedying of seriously improper conduct
  - the preparation for, or conduct of, proceedings before any court or tribunal
  - the implementation of the orders of a court or tribunal
- the CCTV footage will not be disclosed to other parties inappropriately or unnecessarily
  - it is not appropriate to get the individual's consent to obtain the CCTV footage.

An approving officer may consult General Counsel or the Ombudsman on the appropriateness of approving a request to release CCTV footage.

Once the authorised officer has approved the request (signed Appendix C), the authorised officer is responsible for scanning a copy of the approval and saving into the Office's electronic recordkeeping system. Once this has been done the form must be taken to the BSC along with the encrypted USB.

### **5.10.3 BSC CCTV footage extraction**

The BSC will complete the Appendix D Level 18 Albert Street request for recorded CCTV footage form and return the footage on the encrypted USB to the authorised officer. Any issues in relation to the extraction of the CCTV footage are to be discussed with the authorised officer.

The authorised officer will provide the encrypted USB to the requestor giving consideration to 5.10.4 De-identifying CCTV footage. The requestor is responsible for managing the CCTV footage in accordance with the Office's recordkeeping policies.

The BSC is the primary capturer of extracted CCTV footage from the CCTV system, and those images will initially be stored on the Level 17 CCTV base computer.

As the owners (at least in common), of the captured CCTV footage, the Office has a duty of care to ensure that BSC and QPPS are providing proper management of the captured CCTV footage. To assist the Queensland Ombudsman in meeting this obligation the BSC will provide the Chief Financial Officer with a copy of the report detailing what footage has been exported.

### **5.10.4 De-identifying CCTV footage**

If there is a requirement for a person/people captured on CCTV footage to have their identity removed/blurred/de-identified, the CCTV vendor can be engaged to undertake the task on a 'pay per job' basis, or alternatively it can be done in-house by CSU-IS using a software application such as Adobe Elements or Adobe Premiere Pro.

## **5.11 Criminal or disciplinary discovery**

If during the undertaking of surveillance (whether overt or covert) a reasonable suspicion that a criminal offence or corrupt conduct has occurred, the appropriate authority will be notified.

Subject to any criminal investigation, where disciplinary action against an employee is proposed, the employee and their union and/or legal representatives may be entitled access to a copy of the relevant sections of the recorded CCTV footage where it is to be submitted into evidence. In instances where the CCTV footage relates to alleged criminal proceedings, authority and permission to view or obtain a copy of the data shall be via the lead agency or investigating

authority. Where the matter relates to possible disciplinary action, permission and approval shall be obtained from the Queensland Ombudsman, or authorised officers.

CCTV footage, which may be used as evidence in a court, should be a copy of the original images and be clear and contain a creation date, data and time stamp, proof of non-tamper and verification methodology. Advice should be sought from the relevant law enforcement agency about the proper way to deal with potential evidence.

### **5.12 Storage and disposal of surveillance images**

Overt primary surveillance images are stored for a minimum period of 30 days and a maximum period of 90 days, unless otherwise directed by the Queensland Ombudsman. Images are then overwritten.

The retention period covering an individual piece of CCTV footage depends on the nature of the incident, as well as who has been captured on it. The requestor will ensure that the retention is in accordance with Office recordkeeping policies.

### **5.13 CCTV signage**

CCTV signage will:

- be sited to inform the public that cameras are in operation and promote easy readability
- identify the owner of the CCTV system, including contact details
- be mounted as close as practical to an adult's line of sight. For a standing adult this will be approximately five degrees up or down from a point 1500mm above the ground level in front of the observer (approximately 1700mm above the ground)
- not be placed close to other unrelated signs (i.e. not safety related) which may limit the ability for the information to be processed and understood
- signage will be located to encourage the public to read and recognise the sign
- signs will be regularly inspected for damage and effectiveness by authorised officers and promptly replaced if compromised.

### **5.14 Evaluation**

The CCTV framework/operations should be evaluated every five years to identify whether the purpose is being complied with and objectives are being achieved.

Evaluation of CCTV operations will include:

- assessment of whether CCTV is continuing to meet the purposes of:
  - acting as a deterrent to unwanted behaviour
  - effectively aiding in the monitoring of people, events or activities and assisted in timely and effective response to incidents
  - gathering evidentiary material
- the views of the stakeholders on the operation of the CCTV system
- compliance with the Guideline for the ethical use of the CCTV system, policy/protocols and operating procedures
- reviewing any breaches
- whether or not the CCTV policy and other related documentation requires amendment.

The results of the evaluation will be considered by Corporate Services Unit for future management and functioning of CCTV operations, and to determine funding requirements to undertake any agreed remedial actions.

### 5.14.1 Ongoing monitoring

The Director, Corporate Services Unit, Chief Financial Officer and the Principal Officer – Information Services will regularly monitor and appraise the performance of the CCTV system's surveillance environment to ensure its proper operation and management including:

1. managing and rectifying any issues or concerns from the Building Services Coordinator (BSC) or other stakeholders
2. overseeing the status of current extracted CCTV footage holdings on the system

### 5.15 Public information

The following documents will be available on the internet:

- CCTV system policy and procedures
- Guideline for the ethical use of the CCTV system and forms to access CCTV footage
- Complaint procedures.

## 6. Roles, responsibilities and authorisation

Officer	Responsibilities and authorisation
Queensland Ombudsman	<ul style="list-style-type: none"> <li>• the authorisation of CCTV-related policies, protocols, procedures and forms</li> <li>• the authorisation of modifications, enhancements or other CCTV related initiatives</li> <li>• the delegation of who has authorisation and the level of that authorisation</li> <li>• the delegation of the extraction and handing over of CCTV footage</li> <li>• the authorisation of the viewing of CCTV footage</li> <li>• the viewing of CCTV footage</li> <li>• the viewing of live CCTV footage</li> <li>• the authorisation of covert surveillance</li> <li>• the authorisation of the undertaking of covert CCTV surveillance</li> <li>• the authorisation of the viewing of covert CCTV footage</li> <li>• the authorisation of the extraction and handing over of covert CCTV footage</li> <li>• the definition of covert CCTV footage's expiry date including final destruction</li> <li>• the viewing of covert CCTV footage</li> <li>• the authorisation of images to be identified and/or de-identified</li> <li>• completing Appendix C: Request for recorded CCTV footage</li> <li>• approval of Appendix C: Request for recorded CCTV footage</li> <li>• obtaining encrypted USB for the BSC</li> <li>• liaison with BSC to obtain extracted CCTV footage</li> <li>• organising de-identification of individuals in footage</li> <li>• providing CCTV footage to a member of the public or law enforcement agency authorised to have access to the footage</li> </ul>



<p>Executive Director Corporate Strategy Chief Financial Officer</p>	<ul style="list-style-type: none"> <li>• as delegates of the Ombudsman: <ul style="list-style-type: none"> <li>– the authorisation of modifications, enhancements or the CCTV system</li> <li>– the authorisation of who has authorisation and the level of that authorisation</li> <li>– the authorisation of the extraction and handing over of CCTV footage including identifying and/or de-identifying images</li> <li>– the authorisation of the viewing of CCTV footage</li> <li>– the viewing and searching of stored CCTV footage with the BSC</li> <li>– the viewing of live CCTV footage</li> <li>– the authorisation of images to be identified and/or de-identified</li> <li>– completing Appendix C: Request for recorded CCTV footage</li> <li>– approval of Appendix C: Request for recorded CCTV footage</li> <li>– obtaining encrypted USB for the BSC</li> <li>– liaison with BSC to obtain extracted CCTV footage</li> <li>– organising de-identification of individuals in footage</li> <li>– providing CCTV footage to a member of the public or law enforcement agency authorised to have access to the footage</li> </ul> </li> </ul>
<p>Building Services Coordinator (BSC)</p>	<ul style="list-style-type: none"> <li>• the operation of the CCTV system</li> <li>• the viewing of live CCTV footage</li> <li>• the viewing and searching of CCTV footage</li> <li>• the authorised extraction and handing over of CCTV footage to an authorised Officer defined under this policy</li> <li>• the authorised deletion of CCTV footage</li> <li>• the authorised undertaking of covert CCTV surveillance as approved by the Queensland Ombudsman</li> <li>• the authorised deletion of covert CCTV footage as approved by the Queensland Ombudsman</li> <li>• the authorised viewing of covert CCTV footage as approved by the Queensland Ombudsman</li> <li>• CCTV maintenance and support coordination</li> <li>• advice to agencies during periods when CCTV is not working</li> </ul>
<p>General Counsel</p>	<ul style="list-style-type: none"> <li>• as delegate of the Ombudsman: <ul style="list-style-type: none"> <li>– the authorisation of the extraction and handing over of CCTV footage including identifying and/or de-identifying images</li> <li>– the authorisation of the viewing of CCTV footage</li> <li>– the viewing and searching of stored CCTV footage with the BSC</li> <li>– the viewing of live CCTV footage</li> <li>– the authorisation of images to be identified and/or de-identified</li> <li>– completing Appendix C: Request for recorded CCTV footage</li> <li>– approval of Appendix C: Request for recorded CCTV footage</li> <li>– obtaining encrypted USB for the BSC</li> <li>– liaison with BSC to obtain extracted CCTV footage</li> <li>– organising de-identification of individuals in footage</li> <li>– providing CCTV footage to a member of the public or law enforcement agency authorised to have access to the footage</li> </ul> </li> </ul>
<p>Intake Team staff of the Office of the Queensland Ombudsman Senior Human Resource Officer, Office of the Queensland Ombudsman</p>	<ul style="list-style-type: none"> <li>• the viewing of live CCTV footage on a defined set of CCTV cameras</li> <li>• inspection and maintenance of CCTV warning signs</li> </ul>
<p>Right to Information Officer</p>	<ul style="list-style-type: none"> <li>• completion of Appendix C: Request for recorded CCTV footage form and obtaining approval</li> <li>• obtaining encrypted USB for the BSC</li> <li>• liaison with BSC to obtain extracted CCTV footage</li> <li>• organising de-identification of individuals in footage</li> <li>• providing the footage to the member of the public authorised to have the footage</li> </ul>

<p>Queensland Ombudsman Information Services employees</p> <p>Chief Financial Officer</p> <p>Senior Human Resource Officer, Office of the Queensland Ombudsman</p>	<ul style="list-style-type: none"> <li>• as may be necessary in the undertaking of CCTV system support: <ul style="list-style-type: none"> <li>– the operation of the CCTV system</li> <li>– the viewing of live CCTV footage</li> <li>– the viewing and searching of CCTV footage</li> <li>– the authorised extraction and handing over of CCTV footage</li> <li>– establishing the authorisation of who has authorisation and the level of that authorisation</li> <li>– maintenance, enhancement and support of the CCTV system's technical infrastructure in relation to level 18</li> </ul> </li> <li>• inspection and maintenance of CCTV warning signs</li> <li>• de-identifying images</li> </ul>
<p>Senior Lease Manager, Department of Energy and Public Works</p>	<ul style="list-style-type: none"> <li>• maintenance, enhancement and support of the CCTV system's technical infrastructure on behalf of all tenants from level 17 to 22</li> <li>• cost apportionment of charges relating to maintaining and managing the CCTV system</li> </ul>
<p>CCTV vendor technical support staff</p>	<ul style="list-style-type: none"> <li>• as may be necessary in the undertaking of CCTV system support: <ul style="list-style-type: none"> <li>– the operation of the CCTV system</li> <li>– the viewing of live CCTV footage</li> <li>– the viewing and searching of CCTV footage</li> <li>– the authorised extraction and handing over of CCTV footage</li> <li>– establishing the authorisation of who has authorisation and the level of that authorisation</li> <li>– maintenance, enhancement and support of the CCTV system's technical infrastructure</li> </ul> </li> </ul>

## 7. Definitions

Term	Definition / Explanation / Details
Activities	Workplace operations, processes or functions for the safe and effective delivery of services.
Authorised officer	A person authorised by the Queensland Ombudsman to view, operate the CCTV system, or perform other CCTV-related duties, as defined in 6. Roles, responsibilities and authorisation
Closed Circuit Television (CCTV)	A television system that transmits images on a 'closed loop' basis, where images are only available to those directly connected to the transmission system. The transmission of closed circuit television images may involve the use of coaxial cable, fibre-optic cable, telephone lines, IP networks, infra-red and radio transmission systems.
CCTV footage	Images captured via the CCTV system.
CCTV operations	All aspects of CCTV surveillance management, use, recording, maintenance and access to recorded material.
Covert images and data	Covert surveillance is where: <ul style="list-style-type: none"> <li>• the employees have not been notified before the intended surveillance is conducted</li> <li>• cameras or evidence of their existence are not clearly visible at the workplace</li> <li>• there are no clearly visible signs at the entrance to the workplace to notify people that they may be under CCTV surveillance.</li> </ul>
Incident	Any event or circumstance involving or affecting the individual or organisation that causes or is likely to cause a loss (physical or otherwise), disruption or fear arising from the deliberate activities of other parties. Where impacts are, or could potentially be, realised against people, property or information.
Owner (security)	Is the legal person or entity designated as having overall responsibility for the formulation and implementation of the policies, purpose and control of a CCTV system.

Original images	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.
Primary images	The first instance in which an image is recorded onto any media. The primary image is generally overwritten after a specified period of time, when the footage could be considered to have no further administrative use.
Security	The preparedness, protection and preservation of people, property and information, both tangible and intangible.
Surveillance	Refers to the use of electronic security equipment (closed circuit television or video monitoring) to monitor vulnerable areas.
Working images	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.)
Workplace	A place where work is carried out for a business or undertaking and includes any place where a worker goes, or is likely to be, while at work.

## 8. Authority

*Information Privacy Act 2009*

## 9. Related documents

Standards Australia's CCTV standard AS 4806.1–2006:

- AS 4806.1–2006–Closed circuit television (CCTV)–Part 1: Management and operation
- AS 4806.2–2006–Closed circuit television (CCTV)–Part 2: Application guidelines
- AS 4806.3–2006–Closed circuit television (CCTV)–Part 3: PAL signal timings and levels
- AS 4806.4–2008–Closed circuit television (CCTV)–Part 4: Remote video
- AS 2201.1:2007 - Intruder alarm systems - Client's premises - Design, installation, commissioning and maintenance
- AS/CA S009:2013 – Installation requirements for customer cabling (Wiring Rules)

*Information Privacy Act 2009*

*Public Records Act 2002*

Records Governance Policy April 2019

*Right to Information Act 2009*

*Crime and Corruption Act 2001*

*Security Providers Act 1993*

*State Buildings Protective Security Act 1983*

Queensland Government - Surveillance and monitoring records

<https://www.forgov.qld.gov.au/information-and-communication-technology/recordkeeping-and-information-management/recordkeeping/manage-specific-record-types-and-activities/surveillance-and-monitoring-records>

Queensland's Office of the Information Commissioner Guideline - Camera Surveillance and Privacy [https://www.oic.qld.gov.au/\\_\\_data/assets/pdf\\_file/0010/28099/guideline-camera-surveillance-and-privacy.pdf](https://www.oic.qld.gov.au/__data/assets/pdf_file/0010/28099/guideline-camera-surveillance-and-privacy.pdf)

**10. Approval**

<b>Author:</b>	Richard Bosanquet, CFO
<b>EDCS:</b>	Leanne Robertson
<b>Authorised by:</b>	Angela Pyke, Acting Ombudsman
<b>Authorisation date:</b>	12 December 2022
<b>Review date:</b>	Three years from date of approval (30 November 2025)

**11. Document control**

<b>Version</b>	<b>Edocs Ref</b>	<b>Effective date</b>	<b>Review date</b>	<b>Amendment history</b>
1.0	55392	September 2016	September 2019	Redrafted to reflect CCTV system after move to Level 18.
2.0	88714	October 2018	October 2021	Redrafted after Commonwealth Ombudsman departed tenancy and co-ordination of maintenance of CCTV transferred to Department of Housing and Public Works. Removal of Edward Street corridor camera.
3.0	171421	December 2022	November 2025	Minor changes to titles.

## Appendix A: Guideline for the ethical use of the CCTV system

This guideline has been developed to ensure that the highest ethical standards are maintained by all authorised officers who operate the Level 18 CCTV system.

Authorised officers are staff of the Office of the Queensland Ombudsman (the Office) or other persons, (e.g. CCTV technical support personnel), authorised by the Queensland Ombudsman (Refer CCTV Policy).

### **Non-compliance with the guideline**

CCTV operations require high standards of integrity and honesty. As a consequence, unethical use of the CCTV system could result in disciplinary action as provided for in the Office’s code of conduct.

### **Ethical use of CCTV systems and recorded material**

The Office has the highest expectation of all authorised officers to:

- at all times, act in an honest and legal manner when operating the CCTV system
- treat all live and recorded images in an ethical manner and with the utmost of care, respect and dignity
- interact with all stakeholders in a timely, courteous and cooperative manner.

### **Confidentiality**

The Office expects authorised officers to ensure confidentiality of information gathered by or from CCTV operations by not disclosing or discussing any events with unauthorised personnel or associates who have no direct responsibility relating to CCTV operations.

In addition, authorised officers must not identify any involved person or party with family, friends or acquaintances and must not disclose any information to third parties, including the media, without prior written approval in accordance with CCTV operation policy/protocol.

### **Operating conditions**

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

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

Recorded material must only be released when requested in writing on an approved and authorised application.

Recorded material must not be copied or taken from the CCTV system without an approved written and authorised application.

All copies of recorded material must only be copied or be taken from the CCTV system on an encrypted and/or password protected device.

CCTV operational records (hard copy or electronic) can only be destroyed with written authorisation and in accordance with approved Office recordkeeping policies and procedures.

### **Reporting unethical use of the CCTV system**

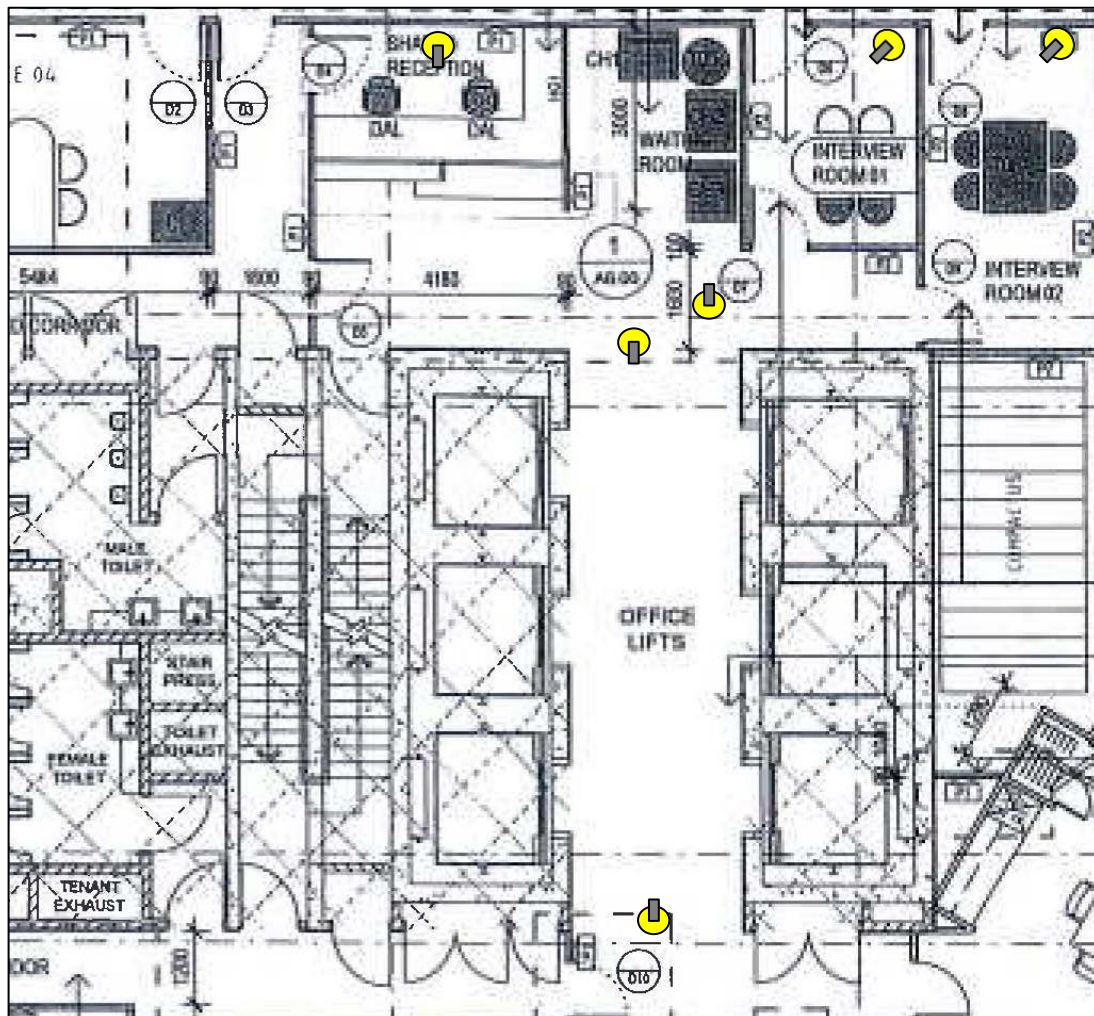
If any person becomes aware that an officer’s or contractor’s work behaviour is or was inappropriate in relation to the Office’s CCTV system policy and procedure the person is obliged to report the incident to their manager or the Queensland Ombudsman.

I have read and understood the CCTV guideline for the ethical use of the CCTV system.

NAME: .....

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

## Appendix B: Level 18 camera locations



## Appendix C: Request for recorded CCTV footage form

<b>Requestor</b>	<b>Name</b>			
	<b>Position</b>			
	<b>Contact number</b>			
	<b>Email address</b>			
	<b>Signature</b>			
<b>Date request lodged</b>		<b>Time request lodged</b>		
<b>Request details:</b>				
<b>Reason for request (e.g. the nature and description of incident)</b>				
<b>Date of footage</b>		<b>Start time</b>		<b>Duration (in minutes)</b>
<b>From an RTI request?</b>		<input type="checkbox"/> Yes <input type="checkbox"/> No	<b>RTI reference:</b>	
<b>Are staff from other agencies or the public likely to be captured on the footage?</b>		<input type="checkbox"/> Yes <input type="checkbox"/> No	<b>Staff likely to be identified:</b> <input type="checkbox"/> Queensland Ombudsman <input type="checkbox"/> Other level 18 agency	<b>De-identification required:</b> <input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Please describe the incident or scenario that you are requesting footage of</b>				
<small>(This will assist the CCTV authorised officer recover the correct footage from the correct camera. However, it is not compulsory to provide this information)</small>				
<b>Please tick the cameras listed that you think cover the footage you are requesting</b>				
<input type="checkbox"/> Level 18 Reception		<input type="checkbox"/> Level 18 Interview Room 1		
<input type="checkbox"/> Level 18 Lift Lobby Edward St		<input type="checkbox"/> Level 18 Interview Room 2		
<input type="checkbox"/> Level 18 Lift Lobby Albert St		<b>Building owner's CCTV system's cameras</b>		
<input type="checkbox"/> Level 17 Data Centre		<input type="checkbox"/> Ground floor foyer		
		<input type="checkbox"/> Goods lift		
<b>Authoriser</b>	<b>Name</b>			
	<b>Position</b>			
	<b>Contact number</b>			
	<b>Email</b>			
	<b>Signature</b>			

Appendix D: **Level 18, 53 Albert Street request for recorded CCTV footage (to be completed by BSC)**

<b>Name of authorised officer making request</b>					
<b>Extracted footage</b>					
<b>Date of footage</b>		<b>Start time</b>		<b>Duration (in minutes)</b>	
<b>Please tick the cameras from which the footage was extracted</b>					
<input type="checkbox"/> Level 18 Reception		<input type="checkbox"/> Level 18 Interview Room 1			
<input type="checkbox"/> Level 18 Lift Lobby Edward St		<input type="checkbox"/> Level 18 Interview Room 2			
<input type="checkbox"/> Level 18 Lift Lobby Albert St		<b>Building owner's CCTV system's cameras</b>			
<input type="checkbox"/> Level 17 Data Centre		<input type="checkbox"/> Ground floor foyer			
		<input type="checkbox"/> Goods lift			
<b>Location of extracted footage</b>					
<b>Location of extracted footage</b>		<b>Workstation footage stored on</b>		<input type="checkbox"/> Ground floor	
				<input type="checkbox"/> 18 <sup>th</sup> Floor	
<b>Name of extracted footage</b>		<b>Snap shots taken?</b> Yes <input type="checkbox"/> No <input type="checkbox"/> If yes, list snap shots taken:			
<b>Footage extraction media</b>		<b>Encrypted</b>		<input type="checkbox"/> Yes	
<input type="checkbox"/> USB <input type="checkbox"/> Other (if other please describe)		<b>Type password:</b>		<input type="checkbox"/> Yes	
		<b>Footage extraction media's name or identifier:</b>			
<b>Agency or Law enforcement agency that extracted footage is being given to:</b>					
<b>Extracted footage receiver</b>		<b>Name</b>			
		<b>Position</b>			
		<b>Contact number</b>			
		<b>Email</b>			
<b>Date extracted received</b>					
<b>Time extracted received</b>					
<b>Signature</b>					