



CITY OF MARICOPA POLICE DEPARTMENT

OPS 2.70

AUTOMATED LICENSE PLATE READERS (ALPR)

08/25/2026

Purpose and Scope

Automated License Plate Reader (ALPR) technology provides automated detection of license plates and associated vehicle characteristics visible from public roadways. The Maricopa Police Department uses ALPR technology only for official and legitimate law enforcement and public-safety purposes, including identifying stolen or wanted vehicles and plates; locating missing, endangered, or wanted persons; gathering information related to active warrants; recovering stolen property; supporting suspect identification and interdiction; canvassing crime scenes; and conducting authorized criminal investigations and crime-suppression activities.

ALPR information is an investigative lead and shall not, by itself, establish reasonable suspicion or probable cause. Access to ALPR equipment, data, alerts, and administrative functions is governed by this policy, applicable law, City requirements, and authorized agreements.

Administration of the ALPR Program

The Chief of Police shall designate a Police Commander as the ALPR Program Manager. The Program Manager is responsible for program oversight, equipment and vendor coordination, system configuration, data retention, access controls, data-sharing settings, audit compliance, and assignment of one or more trained ALPR administrators.

Administrator permissions shall be limited to the minimum number of personnel whose assigned duties require that level of access. Administrator access shall not be granted based solely on rank, supervisory status, or convenience. Non-MPD personnel shall not receive administrator access unless specifically authorized in writing by the Chief of Police or designee and supported by a current agreement or documented operational need.

Training and User Authorization

No person shall operate ALPR equipment, access ALPR data, create or manage a hotlist entry, or perform an ALPR search without department-approved training and an individually assigned account. Users shall receive training on authorized and prohibited uses, required documentation, alert verification, privacy and civil-rights protections, data sharing, information security, auditing, and reporting suspected misuse.

- Shared accounts and credential sharing are prohibited.
- Multi-factor authentication shall be used when supported by the system and required for all administrator accounts.
- Access and permissions shall be based on assignment and job function and shall reflect the user's current duties.
- Users shall complete refresher training when material policy or system changes occur and as otherwise directed by the Program Manager.

Authorized Operation and Search Documentation

An ALPR may be used in conjunction with a patrol operation, active incident, authorized criminal investigation, missing-person investigation, crime-scene canvass, or other official law enforcement activity. Reasonable suspicion or probable cause is not required to view or query ALPR information;



CITY OF MARICOPA POLICE DEPARTMENT

OPS 2.70

AUTOMATED LICENSE PLATE READERS (ALPR)

08/25/2026

however, every access or search must have a specific, articulable connection to an authorized law enforcement purpose.

Required Search Entries

Before conducting a search, the user shall accurately enter all information required by the ALPR system, including:

- The complete and valid MPD Department Report (DR) number in the Case Number field.
- The applicable offense or incident type.
- A specific and descriptive reason for the search sufficient to permit an independent auditor to understand its relationship to the associated incident or investigation.

Generic entries such as "Intel," "Active Investigation," "Investigation," "Follow-Up," "Patrol," "Other," or similar language are not acceptable substitutes for a valid DR number or a specific search justification. Search fields shall contain only the information necessary to establish and audit authorized use. Users shall not place confidential source information, investigative strategy, victim or witness information, officer-safety information, or other sensitive case details in the vendor's Case Number, Search Reason, or similar fields. The DR number and standardized offense category should serve as the principal link to the Department's controlled investigative record.

Immediate Operational Searches

A historical-data search should not be conducted until an MPD DR number is available. If an immediate search is necessary to address an unfolding threat to life or public safety and obtaining a DR number first is impracticable, the user may conduct the search only through an emergency or exigent-search function approved by the Program Manager. The user shall obtain a DR number and document the search in the Department record as soon as practicable and before the end of the shift. The system entry shall not use a CAD number, "Intel," "Active Investigation," or another substitute in the Case Number field. Every emergency or exigent search shall be automatically routed for supervisory and monthly audit review.

Documentation of the Plate and Vehicle

Every license plate searched shall be documented under the associated DR number in the Department's records-management, case-management, or other authorized law-enforcement system. A CAD comment may be used when it is the normal operational record and does not disclose sensitive information; however, personnel shall not create a separate CAD comment merely to duplicate information already maintained in the associated Department record.

When disclosure in CAD could compromise an investigation, reveal a confidential source or investigative technique, identify a victim or witness, or create an officer-safety concern, the plate and its connection to the investigation shall be documented only in the appropriate report, supplement, or case-management entry. Documentation should be concise and shall not include more sensitive information than is reasonably necessary to establish the lawful investigative connection.

When the vehicle has been reasonably identified and is relevant to the incident, the vehicle should also be added as an involvement in the records-management system. A vehicle that is merely an unconfirmed



CITY OF MARICOPA POLICE DEPARTMENT

OPS 2.70

AUTOMATED LICENSE PLATE READERS (ALPR)

08/25/2026

lead or possible match shall be documented as such and shall not be represented as a confirmed involvement.

Outside-Agency Assistance

A search conducted for another agency shall be tied to an MPD DR documenting the requesting agency, its case number, the general authorized purpose of the request, and the MPD employee who conducted the search. When the ALPR system reliably captures the requesting user or agency, date, time, plate, and MPD user, those fields need not be duplicated in a separate narrative record. Sensitive facts supplied by the requesting agency shall not be entered into vendor search fields and shall be maintained only in an appropriate Department record when necessary.

Prohibited Uses

Department personnel shall not use, attempt to use, or permit another person to use ALPR equipment or data for an unauthorized purpose. Prohibited uses include:

- Any personal, private, retaliatory, harassing, political, commercial, or curiosity-based purpose.
- Searching for a family member, household member, romantic partner, acquaintance, coworker, neighbor, public official, public figure, or other person unless the search is directly connected to a documented and authorized law enforcement matter.
- Monitoring a person based solely on race, color, ethnicity, national origin, religion, sex, gender, sexual orientation, disability, political viewpoint or affiliation, or another protected characteristic.
- Monitoring lawful First Amendment-protected activity, including demonstrations, political activity, religious activity, association, or expression, unless directly related to a documented criminal investigation supported by articulable facts.
- Immigration enforcement unless required by law or directly connected to an independently authorized state or local criminal investigation.
- Private repossession, civil debt collection, private employment matters, or personal service of process.
- Using another person's credentials, sharing credentials, circumventing access controls, entering false or misleading search information, or attempting to conceal activity from an audit.

Alerts, Hotlists, and Enforcement Action

Alert Verification

An ALPR alert is an investigative lead. Before taking enforcement action based substantially on an alert, personnel shall independently confirm the license plate characters, state of issuance, vehicle description, alert status, and whether the underlying record remains active through ACJIS or another authoritative source. If immediate action is required to address an articulable threat to officers or public safety, verification shall occur as soon as circumstances permit. No ALPR operator may access ACJIS unless separately authorized.



CITY OF MARICOPA POLICE DEPARTMENT

OPS 2.70

AUTOMATED LICENSE PLATE READERS (ALPR)

08/25/2026

Locally Created Hotlists and Alerts

Locally created hotlist or alert entries shall be supported by a valid DR number, a documented lawful purpose, and supervisor approval. The entry shall identify the submitting user, approving supervisor, date entered, reason, and expiration or review date. Entries shall be reviewed for continued validity and promptly removed when the underlying basis no longer exists. System-generated hotlists obtained from an authorized criminal justice source are not subject to individual supervisor approval but remain subject to verification before enforcement action.

Data Collection, Retention, Evidence, and Disclosure

ALPR data and images are for the official use of the Maricopa Police Department. They may contain sensitive criminal-investigative, criminal-justice, victim, witness, privacy, officer-safety, or law-enforcement security information. Access, disclosure, and release shall comply with applicable law, City records procedures, discovery obligations, court orders, and this policy.

ALPR detection data shall be retained for no longer than 30 days after collection and shall thereafter be automatically deleted unless particular data has been affirmatively preserved because it has become, or is reasonably believed likely to become, evidence; is subject to a litigation or legal hold; or must be retained pursuant to subpoena, court order, discovery obligation, public-records preservation requirement, or other legal authority.

Only data reasonably related to the identified matter shall be preserved. Preserved data shall be exported and booked into the approved evidence-management system or otherwise maintained in accordance with MPD evidence procedures, with the associated DR number and basis for preservation documented. Preserved data shall not remain indefinitely in the searchable ALPR database merely because it may have investigative value.

Public Records and Other Requests

All public-records, media, civil, administrative, or non-law-enforcement requests for ALPR data, audit information, system logs, screenshots, or related records shall be referred to the Records Supervisor and, when appropriate, the City Attorney. Department personnel shall not directly disclose ALPR information in response to such a request.

Records personnel shall evaluate each request under applicable law and shall consider whether disclosure would reveal information protected by statute, court rule, privilege, privacy interests, the best interests of the State, an active or prospective investigation, investigative techniques, officer-safety information, criminal-justice system information, or another lawful basis for withholding or redaction. This policy does not declare all ALPR records categorically public or categorically confidential.

Records Minimization

Personnel shall create and retain records reasonably necessary to document official activity and comply with law, evidence requirements, and Department policy. To reduce unnecessary duplication and the risk of compromising investigations, personnel shall use existing system-generated logs and the underlying DR as authoritative records whenever practicable. Personnel shall not create or retain duplicate screenshots, exports, spreadsheets, emails, CAD comments, or narrative summaries unless they serve a



CITY OF MARICOPA POLICE DEPARTMENT

OPS 2.70

AUTOMATED LICENSE PLATE READERS (ALPR)

08/25/2026

documented operational, evidentiary, supervisory, audit-exception, legal, or records-management purpose. Records shall not be destroyed, altered, concealed, or omitted to avoid disclosure, discovery, audit, or a lawful retention requirement.

Security, Access Control, and Account Management

ALPR data shall be protected by procedural and technological safeguards. Access shall be through individually assigned, password-protected accounts capable of recording the user, date and time, search criteria, reason, case number, results accessed, exports, sharing activity, administrative changes, and other system activity when supported.

- The Program Manager or designee shall review user accounts, roles, categories, and administrator permissions at least quarterly.
- Accounts shall be deactivated promptly when a person separates from MPD, transfers to an assignment that no longer requires access, or otherwise no longer has an operational need.
- Permissions shall follow the principle of least privilege. Administrative, audit, hotlist-management, investigative, supervisory, and ordinary user functions shall be separated when the platform permits.
- Vendor or technical-support access shall be limited to documented support, security, maintenance, or contractual purposes and shall be logged when supported.
- Suspected credential compromise or unauthorized access shall be reported immediately to a supervisor, the Program Manager, and Information Technology as appropriate.

Data Sharing

Routine ALPR data sharing shall be limited to authorized and verified criminal-justice agencies within Arizona and shall be configured according to offense type and legitimate operational need when the platform permits. Sharing outside Arizona is prohibited unless specifically authorized in writing by the Chief of Police or designee for a documented law enforcement purpose and permitted by law.

- Recipient agencies shall use MPD ALPR data only for official law enforcement purposes consistent with this policy and shall not reshare the data without MPD authorization.
- MPD may restrict sharing by agency, offense type, or use case and may suspend or terminate access for suspected misuse, inadequate safeguards, or policy incompatibility.
- Outside-agency access shall be auditable and should record the accessing user and agency, date and time, case or incident number, offense type, and reason for access.
- ALPR data may be provided to prosecutors or other authorized persons only as permitted or required by law and applicable discovery or court process.

Auditing and Oversight

Automated Audit Assistance

Vendor-provided audit assistance, anomaly detection, proactive lockout, or similar safeguards shall be enabled when available and approved by MPD. Alerts generated by these features shall be reviewed promptly by an authorized administrator. Automated tools supplement, but do not replace



CITY OF MARICOPA POLICE DEPARTMENT

OPS 2.70

AUTOMATED LICENSE PLATE READERS (ALPR)

08/25/2026

supervisory review and independent departmental audits. The absence of an automated alert does not establish that activity complied with policy.

Monthly Audit

The Program Manager shall ensure that an ALPR usage audit is completed each month by trained personnel. The audit shall include all automated anomaly alerts, emergency or CAD-number exceptions, searches lacking required information, sensitive or restricted use categories, administrator activity, exports, locally created hotlist entries, outside-agency activity when available, and a risk-based sample of remaining searches.

The audit shall determine whether each reviewed search or action was conducted by an authorized user; was associated with a valid DR or approved exception; contained an accurate offense type and specific reason; was documented in the underlying record; was reasonably related in scope and date range to the investigation; complied with sharing and retention requirements; and involved appropriate preservation, export, or administrative action.

Routine compliant activity need not be reproduced in a separate narrative audit report. The auditor should rely on the original system review and record only the fact and date of completion, scope or methodology, reviewer, identified exceptions, referrals, and corrective actions. Case-specific details shall remain in the underlying DR or restricted investigative record and shall not be duplicated in a general audit summary unless necessary for review or action.

Access Review and Annual Assessment

At least quarterly, the Program Manager or designee shall reconcile the system user list with current personnel and assignments and shall review all administrator accounts and user-role categories. At least annually, the Office of Professional Standards or another component independent of routine system administration shall assess compliance with this policy, the effectiveness of monthly audits, access controls, sharing settings, retention settings, training, and corrective actions. Findings shall be reported to the Chief of Police.

Audit Integrity and Records

Original audit reviews and search entries shall be preserved in their original form. A user's later explanation or supporting documentation shall be separately dated and attributed and shall not replace or alter the original entry. Audit findings shall be documented as compliant use, documentation deficiency, training issue, policy violation, referred for investigation, or unresolved. Audit records and corrective-action documentation shall be retained according to the applicable records-retention schedule.

Suspected Misuse and Corrective Action

Personnel who become aware of suspected unauthorized access, use, dissemination, credential compromise, or other misuse shall immediately notify a supervisor or commander. The supervisor or commander shall ensure relevant logs and records are preserved and shall promptly notify the Program



CITY OF MARICOPA POLICE DEPARTMENT

OPS 2.70

AUTOMATED LICENSE PLATE READERS (ALPR)

08/25/2026

Manager and the Office of Professional Standards. Notification shall not be delayed solely because a routine audit remains incomplete.

When circumstances reasonably indicate possible misuse or risk to a person, data, or investigation, the Department may immediately suspend the involved user's ALPR access pending review. Confirmed or suspected criminal conduct shall be referred to an appropriate investigative authority. Policy violations may result in retraining, restriction or revocation of access, administrative investigation, discipline, or criminal referral, as appropriate.

Program Review

At least annually, the Program Manager shall evaluate operational effectiveness, privacy and civil-rights protections, audit trends, confirmed misuse, vendor changes, retention and sharing settings, and the continuing need for the program. The review shall be documented in a concise command-level record that does not duplicate case-specific information, investigative methods, system-security details, or personnel-confidential information. Any public release concerning the program shall be coordinated with the Chief of Police, Records Supervisor, Public Information Officer, and City Attorney as appropriate.