CCTV Policy

ARV Corporate Policy

1. Statement

The purpose of this policy is to establish a transparent, accountable, and legally compliant framework for the deployment, operation, and oversight of CCTV (Closed-Circuit Television) video camera surveillance systems at ARV, ensuring they are used solely to enhance community safety, deter unlawful behaviour, enforce regulatory compliance, and protect assets, while respecting the privacy, dignity, and rights of all individuals.

This policy draws on Department of Justice and Regulation's *Guide to developing CCTV for public safety in Victoria* and the Commissioner for Privacy and Data Protection's *Guidelines to surveillance and privacy in the Victorian public sector* best practice guidelines to balance crime prevention and compliance objectives with robust privacy safeguards.

2. Scope

This policy applies to all workplace participants at ARV, and all CCTV systems owned or operated by ARV.

The following types of systems are considered CCTV systems under this Policy:

- Security cameras.
- Webcams which publish images to public-facing ARV websites.
- Licence Plate Recognition (LPR) camera systems.
- Environmental and wildlife monitoring cameras.

3. Requirements

Policy Principles and Lawful Basis

ARV's use of CCTV systems is governed by the following principles: necessity, proportionality, purpose limitation, data minimisation, transparency, security, and accountability.

CCTV must only be used for the legitimate purposes outlined in this Policy and must comply with the *Privacy and Data Protection Act 2014 (Vic)*, the *Charter of Human Rights and Responsibilities Act 2006 (Vic)*, and ARV's Information Security policies.

Any collection, use, disclosure and storage of personal information captured by CCTV must be limited to what is reasonably necessary to achieve the stated purposes and must be secured commensurate with the information's Business Impact Level (BIL).

Establishment of a CCTV Working Group

The Corporate Services General Manager or their delegate is to establish and chair a CCTV working group. The advisory working group is charged with the responsibility of ensuring the management and use of ARV CCTV systems comply with all relevant legislation, corporate policies, and standard operating procedures. The working group will include interested members of the ARV Consultative Committee and other relevant staff.

ARV is required to establish a CCTV steering committee or similar working group before entering into a memorandum of understanding (MOU) or to develop a CCTV Program or Register in collaboration with Victoria Police.

Prohibited Practices and Placement Controls

ARV strictly prohibits any type of:

- CCTV in private areas such as bathrooms, change rooms, nappy change areas, and other places where individuals have a high expectation of privacy.
- CCTV audio recording, unless expressly authorised by law, approved by the Corporate Services General Manager, and following a Privacy Impact Assessment (PIA).
- Covert CCTV surveillance, except where undertaken by law enforcement under lawful authority and in accordance with the *Surveillance Devices Act 1999 (Vic)*.

Camera placement must be fit-for-purpose and avoid unjustified surveillance of private premises.

New camera locations are approved in writing by the relevant General Manager of the work centre and recorded in the CCTV Camera Location Register by the ICT team.

CCTV Standard Operating Procedures (SOP) Manual

The Corporate Services General Manager is to publish an internal Standard Operating Procedures (SOP) manual to provide technical instructions for the operation and maintenance of ARV CCTV systems. The SOP is to be issued to workplace participants who will use and access ARV CCTV systems.

Australian Standard AS4806.1-2006 *Closed circuit television (CCTV) – Management and Operation* provides further standards for the management and operation of CCTV systems.

Signage and Public Notices

ARV will ensure conspicuous signage is displayed at entrances to CCTV-monitored areas and, where practicable, within the camera field of view. Signage notices must state:

- The purpose(s) of monitoring.
- Advise that ARV is the data custodian.
- A reference to the ARV CCTV Policy (published on ARV's corporate website).
- Contact details for enquiries.

Model wording:

> *"This area is under CCTV surveillance for safety, asset protection and compliance purposes. Footage is managed by Alpine Resorts Victoria in accordance with the ARV CCTV Policy and the Privacy and Data Protection Act 2014 (Vic). For more information visit www.alpineresorts.vic.gov.au/privacy For enquiries email info.<resortname>@alpineresorts.vic.gov.au."*

Data Lifecycle, Classification, Retention and Disposal

CCTV recordings are public records and must be created, captured, stored, retained, and disposed of in accordance with the *Public Records Act 1973 (Vic)* and ARV's Records Management Policy.

- Classification and access: All recordings must be classified according to their sensitivity and assigned a Business Impact Level (BIL). Access controls must align with ARV's Information Security and Records Management policies.
- Default retention: Routine CCTV recordings are to be retained for the shortest period necessary (typically 6 months), unless extended for a lawful reason.
- Extension triggers: Retention must be extended where recordings are reasonably likely to be required for an incident investigation, complaint, legal matter, FOI request, or integrity review.
- Disposal: When retention periods expire, recordings must be securely deleted or destroyed.

Workplace Participant Training and Access

Access to CCTV systems is role-based and granted strictly on a need-to-know basis. A matrix of which roles can access which sets of cameras is detailed in the CCTV Standard Operating Procedures (SOP) manual.

Authorised staff may access CCTV only after a valid National Police Check and Victorian Employee Working with Children Check are recorded on their personnel file. Induction training is required before access, with annual refresher training thereafter.

Reviewing live "real time" images is only for the purposes of operational need and incident response. Live images are to be viewed only on a lockable end user device. Use of "TV monitors" or similar control room setup running live feeds continuously is not permitted.

Accessing previously recorded footage by ARV workplace participants is only for the purposes of reviewing operational incidents, law enforcement, OHS, integrity or P&C investigations, and must follow the ARV Incident Management Procedure and relevant P&C policies.

FOI Disclosures to Individuals

Disclosures of CCTV footage to individuals is handled under the Information Privacy Principles and *Freedom of Information Act 1982 (Vic)* process. Decisions and artefacts are recorded in the CCTV Request/Disclosure Log.

Disclosures to Law Enforcement

Disclosures of CCTV footage to law enforcement is only upon written request, lawful authority, or warrant. Decisions and artefacts are recorded in the CCTV Request/Disclosure Log. Law enforcement requests are managed in line with existing MOUs with Victoria Police, where applicable.

Where ARV operates CCTV on licensed premises subject to a security-camera licence condition under section 18B of the *Liquor Control Reform Act 1998*, ARV must:

- Verify authority (Police ID or Licencing Inspector credentials) and log the request in the CCTV Disclosure/Request Log.
- Provide copies of recordings to Victoria Police or a Licensing Inspector on request, in line with the Act and the Regulations standards of frame rate (Reg 8 continuous ≥8 fps) and minimum image quality (Reg 9).
- Export securely, maintain chain-of-custody, and apply a legal hold until the matter is resolved.
- Treat any other Victoria Police requests outside liquor-licence scope under the general law-enforcement disclosure requirements, or ARV's VicPol MOUs where applicable.

CCTV Systems Security and Controls

The ICT team are to implement minimum security controls for ARV CCTV systems aligned to the Victorian Protective Data Security Standards (VPDSS) and ARV's Information Security policies:

- Identity and access to CCTV systems are managed through unique accounts, following the principle of least privilege, and utilising multi-factor authentication where supported. Elevated access is granted only for limited times and is subject to periodic review.
- Protective controls are in place, including encryption of data both at rest and in transit wherever possible. Any exports from the system are to be securely processed, such as by applying watermarks or hashes where possible, and uncontrolled USB exports are disabled. Administrative interfaces are hardened, and secure configurations are maintained.
- Physical security measures include housing recording equipment and switching devices in secure areas, and adhering to the ARV Physical Access Security Policy.
- Monitoring and logging are performed regularly, with system health checks, audit logs capturing all access and export activity, and exception reports reviewed.
- Change management and patching involve applying vendor updates and security patches through a controlled process, with any vulnerabilities tracked until remediation.

Incident Management and Data Breach

Loss, unauthorised access, unauthorised disclosure, compromise, or suspected compromise of ARV CCTV systems or recordings is a cyber incident. Workplace participants must immediately report the incident according to the ARV Cyber Incident (Data Breach) Response and Notification Policy.

Change Management, PIA, and Procurement

Any new substantial CCTV deployment or material change (eg, analytics, hosting, integration, relocation) requires:

- A Privacy Impact Assessment (PIA).
- Appropriate stakeholder consultation.
- Procurement and vendor due diligence (data location, subcontractors, support SLAs, incident/breach notification, exit/deletion).

Child Safety Guardrails

CCTV in ARV-managed toboggan parks, Buller Airzone, and Falls Creek Early Childhood Education and Care settings must uphold the best interests, safety, and wellbeing of children and comply with ARV's Child Safety & Wellbeing Policy, and all relevant ECEC legislation and regulations. Surveillance must be necessary, proportionate and transparent, and must never be covert.

Parents/guardians may request footage under FOI that relates to their child only. ARV may apply redaction/blurring to protect the privacy of other children and workplace participants.

Machine-Vision Analytics and Biometrics Guardrails

Machine-vision video analytics (eg, motion detection, object counting, occupancy analytics, event descriptors) may be used only to support the purposes in this Policy. Licence Plate Recognition (LPR) is detailed in section 4 of this Policy.

Biometric identification (eg facial recognition) and inference analytics (eg emotion, demographic attribution) are prohibited and are not to be used in ARV CCTV systems.

CCTV Systems Decommissioning and Asset Disposal

Before decommissioning any CCTV camera, NVR or storage media, the ICT team must:

- Confirm final retention/disposal authority with the Information and Records Officer.
- Arrange the secure erasure/sanitisation of storage media.
- Update the CCTV Camera Location Register.
- Arrange for the removal or updating of related signage.

4. Specialty CCTV System Governance

Licence Plate Recognition (LPR) Cameras

LPR systems are limited to resort entry compliance, capacity/traffic management, and other enforcement consistent with ARV's regulatory and operational functions. Requirements include:

- Signage that clearly alerts drivers to LPR use and its purposes.
- Evidence handling procedures to support infringements and appeals.
- Retention aligned to infringement and review cycles, extended for appeals/disputes and then disposed of per PROV standards.
- Restrictions on secondary use, including no routine person-tracking or unrelated profiling.

Where third parties supply, host or support LPR systems, vendor contracts must include:

- Data location and sovereignty.
- Information security and privacy obligations (aligned to VPDSS).
- Audit rights and cooperation.
- Incident/breach notification SLAs.
- Support and patching commitments.
- Secure data return/erasure at contract end.

Environmental and Wildlife Monitoring Cameras

Environmental and wildlife monitoring cameras are considered CCTV systems under this Policy and must comply with the same governance, security, and privacy principles. Additional requirements apply:

- Purpose limitation: Cameras may only be used for ecological monitoring, research, or environmental management purposes, and approved in writing by a Resort General Manager.
- Positioning: Cameras must be installed to minimise incidental capture of individuals. Where unavoidable, signage must be placed at access points to inform the public of monitoring activities.
- Data handling: Images and recordings are classified as public records and must be retained and disposed of in accordance with ARV's Records Management policies and PROV Standards.
- Access and disclosure: Access is restricted to authorised personnel or research partners under formal agreements. Any secondary use (eg marketing, publishing datasets to Data Vic) requires review and approval by a General Manager.
- Compliance: Deployments must align with relevant wildlife permits, protected areas, and research ethics approvals.

Webcams

ARV webcams provide environmental imagery (eg, weather, snow conditions) for visitor information and safety. They are not intended to identify individuals and must comply with this CCTV Policy and the *Privacy and Data Protection Act 2014 (Vic)*.

Webcams are to be configured to provide wide environmental scenes, with no audio, and minimal retention (extended only for incidents or legal reasons). ARV webcams are only to be published to ARV websites, or to approved third party platforms under contract.

5. Responsibilities

Position	Responsibility
Corporate Services General Manager	Establish CCTV working group. Publish the internal CCTV Standard Operating Procedures (SOP) manual.
CCTV working group	Cross-functional oversight, review material changes to the SOP manual and advise on staff and community impacts.
Head of Information and Communications Technology (ICT)	Overall CCTV systems governance, alignment with VPDSS/PROV requirements, and cyber security oversight.
ICT team (Officers, Engineers)	Oversee trades installation of approved CCTV cameras. Maintain the CCTV Camera Location Register, user access, signage requirements, perform local checks, coordinate equipment repairs, and equipment disposal. Applies per-camera retention settings.
Information and Records Officer	Provides record disposal authority advice.
Head of Governance and Risk	Manage individual FOI access/correction requests. Manage privacy complaints.
Resort General Manager	Approves new camera locations. Approves environmental/wildlife monitoring camera programs.

6. Legislation

- *Charter of Human Rights and Responsibilities Act 2006*, sections 7, 13
- *Evidence Act 2008*
- *Freedom of Information Act 1982*
- *Liquor Control Reform Act 1998* section 18B
- *Liquor Control Reform Regulations 2023* sections 8, 9
- *Privacy and Data Protection Act 2014* (Vic)
- *Public Records Act 1973*
- *Surveillance Devices Act 1999*

7. Related Documents

- Community Crime Prevention Unit (2018). *Guide to developing CCTV for public safety in Victoria*. Department of Justice and Regulation. https://www.crimeprevention.vic.gov.au/resources/cctv/guide-to-developing-cctv-for-public-safety-in-victoria
- Office of the Commissioner for Privacy and Data Protection (2017). *Guidelines to surveillance and privacy in the Victorian public sector*. Commissioner for Privacy and Data Protection. https://www.crimeprevention.vic.gov.au/resources/cctv/guidelines-to-surveillance-and-privacy-in-the-victorian-public-sector
- Australian Standard AS4806.1-2006 Closed circuit television (CCTV)
- ARV Incident Management Policy
- Physical Access Security Policy
- BP.IT.4.-Policy-Cyber Incident (Data Breach) Response and Notification Policy (updated)
- Records Management Policy

8. Definitions

For the purposes of this policy, the following definitions apply:

Term	Definition
Business Impact Level (BIL)	A rating that indicates how critical information or systems are to the organisation, guiding the level of security and protection required.
CCTV system	Closed-Circuit Television system. This includes any physical element of a video surveillance system. It generally consists of several main assets, such as cameras, relay systems like cabling or wireless antennas, video data storage, and viewing devices.
LPR system	Licence Plate Recognition system. A specialty CCTV system primarily used for the purposes of enforcing vehicle resort vehicle entry permits under the *Alpine Resorts (Management) Regulations 2020*.
Personally Identifiable Information (PII)	Information that can be used to identify an individual, such as a name, address, date of birth, or identification number.
Public record	Any document, data, or information created or received by a Victorian public sector agency in the course of its official duties, which must be managed and retained according to the *Public Records Act 1973 (Vic)*.
Workplace participant	Any member of the Alpine Resorts Victoria board, executives, managers, employees, contractors, volunteers, students on work-placement, and other personnel at workplaces under the management or control of ARV.

9. Approval and Implementation

Policy Custodian	Policy contact details	Approval Date	Approver
Head of Information and Communications Technology (ICT)	policyregister@alpineresorts.vic.gov.au	6/11/2025	Corporate Services General Manager

10. Version Control

Version Number			
Document Reference:	ARV-CORP-ICT-0085	**Policy Custodian:**	HoICT
Approved By:	GMCS	**Approval Date:**	6/11/2025
Last Amended:	Nov 2025	**Next Review Date:**	Nov 2028

Comments:

This policy replaces the Southern Alpine RMB Workplace Surveillance Policy 2022.