

CALIFORNIA

AUTOMATED LICENSE PLATE READER (ALPR) CAMERA USAGE AND PRIVACY POLICY

Morada Area Association

Policy Number	2026-1
Effective Date	September 1, 2026
Last Reviewed	September. 1, 2026
Next Scheduled Review	September 1, 2027
Policy Custodian / ALPR Administrator	Gordon Rupp, Traci Lowery, and Temple Gallagher
Approved By	Morada Area Association
Legal Authority	<i>Cal. Civil Code §§ 1798.90.5–1798.90.55 (SB 34); Cal. Penal Code § 637 et seq., as applicable</i>

- Morada Area Association representatives, currently: Gordon Rupp, MAA Area Rep, Traci Lowery, MAA President, and Temple Gallagher, MAA Treasurer and Neighborhood Watch Coordinator - full administrative access for system maintenance, user provisioning, and audit functions;

Access requests must be submitted in writing to the ALPR Administrator, identify the requestor's job title and operational need, and be approved before credentials are issued. Access is reviewed at least annually; Access is revoked immediately upon separation, reassignment, or a change in responsibilities that eliminates the operational need.

2.3 Training Requirements

Before receiving access, all authorized personnel must complete initial ALPR training covering:

- The requirements of this policy and applicable state and federal privacy law, including Cal. Civil Code §§ 1798.90.5–1798.90.55;
- Authorized and prohibited uses of ALPR technology and data;
- Proper system operation, query documentation, and hot-list verification procedures; and
- Consequences of policy violations, including discipline and potential personal civil liability under Cal. Civil Code § 1798.90.54.

Refresher training is required at least every 24 months, and immediately following any material change to this policy, applicable law, or the ALPR system. The Agency maintains records of training, including dates and topics covered, for a minimum of 4 years.

3. How the System Will Be Monitored

3.1 Continuous Use Logging

The ALPR system automatically logs every query, alert, and record access, capturing at minimum: the user ID of the person accessing the system, the date and time of access, the specific plate or data queried, and the stated purpose of the query. Logs are immutable and cannot be edited or deleted by end users.

3.2 Supervisory and Administrator Review

- The MAA primary Flock Administrator reviews a sample of ALPR queries made by staff under their supervision on a monthly basis to confirm each query matches an authorized purpose;
- The MAA ALPR Administrator reviews system-generated exception reports (e.g., unusually high query volumes, out-of-jurisdiction searches) and follows up on anomalies within 10 days;
- Any suspected misuse is escalated immediately to the MAA president and affiliated Agency leader for investigation under Section 7.3.

3.3 Periodic Compliance Audits

The ALPR Administrator conducts a formal audit of the ALPR system at least annually (and more frequently if warranted). Each audit documents and verifies:

- That access is limited to currently authorized agencies and job titles identified in Section 2;

- That a representative sample of queries were made for an authorized purpose and properly documented;
- That data sharing during the audit period complied with Section 4;
- That retention and destruction practices complied with Section 6; and
- Corrective actions taken in response to any deficiencies identified.

A written summary of each audit is retained by the MAA ALPR Administrator and made available to Morada Area Association Board of Directors and, upon request, to the public consistent with the California Public Records Act.

4. Data Sharing, Access, and Accuracy Controls

4.1 Data Sharing Restrictions

- ALPR information shall never be sold.
- ALPR information shall not be shared with private persons or private entities, except as required to respond to a valid subpoena or court order.
- ALPR information shall not be shared with federal agencies or out-of-state or out-of-jurisdiction law enforcement agencies for the purpose of civil immigration enforcement.
- ALPR information may be shared with other California public agencies only where: (1) the requesting agency has an authorized purpose consistent with Section 1; (2) the request and purpose are documented in writing; and (3) the receiving agency agrees in writing to comply with restrictions at least as protective as this policy.
- All sharing requests, approvals, and denials are logged by the ALPR Administrator and included in the periodic audit described in Section 3.3.

4.2 Access Controls

- Each authorized user is issued a unique login credential; shared or generic accounts are prohibited;
- Multi-factor authentication is required for all system access;
- System access is role-based and limited to the functions necessary for the user's job title, consistent with Section 2.2;

4.3 Accuracy Controls

- Hot lists and reference databases used for alert comparison are updated at least [daily] and sourced only from authoritative databases (e.g., NCIC, CLETS, DOJ);
- No enforcement action (e.g., vehicle stop) may be initiated on the basis of an ALPR alert alone; personnel must independently visually verify the plate match before taking action;

5. Security Procedures and Practices

5.1 Administrative Safeguards

- All personnel sign a confidentiality/acceptable-use agreement before receiving credentials;
- Vendor and third-party service contracts require compliance with Cal. Civil Code §§ 1798.90.5–1798.90.55, prohibit the vendor's independent use of ALPR data, and require the vendor to notify the Agency of any actual or suspected security incident within 48 hours.

5.2 Technical Safeguards

- ALPR data is encrypted in transit and at rest using industry-standard encryption (e.g., AES-256 / TLS 1.2+);
- ALPR data is stored on cloud servers located within the United States; offshore storage or processing is prohibited.
- Network segmentation, firewalls, and intrusion detection/prevention systems protect ALPR infrastructure from unauthorized access as provided by Flockk Safety;
- Software and firmware are kept current.
- Automated alerts notify the ALPR Administrator of failed login attempts, unauthorized access attempts, or other anomalous system activity.

5.3 Physical Safeguards

- No physical records or equipment is downloaded or kept by MAA.
- Camera hardware is mounted and secured to elevated poles to prevent tampering, theft, or unauthorized repositioning;
- Portable storage media containing ALPR data is prohibited unless expressly authorized and encrypted.

5.4 Security Incident and Breach Response

Any suspected or confirmed unauthorized access to, or disclosure of, ALPR information is reported to the appropriate law enforcement agency immediately upon discovery. The ALPR Administrator documents the scope, cause, and remediation of each incident and reports findings to MAA Board of Directors within 30 days.

6. Data Retention

Except as described below, ALPR information is retained for a default period of 30 days from the date of collection, after which it is automatically archived or deleted from MAA systems and vendor-hosted environments.

Data Type	Retention Period	Notes / Justification
Routine (non-alert) ALPR reads	30 days	Default retention absent an investigative hold

Data Type	Retention Period	Notes / Justification
Data linked to an active investigation	Duration of investigation + 1 year	Requires documented investigative hold approved by Detective or Dept. Manager
Data subject to litigation hold / public records request	Until hold released	Coordinated with legal counsel / records custodian
System access and audit logs	2 years	Retained separately from ALPR read data for audit purposes
Downloaded / exported ALPR data (e.g., case exhibits)	Per applicable records retention schedule	Governed by case file retention policy, not this default

6.1 Destruction Process

- Retention periods are enforced automatically by the ALPR system.
- Before destruction, the system verifies that the data is not subject to an active investigative hold, litigation hold, or public records request;
- Destruction is enforced automatically by the ALPR system;
- Data subject to an investigative or litigation hold is reviewed at least quarterly to determine whether continued retention remains necessary; holds are released and the data destroyed once no longer required.

7. Policy Administration

7.1 Public Availability

Consistent with Cal. Civil Code § 1798.90.51(c), this policy is available in writing on the Agency's website (MoradaAreaAssociation.com) and is available in writing upon request.

7.2 Right of Action and Enforcement

Individuals who believe this policy or applicable law has been violated may have a right of action under Cal. Civil Code § 1798.90.54. Agency personnel who violate this policy are subject to discipline up to and including termination, and may be individually liable under applicable law.

7.3 Complaints and Investigations

Complaints regarding ALPR use may be directed to the Morada Area Association or Flock Safety. Complaints are logged, investigated, and resolved within 30 business days, with findings documented and retained consistent with Section 6.

7.4 Policy Review

This policy is reviewed at least annually by the ALPR Administrator and updated as needed to reflect changes in technology, operational practice, or applicable law, including Cal. Civil Code §§ 1798.90.5–1798.90.55 as amended.

Revision History

Version	Date	Description of Change	Approved By
1.0	9-1-26	Initial policy adoption	MAA BOD

Approval

This policy has been reviewed and approved for adoption by the Morada Area Association

 9/1/26
Traci Lowery, MAA President Date: 9/1/2026

 9/1/2025
Ryan Gresham, MAA Vice President Date: 9/1/2026

 9/1/26
Temple Gallagher, MAA Treasurer Date: 9/1/2026

 09-01-2026
Gordon Rupp, MAA Area Representative Date: 9/1/2026

Note: This document approved by a vote of the Morada Area Association Board