Australian Capital Territory

Corrections Management (CCTV) Operating Procedure 2026

Notifiable instrument NI2026–121

made under the

Corrections Management Act 2007, s14 (Corrections policies and operating procedures).

---

1 Name of instrument

This instrument is the *Corrections Management (CCTV) Operating Procedure 2026.*

2 Commencement

This instrument commences on the day after notification.

3 Operating Procedure

I make this operating procedure to facilitate the effective and efficient management of corrections services.

Leanne Close [APM]
Commissioner
ACT Corrective Services

11 March 2026

OPERATING PROCEDURE	Closed-Circuit Television (CCTV)
OPERATING PROCEDURE NO.	35.1
SCOPE	ACT Correctional Services facilities

PURPOSE

To provide instructions for the monitoring and management of Closed-Circuit Television (CCTV) systems across ACT Corrective Services (ACTCS) correctional centres, facilities, secure escort vehicles and community operations.

PROCEDURES

1. Roles and responsibilities

1.1. The Divisional Executives are responsible for:

a. maintaining and ensuring the security of CCTV systems and video footage in accordance with the *Territory Records Act 2002*

b. ensuring that appropriate signage is on display where CCTV is in operation, according to the *ACT Government CCTV Policy*

c. ensuring that appropriate training in the operation and monitoring of CCTV systems is provided to staff, where required

d. authorising CCTV footage use, and

e. reporting the misuse of CCTV surveillance immediately to the Director, Security and Information Systems for investigation with the relevant Senior Director.

1.2. The Security Systems team is responsible for:

a. maintaining systems

b. managing access

c. processing CCTV footage requests and retention

d. performing audits, and

e. maintaining access registers.

1.3. The vendor maintains the Electronic Security System (ESS), including hardware such as cameras and workstations.

1.4. The Senior Director, Information, Security and Business Solutions, is responsible for ensuring that protective security measures are implemented to protect against unauthorised access, tampering, or disruption of CCTV systems. The Security Systems team will establish physical and electronic security arrangements to protect CCTV systems from unauthorised access or viewing, including appropriate systems to allow authorised individuals to access CCTV footage, and providing the capacity for ACTCS to review and audit CCTV footage access history.

2. Daily operations

2.1. CCTV must operate continuously in designated areas, except escort vehicles when the vehicle is switched off.

2.2. Time/date stamps must be verified daily and discrepancies reported immediately. Footage must be logged with start and end times and location identifiers.

2.3. Cameras must not be obstructed, switched off, compromised or moved in a way that obstructs the line of sight the camera is intended to monitor. Breaches will result in disciplinary action.

2.4. All ESS faults must be recorded, including detailing who was notified, e.g. the Security Systems team or Chubb. The Security Systems team contact is: ACTCSSecuritySystems@act.gov.au or 6207 9390. The Chubb contact details are located at the Alexander Maconochie Centre Gatehouse supervisor's desk.

3. Escort vehicles

3.1. CCTV surveillance in ACTCS secure escort vehicles activates only when the vehicle ignition is turned on.

3.2. The date and time stamp of CCTV in all secure escort vehicles will be checked daily. Any errors or inconsistencies must be reported to the Senior Director, Court Transport Unit (CTU).

3.3. CCTV in CTU escort vehicles is managed by the Security Systems team, with all footage retained and managed exclusively via hard drive-based systems.

3.4. Only approved hardware and software is to be installed into escort vehicles. This includes CCTV cameras. Approvals are via consultation with the Security Systems team, Senior Director Operations and CTU Senior Director.

4. Incident management

4.1. Footage of incidents must include a minimum of 10 minutes of recording, both prior to and after the event.

4.2. Footage related to use of force incidents must be managed in accordance with the *Use of Force and Restraint Operating Procedure*.

4.3. Complaints relating to CCTV surveillance must be managed in accordance with the *Detainee Requests and Complaints Policy* or *Justice and Community Safety Directorate Complaints Management Policy*, as appropriate.

5. Access and review

5.1. Access to the ACTCS CCTV system is restricted to authorised personnel only. Non-operational access (i.e. requests received from the Intelligence Unit, Accommodation, Security, and Operations) requires written approval from a Senior Director or above. Information should only be accessed on a strictly need-to-know basis.

5.2. All requests for access to ACTCS CCTV must be submitted using the *ACTCS CCTV Access Agreement Form* (Attachment A) available from the Security Systems team. The completed

form should be emailed to the relevant Senior Director for review and approval. Once approved, a copy must be forwarded to the Security Systems team to enable access.

5.3. All authorised personnel (except the Master Control Room (MCR) and Operations posts) will have individual logins and credentials that must not be shared.

5.4. Viewing workstations must be in secure, private areas. Access changes must be reported to the Security Systems team and workstations must be logged out or shut down after use.

5.5. CCTV footage may be reviewed for up to 30 days following the date and time the footage was recorded. ACTCS will only guarantee CCTV footage availability up to 30 days.

5.6. CCTV footage handling:

a. storage requirements - footage downloaded for the purpose of approved sharing must only be stored in authorised Justice and Community Safety Directorate (JACS)/ACTCS secure systems, such as the ACTCS Secure Shared Network Drive (G:) or other approved enterprise storage. These systems must enforce role-based access controls, including restricted access groups, audit logs, and prevention of unauthorised copying

b. use of removable media - CCTV footage must not be copied to CDs, USBs, or any removable media unless explicit approval is granted by the Senior Director or Director, Security and Information Systems

c. prohibition on distribution/distributing further - footage must not be distributed further under any circumstances. Distribution includes forwarding, copying, uploading, or sending the footage to any additional parties beyond those originally approved

d. sharing - refers to the controlled release of footage undertaken solely by the Security Systems Unit or Intelligence Unit, and only upon receipt of a valid and approved internal or external request, or where legally compelled (e.g., a subpoena).

5.7. Live viewing is only permitted in the following designated locations:

a. MCR

b. AMC Security Unit

c. Security Systems Unit

d. CTU Control Room, to monitor operational areas for safety and security

e. Intelligence Unit

f. Operations Building, and

g. General Manager's Conference Room.

5.8. Approval for access to review CCTV outside the normal course of duties will be considered by both the Senior Director, Operations and the Director, Security and Information Systems.

5.9. Users must log out once they have finished viewing, monitoring or accessing CCTV footage, and all ACTCS CCTV footage must be securely stored in the ACTCS CCTV Library with restricted access.

5.10. A register of ACTCS staff authorised to access CCTV will be maintained and updated by the Security Systems team.

6. Internal requests

6.1. All requests to download CCTV footage within ACTCS must be made in writing to the Security Systems Unit, Intelligence Unit or the Office of the Commissioner. This includes where footage is requested for training purposes. Any requests must be made by personnel with the appropriate delegation.

6.2. Requests for footage must specify camera locations, dates and timeframes. Early Incident emails are insufficient. The Security Systems team will not research footage requirements. Early Incident emails are insufficient.

6.3. The Security Systems team takes no responsibility for missed footage that might be required at a later date. It is the requestor's responsibility to ensure all footage required is retained.

7. External requests

7.1. The following table indicates where external requests for CCTV footage are to be directed to. All relevant areas within ACTCS will manage requests in consultation with the Director, Security Systems**,** for decisions on if, and how, information can be released**.**

Request relating to:	**Contact:**
A correctional centre	Security Systems team
Community Corrections	Security Systems team
ACT Policing	Intelligence Unit, via ACTCS-Intelligence@act.gov.au
Subpoena	Litigation team
Freedom of Information	Ministerial Support Unit, via ACTCSCommissionersOffice@act.gov.au
All other enquiries	Director, relevant area within ACTCS

8. Data handling and retention

8.1. CCTV, including media files (photographs or hand-held footage), must not be shared via unapproved mechanisms. CCTV footage must not be downloaded or stored, including on G:\ or H:\ Drives, without prior approval.

8.2. The retention period for requested CCTV footage is seven (7) years in accordance with the *Territory Records Act 2002*.

8.3. CCTV and video camera footage related to offender management must be retained for a period of seven (7) years for the following matters:

a. incidents where further action is taken within 12 months (*Incident Reporting, Notifications and Debriefs Policy*)

b. use of force (*Use of Force and Restraints Policy*), or

c. as directed by a Divisional Executive.

8.4. Footage must still be retained where cameras are knowingly covered or blocked, as this may be considered evidentiary footage.

8.5. All requests to retain footage must be in writing to the Security Systems team and the Intelligence Unit. Area Managers, Directors (Intelligence Unit, Community Operations and Litigation Unit) and above are authorised to request footage retention.

8.6. CCTV retention requests must clarify who is requesting the footage, and what CCTV is required.

8.7. The Security Systems team will not over-ride any footage. In line with review and retention practices, footage that is no longer required will be deleted after checks are conducted and logged in the deletion register. If increased storage for files is required, they will liaise with Digital Canberra and the Senior Director, Information, Security and Business Solutions Unit, for approval before purchasing more.

8.8. Disposal is overseen by the Senior Director, Information, Security and Business Solutions Unit. This includes the disposal of governance records, for example, title of footage, checks with ACTCS Litigation team, date of disposal.

9. Training

9.1. Officers will complete MCR training, which involves CCTV operation. This includes incident response procedures and on-the-job learning during placement sessions in the MCR.

9.2. New officers are also required to complete mandatory induction courses on security awareness, JACS procedures, fraud and ethics. These courses include privacy obligations and relevant legislation.

9.3. The mentoring of officers in the MCR will be undertaken by an experienced operator, designated by the Senior Director, Operations, to ensure relevant information is consistently covered and understood.

9.4. The relevant Divisional Executive can authorise the use of CCTV footage for training purposes where appropriate and with consideration of privacy, human rights and dignity of staff, offenders and community members, and learning outcomes for using CCTV. The authorisation should provide a clear understanding of what the approval is for.

10. Compliance

10.1. The Director, Security and Information Systems will ensure that an audit of CCTV systems is undertaken at least annually.

10.2. User access reviews are conducted tri-monthly, as requested by JACS Chief Information Officer Branch.

10.3. CCTV access and usage audits are led by the Director, Security and Information Systems, or delegate. Anomalies must be reported to the Senior Director, Information, Security and Business Solutions, and to the Assistant Commissioner, Custodial Operations or relevant Divisional Executive.

10.4. Unauthorised sharing or storing of media files is strictly prohibited, this includes Audio, Video or Images, and subject to disciplinary action.

11. Hand-held camera footage

11.1. The *Hand-Held Video Cameras Operating Procedure* outlines the operational requirements for hand-held video cameras.

11.2. Hand-held camera footage is subject to the same operational and access controls as fixed CCTV systems. Only ACTCS correctional officers are authorised to operate hand-held cameras.

11.3. All footage must be downloaded and stored exclusively by the Security Systems team.

11.4. Following any incident involving the use of a hand-held video camera, Security Unit Officer, Officer in Charge (OIC), or Incident Commander if appointed, must ensure the camera is provided to the Security Systems team within two (2) business days, to be downloaded and logged.

11.5. The Security Systems team will then download and retain in the CCTV library and delete the footage from the camera. Removal or deletion of footage must comply with access controls and retention standards. Hand-held camera footage is retained and disposed of in accordance with the same retention timeframes and disposal procedures as CCTV footage.

12. Use and records management

12.1. In addition to the purpose for CCTV surveillance, CCTV footage and hand-held camera footage:

a. can be considered admissible as evidence

b. may be provided to ACT Policing or other authorised parties under this policy, the *ACT Government CCTV Policy* or *Freedom of Information Act 2016*, and

c. may be used for investigative purposes.

12.2. The Director, Security and Information Systems, will maintain a register for all downloaded and retained imagery that includes the logged start and end time, date and location of the footage.

12.3. The Security Systems team, the Intelligence Unit and the Office of the Commissioner must maintain registers regarding requests for CCTV footage from external agencies.

12.4. The Security Systems team register must include the date, time, requestor and footage provided/shared or retained etc. Written requests and approvals must also be retained.

12.5. Reviewing registers is part of the compliance review process. The Directors and Security Systems team review all CCTV logs, registers etc. including details of:

a. the requesting agency/entity

b. the reported purpose of the request and the details of the requested footage

c. if the footage was provided, the request date and the date the footage was provided.

RELATED DOCUMENTS

- ACT Corrective Services CCTV User Acceptance Form
- ACT Government CCTV Policy
- ACT Government Protective Security Framework
- ACT Public Sector Workplace Privacy Policy 2024
- CCTV Policy

- Corrections Management Act 2007
- Detainee Requests and Complaints Policy
- Freedom of Information Act 2016
- Human Rights Act 2004
- Incident Reporting, Notifications and Debriefs Policy
- Information Privacy Act 2014
- JACS Care and Custody of Assets Standard Operating Procedure
- JACS CCTV Governance Policy
- JACS Complaints Management Policy
- JACS Privacy Policy
- JACS Records and Information Management Standard Operating Procedure
- Privacy Act 1988 (Cth)
- Territory Records Act 2002
- Use of Force and Restraint Operating Procedure
- Use of Force and Restraint Policy
- Workplace Privacy Act 2011.

Cherry Wang
A/g Executive Branch Manager, Corporate Services
ACT Corrective Services
6 March 2026

Document details

Criteria	Details
Document title:	*Corrections Management (Closed-Circuit Television) Operating Procedure 2026*
Document owner/approver:	Executive Branch Manager, Corporate Services, ACT Corrective Services
Date effective:	The day after the notification date
Review date:	One (1) year after the notification date. The standard five (5) years review date is too infrequent given the pace of technological and legal change in this area.
Responsible Officer:	Senior Director, Information, Security and Business Solutions
Compliance:	This operating procedure reflects the requirements of the *Corrections Management (Policy Framework) Policy 2024*

Version Control			
Version no.	**Date**	**Description**	**Author**
V1	March-26	First Issued	A Clarke

ACT CORRECTIVE SERVICES CCTV USER ACCEPTANCE FORM

This form must be completed by any ACT Corrective Services (ACTCS) staff member requesting individual login access to the CCTV system.

USER DETAILS

Name: _____

Position Title: _____

Business Unit: _____

Contact Number: _____

Email Address: _____

ROLE JUSTIFICATION

Briefly justify your need for CCTV access and activities (e.g., live monitoring, footage review):

_____

_____

USER RESPONSIBILITIES

- Do not share login credentials under any circumstances.
- Use CCTV only within the scope of your professional role.
- All CCTV activities must be lawful and auditable.
- Report any misuse or unauthorised access to Security Systems.
- Understand that misuse may result in disciplinary action and breach of legislation.

RELEVANT LEGISLATION

- *Workplace Privacy Act 2011 (ACT)* – governs workplace surveillance and requires formal notification to staff.
- *Information Privacy Act 2014 (ACT)* – mandates secure handling of personal information, including CCTV footage.

- Australian Privacy Principles (APPs) under the *Privacy Act 1988 (Cth)* – apply to the collection, use, and disclosure of personal information.

DECLARATION: I have read and understand the CCTV Policy and CCTV Operating Procedure, and accept the responsibilities associated with accessing the ACTCS CCTV system.

Staff Signature: _____

Date: _____

***Please forward the completed and signed form via email to your Senior Director for review, and ensure the Security Systems team is copied into the email to support efficient processing**

Senior Director Name: _____

Signature: _____

Date: _____

Security Systems Team

Decision and reason for decision (i.e. access necessary for role):

_____

_____

Staff Name: _____

Staff Signature: _____

Date: _____