



STATE OF MISSOURI
DEPARTMENT OF PUBLIC SAFETY

AUTOMATED LICENSE PLATE READER

Best Practices Guide

September 30, 2026

The Missouri Department of Public Safety is providing the following automated license plate reader (ALPR) guidance to Missouri state, county and local law enforcement agencies as directed by Governor Mike Kehoe in [Executive Order 26-18](#), issued September 16, 2026. It follows a review of Missouri state, county, and local law enforcement ALPR policies along with national law enforcement associations' best practices, standard operating procedures, directives, agreements and training materials. This guide is intended to be used as a reference by Missouri agencies developing or evaluating an ALPR program. It is not presented as a statement of Missouri law or as legal advice. Its recommendations must be adapted to applicable law, record retention schedules, contracts, and other factors related to each agency. Missouri law enforcement agencies shall consult directly with their general counsels concerning any questions they might have relating to the best practices outlined in this guide.

As stated in EO 26-18, Governor Kehoe directed all state agencies, boards, commissions, and local law enforcement entities that receive state funding and utilize ALPR technology to implement minimum standards governing the use of ALPR technology until a permanent legislative enactment is made. These standards include data retention limits and exclusive ownership, prohibited uses and mandatory safeguards, and auditing and misuse penalties.

The strongest ALPR policies reviewed mandated the use of ALPR systems as an investigative and public-safety tool – and not as an unrestricted database of vehicle movements. The most durable controls are built around five principles: legitimate purpose, individual accountability, proportional access, controlled retention, and auditable use.

The provisions contained herein are subject to revision at the discretion of the Director of the Department of Public Safety.

The table below consists of best-practice principles as a guide for the ethical, legitimate, and transparent use of ALPR technology.

Best-Practice Principle	Operational Standard
Legitimate purpose	ALPR access and searches must be tied to an authorized law-enforcement, public-safety, or expressly authorized administrative purpose.
Individual accountability	Each user has an individual assigned account; credentials are not shared; every affirmative search is traceable to a user and a stated reason.
Verification before enforcement	An ALPR alert is an investigative lead. Officers independently verify the plate, alert status, and circumstances before enforcement action.
Proportional historical searching	Historical searches are documented, reasonably related to the investigative purpose, and not used to create unjustified patterns-of-life records.
Limited retention	Routine non-evidentiary data must be deleted within 30 days , and deletion shall be automatic.
Controlled sharing	Law enforcement agencies can only share their data with other law enforcement agencies and must be purpose-limited, documented, and subject to equivalent safeguards.
Vendor accountability	Contracts between law enforcement agencies and vendors must address ownership/control, security, disclosure, retention/deletion, breach notification, audit rights and prohibit secondary use. All data must solely be the property of the contracting law enforcement agency.
Auditing	Law enforcement agencies shall conduct routine audits (at least monthly) plus targeted reviews when suspicious activity, complaints, or anomalies occur.
Training	Access requires documented training, with refresher or supplemental training when policy, law, or technology materially changes.
Corrective action	Misuse triggers documented investigation, access restriction or revocation as appropriate, corrective action, and referral to the Department of Public Safety.

As stated in the Joint Law Enforcement Principles for Responsible Use of Automated License Plate Reader, a framework released on September 14, 2026 by a coalition of 13 national law enforcement and public safety organizations, a mature ALPR program shall be able to answer five questions for any search or disclosure: (1) Who accessed the information? (2) What legitimate purpose supported the access? (3) What case, incident, or other identifier connects the activity to that purpose? (4) What information was obtained or disclosed? and (5) What happened to the information afterward?

The following best practice guidance was compiled following a review of Missouri state, county, and local law enforcement ALPR policies along with national law enforcement associations' best practices, standard operating procedures, directives, agreements and training materials.

1. Purpose, Scope, and Definitions

Policies that follow ALPR best practices shall cover the complete lifecycle of ALPR information including collection, alerts, hot lists, historical searches, storage, access, sharing, preservation, retention, deletion, auditing, and vendor administration.

- Apply the policy to fixed, mobile, portable, trailer-mounted, vehicle-mounted, and vendor-hosted ALPR systems used by or on behalf of the agency.
- Define ALPR-generated information broadly enough to include plate reads, vehicle/plate images, date and time, location, alert status, search results, exports, and associated metadata.
- Define an “alert” or “hit” as a *potential* match, not a conclusive identification.
- Define “historical search” as a search of previously collected ALPR data.
- Define “hot list” as an authorized list used to generate alerts and establish who may create, modify, review, and remove entries.
- Identify an ALPR Administrator/Coordinator with responsibility for access, training, configuration, sharing, retention settings, audits, and vendor liaison functions.
- Any ALPRs installed on Missouri highway right of ways must be approved by the Director of the Department of Public Safety and the Director of the Department of Transportation.

2. Authorized Uses

ALPR systems must only be used for specific, documented purposes that fall within the agency's lawful mission. Authorized uses must include:

- Locating stolen or wanted vehicles or license plates.
- Locating missing, endangered, or abducted persons when the alert or investigation is authorized.
- Investigating criminal offenses and developing investigative leads.
- Investigating hit-and-run, serious/fatal traffic crashes, and other qualifying incidents where ALPR information may reasonably assist.
- Locating vehicles associated with active investigations, warrants, BOLOs, or other authorized alerts.
- Responding to public-safety emergencies and life-safety events.
- Approved crime-scene queries or other retrospective searches reasonably calculated to locate evidence or information relevant to an investigation.

3. Expressly Prohibited Uses

- Personal curiosity or non-official searches.
- Searching oneself, family members, friends, neighbors, coworkers, romantic partners, former partners, public officials, celebrities, or other acquaintances.
- Searching to assist a private individual or as a personal favor.
- Searching to stalk, harass, intimidate, threaten, retaliate against, or improperly monitor another person.
- Searching solely because of race, ethnicity, religion, political affiliation, political activity, or other protected or lawful First Amendment activity.
- Commercial, financial, marketing, data-brokerage, or unauthorized private-investigation purposes.
- Creating personal databases, unauthorized copies, or personal archives of ALPR data.
- Using ALPR to build a long-term pattern of an individual's lawful movements without a legitimate criminal investigative purpose and appropriate authorization.
- Entering false, misleading, fabricated, or intentionally vague search reasons or case identifiers.
- Circumventing audit, logging, access-control, retention, or other accountability mechanisms.
- Providing ALPR information to unauthorized persons or entities.
- Using an alert alone as the basis for arrest, detention, search, or other enforcement action without independent verification and legal justification.
- Prohibit the integration of artificial intelligence facial recognition capabilities or software with ALPR systems to automatically screen faces of individuals by ALPR technology.

4. User Access and Account Security

- Limit access to only personnel whose duties reasonably require ALPR access.
- Require documented authorization by the designated ALPR Administrator or other approving authority.
- Use individual assigned accounts. Shared accounts and credential sharing shall be prohibited.
- Require access through authorized devices, networks, and authentication mechanisms.
- Prohibit conducting searches under another user's account.
- Disable or modify access promptly when an employee transfers, separates, loses authorization, or no longer requires access.
- Designated ALPR administrator shall periodically review the active-user list and permissions.
- Require users to log out or otherwise secure access when the system is no longer required.
- Report suspected unauthorized access, credential compromise, data loss, or disclosure to agency leadership immediately.

5. Training and Competency

Before access is granted, best practices require users to complete documented training addressing:

- Authorized and prohibited uses.
- ALPR alert/hit verification.
- Historical searching and search-reason documentation.

- Constitutional, statutory, and agency restrictions applicable to ALPR use.
- Data security, confidentiality, and dissemination.
- Retention, preservation, and deletion requirements.
- Hot-list creation and removal.
- Audit and accountability requirements.
- Vendor/system-specific operation.
- Evidence handling and investigative documentation.
- Provide refresher or supplemental training when significant changes occur in law, policy, technology, system configuration, or vendor functionality.
- Maintain records showing who completed required training and when the training was completed.

6. Hot Lists and Manual Entries

- Limit hot-list creation to authorized users.
- Record the requesting user, date, plate/state, relevant vehicle information, reason for entry, and associated case/CAD/incident/warrant/BOLO/alert identifier when applicable.
- Establish a review or expiration date when the alert is temporary.
- Remove or deactivate entries immediately when the underlying purpose no longer exists.
- Periodically review hot lists for stale, duplicate, erroneous, or unsupported entries.
- Require manual entries to identify the source and reason for the entry.

7. Alert / Hit Verification

An ALPR alert shall never be treated as self-authenticating evidence of a crime or as a substitute for an independent records check. Officers shall:

- Visually compare the captured plate with the alert/read and confirm the jurisdiction.
- Confirm the underlying record is current through the appropriate law-enforcement database.
- Determine what the alert actually relates to and whether the circumstances justify enforcement action.
- Verify the vehicle/plate and other available identifying characteristics before taking action.
- Establish the legal basis for any stop, detention, search, seizure, or arrest independently of the ALPR alert.
- Document significant verified hits and dispositions according to agency reporting requirements.

8. Historical Searches and Query Documentation

Required Search Element	Best-Practice Standard
User	Every affirmative search is attributable to an individually authorized user.
Purpose	A specific, legitimate law-enforcement/public-safety purpose is stated.
Identifier	Case, report, CAD, incident, warrant, BOLO, or other approved identifier is entered when applicable.
Specificity	The explanation is detailed enough for later supervisory/audit review.
Parameters	The system retains the search parameters where technically available.
Result/use	Significant results and subsequent disclosures/preservations are handled under applicable evidence and records procedures.

9. Historical and Pattern-of-Life Searches

Any historical or pattern-of-life-search must only be in furtherance of a narrowly focused criminal investigation to reconstruct a criminal suspect's or victim's movements over time.

- A search shall be reasonably related in scope and time to the documented investigative purpose.
- A vehicle on a hot list merely to learn where someone travels.
- Broad searches intended to reconstruct long-term movements shall require elevated supervisory review to ensure an active criminal investigation when permitted by the governing policy.
- When a search expands from locating a particular vehicle or detection to analyzing a person's broader movements, the user shall document the investigative justification and obtain any required approval.

10. Data Accuracy and Error Correction

- Treat ALPR as technology capable of misreads and false matches.
- Provide a mechanism for users to identify misreads.
- Correct or remove erroneous manually entered hot-list information immediately upon discovery.
- Establish a process for recurring camera-recognition errors, inaccurate jurisdiction reads, duplicate records, and stale underlying alerts.
- Refer the correction to the responsible data owner when an error originates in an external database.
- Emphasize the fact that a vehicle associated with an alert alone is not proof that the current driver or occupant is the wanted person.

11. Retention, Deletion, and Preservation

Routine, non-evidentiary data must not be retained longer than 30 days. Evidence/legal holds must be preserved separately.

Data category	Best-practice control
Routine, non-evidentiary ALPR detections	Use the shortest retention period that supports the agency's documented mission, applicable records requirements, and approved investigative needs; configure automatic deletion where feasible. All such data must be deleted within 30 days of collection.
Data associated with an active investigation	Preserve in the appropriate investigative/evidence system and under the applicable records-retention schedule.
Evidence / litigation / discovery hold	Preserve independently of routine ALPR deletion until the hold or legal requirement is released.
Audit logs	Retain under the agency's records schedule but long enough to support meaningful compliance review. Audit logs could be subject to review by the Department of Public Safety without notice.
Vendor-hosted data	Contractually establish retention/deletion requirements and prohibit vendor retention beyond authorized periods.

12. Data Security and Confidentiality

- Use multi-factor authentication (MFA).
- Apply role-based access control and least-privilege principles; promptly remove or reduce access when assignments or duties change.
- Protect ALPR data and credentials with encryption in transit and at rest where technically available and appropriate.
- Secure cameras, network connections, and other collection infrastructure against unauthorized access, tampering, and physical compromise.
- Maintain protected, tamper-resistant audit logs preserving user, query, access, and administrative activity.
- Require prompt vendor notification of suspected or confirmed security incidents affecting agency data, systems, or services, with documented remediation and cooperation.
- Periodically review security configurations, privileged accounts, integrations, and vendor security controls.
- Restrict stored ALPR data to authorized users.
- Use access controls appropriate to the sensitivity of the information.
- Maintain automated audit logs where the system supports them.
- Prohibit personal phones, personal computers, personal email, personal cloud storage, and personal messaging applications for storing or transmitting ALPR information unless expressly authorized by agency policy with the same controls, audits, and security systems in place. (This exception

recognizes the possibility of some smaller agencies with limited resources not providing official work phones for officers.)

- Report suspected unauthorized access, loss, disclosure, or compromise promptly.
- Preserve system logs relevant to a suspected security incident.
- Apply vendor security requirements to hosted systems and data processors.

13. Information Sharing and Outside Access

- ALPR information is shared only for legitimate law-enforcement or public-safety purposes.
- National Crime Information Center data-sharing controls shall apply to document disclosures, including the recipient, organization, date/time, information released, purpose, and responsible employee.
- ALPR data is not provided to private individuals or entities for commercial purposes.
- Policies or governing directives must require supervisory approval for disclosure of identifying information from non-alert data, and such approval shall be documented.

14. Vendor and Third-Party Requirements

Contracts must establish that the agency retains ownership and ultimate control of agency ALPR data. Vendors and subcontractors must have no independent right to sell, commercialize, profit, disclose, or otherwise exploit agency data.

Contracts and MOUs shall address at a minimum:

- Agency control/ownership of agency-generated ALPR data.
- Permitted vendor access and the purpose of that access (limited to system maintenance).
- Prohibition on selling, commercially exploiting, or independently disclosing agency data.
- Prohibition on secondary use, data mining, profiling, and unrelated analytics.
- Subcontractor and downstream-provider controls.
- Security safeguards and breach notification.
- Retention and deletion requirements, including verification where appropriate.
- Audit and compliance rights.
- Data return or deletion when the contract terminates.
- Vendor will comply with agency's request for lawful preservation, discovery, records requests, and investigations, and will not disclose any agency data without prior authorization from agency.

15. Privately Owned, Commercial, and Community ALPR

When an agency receives data from privately owned or commercial ALPR systems, the data is subject to the same requirements as outlined in this document.

- Require documented agency authorization before integrating or routinely accessing a private ALPR system.
- Apply agency search, access, sharing, security, retention, and audit requirements to data the agency receives.

16. Auditing and Accountability

Best practices include three complementary audit levels:

Audit level	Minimum scope
Routine / quarterly or comparable periodic audit	Agencies shall implement technology for continuous audit reviews to flag potential misuse. Audit logs must be reviewed by the designated department administrator at least monthly.
Targeted audit	Initiated by complaint, suspicious query patterns, unusual after-hours activity, repeated searches, sensitive-person searches, suspected misuse, or other abnormalities.
Annual comprehensive review	Review users/permissions, training, search logs, sharing, retention/deletion, vendor compliance, complaints, security incidents, audit findings, and program effectiveness.

Audit findings must be documented and reported to the designated executive/administrator. Credible evidence of misuse shall trigger an investigation and immediate access restriction when warranted.

17. Complaints, Misuse, and Corrective Action

- Provide a defined process for receiving and documenting complaints or suspected misuse.
- Preserve relevant audit logs and system records when misuse is alleged.
- Restrict or suspend access when necessary to protect the investigation or data.
- Document corrective action, retraining, access changes, discipline, or referral as appropriate.
- Use substantiated findings to improve training, system configuration, or policy.
- Any misuse by a Missouri law enforcement officer must be reported to the Director of the Department of Public Safety for a Police Officer Standards and Training (POST) investigation.
- Any criminal misuse by any employee of a law enforcement agency must be reported to the appropriate prosecuting attorney for that jurisdiction.

18. Records, Evidence, and Legal Holds

- Treat evidence derived from ALPRs separately from routine historical detections when it becomes part of an investigation.
- Preserve the original ALPR image and relevant metadata when required for evidentiary use.
- Document the circumstances under which an ALPR result became evidence.
- Preserve information subject to litigation, discovery, subpoena, court order, or other lawful preservation requirement.
- Do not allow routine automated deletion to destroy information that is under a valid legal hold.

19. Program Evaluation and Transparency

- Track false alerts and recurring system errors.

- Review audit findings, complaints, security incidents, and access trends.
- Evaluate whether deployment locations and configurations continue to serve documented public-safety objectives.
- When appropriate, publish or otherwise report program-level information consistent with applicable law and record retention requirements.
- False or misread alert rates and error-correction activity.
- Audits performed, significant findings, and corrective actions.
- Complaints, misuse investigations, access suspensions, and disciplinary referrals.
- Relevant year-over-year trends and documented public safety or investigative outcomes.