



NAPERVILLE POLICE

GENERAL ORDER

ORDER NUMBER: 41.16

SUBJECT: AUTOMATED LICENSE PLATE READER

EFFECTIVE: 1/26/2015

REVISED: 9/08/2026

Reference CALEA: 41.3.9

Index As:

- 41.16.1 Automated License Plate Reader
- 41.16.2 Authorized Access, Data Governance, and Privacy
- 41.16.3 ALPR Administration
- 41.16.4 Authorized Use and Prohibited Uses
- 41.16.5 ALPR Deployment
- 41.16.6 Data Storage and Retention
- 41.16.7 Data Searches
- 41.16.8 Hot Lists and Manual Alerts
- 41.16.9 ALPR System—ECC Responsibilities
- 41.16.10 Training
- 41.16.11 ALPR Auditing and Accountability

Purpose:

The Naperville Police Department utilizes Automated License Plate Reader (ALPR) technology to enhance public safety by assisting officers and investigators in locating stolen vehicles, wanted persons, missing or endangered persons, vehicles associated with criminal activity, and other legitimate law enforcement objectives. ALPR technology also provides valuable investigative leads that may assist in identifying suspects, locating witnesses, recovering stolen property, and solving criminal offenses.

The Department recognizes that ALPR technology, while an effective investigative tool, also raises legitimate privacy considerations. Accordingly, the Department is committed to ensuring ALPR technology is used in a manner that is lawful, transparent, accountable, and respectful of individual privacy rights. This policy establishes standards governing the collection, access, use, dissemination, retention, auditing, and security of ALPR data while ensuring compliance with applicable federal and state law, Department policy, and constitutional protections.

Policy:

The Naperville Police Department shall utilize Automated License Plate Reader technology solely for legitimate law enforcement and public safety purposes. ALPR technology is intended to support, not replace, sound investigative practices and officer judgment.

Department members shall use ALPR technology in a manner that:

- A. Supports the Department's mission of protecting life and property.
- B. Respects the constitutional rights of all persons.
- C. Protects individual privacy through appropriate safeguards and accountability.
- D. Promotes transparency and public confidence.
- E. Ensures appropriate oversight through training, auditing, and supervisory review.

No member shall use ALPR equipment or ALPR data for personal purposes, generalized surveillance, or any purpose inconsistent with Department policy or applicable law.

Guiding Principles

The Department recognizes the following principles governing the use of ALPR technology:

- A. Public Safety- ALPR technology is an investigative and officer-safety tool intended to improve the

Department's ability to locate vehicles involved in criminal activity, missing person investigations, public safety emergencies, and other legitimate law enforcement operations.

- B. Constitutional Policing- The Department shall utilize ALPR technology in a manner consistent with the United States Constitution, the Illinois Constitution, applicable statutes, and established case law.
- C. Protection of Privacy- Although license plates displayed on public roadways are generally visible to the public, the Department recognizes that ALPR technology can generate significant amounts of vehicle-location information. Members shall therefore access and use ALPR data only when related to legitimate law enforcement or public safety purposes.
- D. Accountability- Every search, query, and use of ALPR data shall be attributable to an authorized user and subject to auditing and supervisory oversight.
- E. Investigative Tool- ALPR information is intended to provide investigative leads and officer awareness. ALPR alerts, historical data, and vehicle information shall not, on its own, establish reasonable suspicion or probable cause.

Definitions:

Alert—A visual and/or auditory notification generated when the ALPR system identifies a potential match between a captured license plate and a law enforcement database or authorized hot list.

ALPR Data—Information collected by an ALPR system, including license plate information, associated vehicle images, metadata, location information, date, time, camera identification, and associated vehicle descriptors captured by the system.

Authorized User—A Department member who has successfully completed Department-approved training, possesses all required certifications, and has been granted permission to access ALPR equipment or ALPR data.

Automated License Plate Reader (ALPR)—A system of cameras, software, computer hardware, and associated databases that automatically captures, converts, compares, and stores license plate information and associated vehicle data for legitimate law enforcement purposes.

Fixed ALPR System—ALPR cameras permanently fixed to a structure or location.

Historical Search—A query of previously collected ALPR data conducted for a documented law enforcement or public safety purpose using Department-approved search criteria.

Hit—A potential match between an ALPR read and a license plate or vehicle identifier contained in an authorized hot list or alert database.

Hot List—License plate numbers or vehicle identifiers associated with stolen vehicles or plates, wanted persons, missing or endangered persons, AMBER or Silver Alerts, vehicles associated with criminal investigations, or other legitimate law enforcement or public safety purposes.

Mobile ALPR System—ALPR equipment affixed permanently or temporarily to a law enforcement vehicle for mobile deployment.

Portable ALPR System—ALPR equipment that is transportable and may be temporarily deployed at an authorized location.

Read—The capture of a license plate or vehicle image together with associated metadata, which may include date, time, location, direction of travel, camera identification, and vehicle descriptors.

Vehicle Descriptor—A characteristic of a vehicle captured or identified by the ALPR system, including make, model, color, body style, distinguishing features, decals, damage, roof accessories, trailers, or other identifying characteristics.

ORDER:

41.16.1 Automated License Plate Reader

The Department may utilize fixed, mobile, portable, or other Department-approved ALPR systems to assist officers and investigators in carrying out legitimate law enforcement and public safety responsibilities.

Authorized uses include, but are not limited to:

- A. Locating stolen vehicles or stolen license plates.
- B. Locating missing or endangered persons, AMBER Alerts, Silver Alerts, and other public safety alerts.
- C. Identifying vehicles associated with criminal investigations.
- D. Supporting criminal intelligence and investigative efforts when supported by an articulable law enforcement purpose.
- E. Assisting officers during active investigations by identifying vehicles that may have been present at or near the scene of a reported criminal offense.
- F. Supporting mutual aid operations and cooperative investigations with other law enforcement agencies when consistent with this policy.

ALPR technology shall not be used for generalized surveillance of the public or for monitoring individuals or groups absent a legitimate law enforcement purpose.

41.16.2 Authorized Access, Data Governance, and Privacy

- A. Access to the ALPR system, software, associated databases, and data is restricted to authorized Department members performing official law enforcement or public safety duties. Members shall access or use ALPR information only when reasonably related to a legitimate law enforcement purpose or authorized administrative function and in accordance with applicable law, Department policy, and the member's assigned responsibilities.
- B. The Department recognizes that ALPR systems collect information regarding vehicles traveling on public roadways. Department members shall use ALPR technology in a manner that protects individual privacy by limiting the access, dissemination, retention, and use of ALPR data to legitimate law enforcement or public safety purposes.
- C. The Department shall not use ALPR technology to conduct generalized surveillance of the public or to monitor individuals or groups absent a legitimate law enforcement purpose. ALPR technology shall not be used solely to identify, track, or monitor persons engaged in activities protected by the United States Constitution or the Illinois Constitution, including the lawful exercise of freedoms of speech, religion, association, assembly, or the press.
- D. Department members shall not access, search, query, or use the ALPR system, software, associated databases, or data for personal reasons, personal curiosity, or any purpose unrelated to an authorized law enforcement or public safety function. This prohibition includes searches involving Department members, family members, friends, acquaintances, neighbors, public officials, celebrities, or any other individual unless directly related to a legitimate law enforcement purpose or authorized administrative function.
- E. Department members shall not use ALPR technology or associated data in a manner that unlawfully discriminates against or targets any individual or group based solely upon a protected characteristic, including race, color, ethnicity, national origin, religion, sex, sexual orientation, gender identity, disability, political affiliation, or any other classification protected by law.
- F. Every access, search, query, dissemination, modification, or other use of ALPR data shall be attributable to an individual authorized user through system audit logs or other documented means. Department members are accountable for all activity conducted under their assigned user credentials.
- G. Misuse, unauthorized access, unauthorized dissemination, unauthorized disclosure, or any use of the ALPR system inconsistent with this policy may result in suspension or revocation of ALPR access privileges, disciplinary action, criminal prosecution when applicable, and civil liability.
- H. ALPR information shall be released or disseminated only as authorized by law, court order, intergovernmental agreement, or Department policy. Requests for ALPR information shall be processed in accordance with applicable public records laws, criminal discovery obligations, and Department procedures.
- I. Case-specific ALPR information may be shared with another criminal justice agency when there is a legitimate law enforcement or public safety purpose. Whenever practical, the Department shall document the requesting agency, requesting individual, purpose of the request, and information disseminated in accordance with established Department procedures.
- J. Ongoing or system-level access to Department ALPR data through regional, statewide, nationwide, vendor-operated, or other information-sharing networks shall be limited to criminal justice agencies approved by the

Chief of Police or designee. The ALPR System Administrator shall periodically review agencies granted ongoing access and shall revoke access when a legitimate law enforcement need no longer exists or continued access is inconsistent with Department policy, applicable law, or Department interests.

- K. ALPR data shall not be accessed, searched, or disseminated in a manner prohibited by federal or Illinois law or Department policy, including restrictions applicable to civil immigration enforcement or other non-criminal enforcement activity.
- L. The Department shall maintain administrative control over ALPR equipment, software, associated databases, and Department-collected data. Any third-party service provider utilized by the Department shall be required to maintain appropriate security safeguards, comply with applicable Criminal Justice Information Services (CJIS) Security Policy requirements, and protect Department data in accordance with applicable law, contractual obligations, and Department policy.

41.16.3 ALPR Administration

- A. The Chief of Police shall designate one or more Department members to serve as the ALPR System Administrator. The ALPR System Administrator shall have overall administrative responsibility for the Department's ALPR program, including system oversight, governance, compliance, and operational readiness. The ALPR System Administrator shall be responsible for:
 - 1. Establishing and maintaining procedures governing user access, data collection, storage, retention, dissemination, and security consistent with Department policy, applicable law, and CJIS Security Policy requirements.
 - 2. Establishing procedures for preserving ALPR data associated with criminal investigations, prosecutions, civil proceedings, or other lawful evidentiary purposes.
 - 3. Reviewing and approving personnel authorized to operate ALPR equipment or access ALPR data and periodically reviewing user permissions to ensure continued operational need.
 - 4. Coordinating Department-approved training for authorized users and maintaining records documenting required training and certifications.
 - 5. Maintaining records of significant investigative uses, documented evidentiary hits, and other information necessary to evaluate the effectiveness of the Department's ALPR program.
 - 6. Ensuring audits of ALPR system use are conducted in accordance with Section 41.16.11.
 - 7. Reviewing suspected misuse or unauthorized access and ensuring potential policy violations are appropriately documented and referred for investigation.
 - 8. Coordinating with Department information technology personnel and approved vendors regarding system maintenance, software updates, cybersecurity, user authentication, and system security.
 - 9. Ensuring Department retention settings and data-management practices remain consistent with Department policy and applicable law.
 - 10. Periodically reviewing this policy and recommending revisions necessary to address changes in technology, law, operational needs, or best practices.
 - 11. Ensuring no Department member operates ALPR equipment or accesses ALPR data without successfully completing Department-approved training and any required LEADS certification.
 - 12. Periodically reviewing ongoing external-agency access and data-sharing configurations for continued operational need and compliance with Department policy.
- B. Installation, maintenance, repair, replacement, or modification of Department-approved ALPR equipment or software shall be performed only by authorized Department personnel, approved vendors, or other persons authorized by the Chief of Police or designee.
- C. Permanent relocation of fixed ALPR equipment or reassignment of Department-owned mobile ALPR equipment shall require approval of the ALPR System Administrator, Deputy Chief of Police, or designee. Authorized personnel who have received Department-approved training may relocate or install mobile or portable ALPR equipment when approved by the ALPR System Administrator or Deputy Chief of Police.

41.16.4 Authorized Use and Prohibited Uses

- A. Access to and use of Department-approved ALPR systems shall be limited to authorized Department members who have successfully completed Department-approved training and possess any certifications required by law or Department policy.
- B. Department-approved ALPR systems may be deployed as part of routine patrol operations, criminal investigations, traffic safety initiatives, directed patrol operations, missing person investigations, critical

incidents, special events, mutual aid requests, or other legitimate law enforcement or public safety functions approved by the Department.

- C. Portable ALPR deployments and other mission-specific deployments shall be conducted as authorized by Division supervisors or other Department personnel designated by the Chief of Police.
- D. Department members shall not use ALPR equipment, ALPR data, historical ALPR data, vehicle descriptors, or associated databases to:
 - 1. Intentionally capture or collect license plate or vehicle information located on private property and not visible from a lawful public vantage point, except pursuant to lawful authority.
 - 2. Harass, intimidate, retaliate against, or improperly monitor any individual or group.
 - 3. Conduct searches unrelated to an authorized law enforcement or public safety purpose, including curiosity searches.
 - 4. Identify, target, or monitor individuals or groups based solely or primarily upon a protected characteristic, including race, color, ethnicity, national origin, religion, sex, sexual orientation, gender identity, disability, political affiliation, or any other classification protected by law.
 - 5. Identify, monitor, or collect information regarding persons or organizations solely because they are lawfully exercising rights protected by the United States Constitution or Illinois Constitution, including freedoms of speech, religion, assembly, association, or the press.
 - 6. Share user credentials or permit unauthorized individuals to access ALPR equipment or data.
 - 7. Disseminate ALPR information except as authorized by law or Department policy.
 - 8. Download, copy, retain, or otherwise preserve ALPR information outside Department-approved systems except as necessary for evidentiary purposes or as otherwise authorized by Department policy.
 - 9. Alter, delete, conceal, or otherwise interfere with audit logs or records documenting ALPR system use.
 - 10. Use ALPR technology for any commercial, political, or other non-law enforcement purpose.
- E. Department members shall exercise sound judgment when using ALPR technology and shall ensure that each use is consistent with a legitimate law enforcement or public safety purpose and capable of supervisory review.

41.16.5 ALPR Deployment

- A. At the beginning of each use of a mobile ALPR system, officers shall ensure the system has access to the most current Department-approved hot list or alert database available.
- B. Officers utilizing a mobile ALPR system shall verify the functionality of the system prior to deployment and conduct a reasonable pre-operational inspection in accordance with manufacturer guidance. Problems affecting system reliability shall be reported as soon as practical to the ALPR System Administrator. Equipment with significant damage or that is non-functioning shall not be deployed unless authorized by the ALPR System Administrator or Deputy Chief of Police.
- C. An ALPR alert or hit, whether generated from a fixed, mobile, or portable ALPR system, is an investigative lead and does not, standing alone, establish reasonable suspicion or probable cause for a detention, traffic stop, search, arrest, or other enforcement action. Officers shall independently evaluate the totality of the circumstances and verify the alert before taking enforcement action whenever reasonably practical. Prior to initiating enforcement action based upon an ALPR alert, officers shall:
 - 1. Visually verify that the observed license plate matches the alert, including the license plate characters, issuing jurisdiction, and, when available, associated vehicle descriptors.
 - 2. Confirm the current status of the alert through ECC, MDT, or another authorized law enforcement database whenever reasonably practical.
 - 3. Consider any additional facts known to the officer that may corroborate or dispel the alert before initiating enforcement action. When immediate verification is not practical because of officer-safety concerns or exigent circumstances, verification shall occur as soon as reasonably practical.
- D. The receipt of an ALPR alert does not require an officer to initiate enforcement action. Officers shall exercise sound judgment based upon the totality of the circumstances.
- E. For actionable alerts, the officer shall record the disposition in the ALPR system or otherwise document the disposition in accordance with Department procedures. Enforcement action taken in response to an ALPR alert shall be documented in the appropriate incident report.
- F. Officers receiving a valid alert while assigned to another duty or call for service shall:
 - 1. Weigh the seriousness and urgency of the current assignment against the basis of the ALPR alert.
 - 2. When practical or necessary, notify a supervisor or ECC that enforcement action will be taken, or has been taken, in lieu of the assigned duty or call for service. Reassignment may be coordinated by ECC.

3. Give primary consideration to public and officer safety. If reassignment from the current duty would jeopardize public or officer safety, enforcement action on the alert should not be immediately undertaken.
 4. When applicable, notify ECC when unable or unavailable to act on a valid alert so the information may be disseminated to other officers or law enforcement agencies in the area.
- G. The ALPR system may be deployed to assist another law enforcement agency at its request upon approval of the Chief of Police or designee. A Naperville Police Department authorized user shall operate Department ALPR equipment unless otherwise approved. Any data access or dissemination associated with the operation remains subject to this policy.
- H. The absence of an ALPR alert or search result does not establish that a vehicle was not involved in criminal activity or was not present at a particular location. Likewise, the presence of an ALPR alert or search result does not independently establish criminal conduct. ALPR technology shall be considered together with all other available information.

41.16.6 Data Storage and Retention

- A. Collection and retention of ALPR data is subject to the following guidelines:
1. ALPR data shall be transferred, stored, and maintained through Department-approved systems and procedures.
 2. Routine ALPR reads shall be retained for thirty (30) days and thereafter purged unless the data has become, or it is reasonable to believe it will become, evidence in a criminal, civil, or administrative proceeding; is subject to a lawful records-preservation requirement; or is otherwise required to be retained by law or Department policy.
 3. ALPR data preserved for evidentiary or other authorized purposes shall be exported or preserved in a Department-approved manner and handled in accordance with Department evidence and records procedures.
 4. The Department shall periodically evaluate the thirty-day retention period to ensure it remains reasonably necessary to accomplish legitimate law enforcement objectives while minimizing unnecessary retention of ALPR data.
- B. All retained ALPR data shall be safeguarded by appropriate procedural and technological controls. Access to stored ALPR data shall require authorized credentials and shall be capable of documenting user identity, date, time, and activity.
- C. Authorized users may access stored ALPR data only when reasonably related to a documented criminal investigation, public safety incident, missing person investigation, officer-safety concern, authorized administrative inquiry, or other legitimate law enforcement purpose.
- D. Transmission and storage of ALPR data shall comply with applicable LEADS and CJIS security requirements and Department information-security practices.
- E. ALPR data may be shared with other criminal justice agencies only for legitimate law enforcement or public safety purposes, as otherwise permitted by law, and in accordance with Section 41.16.2.
- F. ALPR data shall not be retained outside Department-approved systems for the purpose of circumventing established retention limits.

41.16.7 Data Searches

- A. Historical ALPR search results are investigative leads and shall not, standing alone, establish probable cause or reasonable suspicion. When authenticated and relevant to a criminal investigation, prosecution, or other lawful proceeding, ALPR data may become evidentiary in nature. ALPR information determined to have evidentiary value shall be preserved in accordance with Department evidence procedures.
- B. Authorized users may conduct historical ALPR searches when related to a documented criminal investigation, public safety incident, missing person investigation, officer-safety concern, authorized administrative inquiry, or other legitimate law enforcement purpose.
- C. Historical searches may utilize full or partial license plate information, vehicle descriptions, vehicle descriptors, or other Department-approved search criteria supported by the ALPR system. Searches utilizing vehicle characteristics, travel patterns, location information, or other advanced analytical features shall be reasonably related in scope and duration to the documented investigative or public safety purpose and shall not be used to conduct generalized surveillance.
- D. Each historical search shall include:

1. A valid incident, CAD, or case number.
 2. The incident type or other appropriate classification.
 3. A documented law enforcement or public safety purpose entered into the appropriate search-justification field.
 4. Search criteria and scope reasonably necessary to accomplish the investigative objective.
- E. When exigent circumstances require an immediate ALPR search before an incident, CAD, or case number is available, the authorized user may conduct the search using an appropriate emergency justification. The associated incident, CAD, or case number shall be documented as soon as reasonably practical. Emergency searches shall be subject to review during the monthly audit process.
 - F. Authorized users may conduct nationwide ALPR searches when reasonably related to a documented law enforcement or public safety purpose. Nationwide searches are subject to the same documentation, scope, and audit requirements as other historical searches.
 - G. Every historical ALPR search shall be attributable to an individual authorized user through system audit logs or other documented means and is subject to supervisory review and periodic audit.
 - H. Historical ALPR searches shall not be conducted without a legitimate law enforcement or public safety purpose, for personal reasons or curiosity, or as exploratory, speculative, or generalized searches unrelated to a documented law enforcement purpose.
 - I. The existence or absence of an ALPR search result does not independently establish whether a vehicle was or was not present at a particular location.

41.16.8 Hot Lists and Manual Alerts

- A. The Department may utilize hot lists or alert databases obtained from authorized criminal justice information systems or other Department-approved law enforcement sources. Hot-list information shall be used only for legitimate law enforcement or public safety purposes consistent with this policy.
- B. Authorized users may manually enter a license plate or vehicle identifier into the ALPR system when the entry is reasonably related to a documented criminal investigation, missing or endangered person investigation, officer-safety concern, public safety incident, or other legitimate law enforcement purpose.
- C. Each manual hot-list or alert entry shall include sufficient information to establish and document the basis for the entry, including:
 1. A valid incident, CAD, or case number.
 2. The law enforcement or public safety purpose for the entry.
 3. The identity of the member making the entry.
 4. The date of entry.
 5. An expiration date or review date, when supported by the ALPR system.
 6. Any officer-safety or investigative information necessary to appropriately respond to an alert.
- D. Prior to manually entering a license plate or vehicle identifier, the authorized user shall take reasonable steps to verify the accuracy of the information and confirm that the entry is supported by a legitimate law enforcement or public safety purpose.
- E. Manual hot-list entries shall remain active only for the period reasonably necessary to accomplish the documented law enforcement or public safety purpose. Unless a shorter period is appropriate, manually entered alerts shall expire after thirty (30) days unless reviewed and renewed by an authorized user based upon a continuing documented law enforcement or public safety need.
- F. Renewal of a manual hot-list entry shall require confirmation that the underlying law enforcement or public safety purpose remains valid. The renewal and reason for continued inclusion shall be documented within the ALPR system or other Department-approved record.
- G. A manual hot-list entry shall be removed as soon as reasonably practical when the Department becomes aware that the underlying basis for the entry no longer exists, including when a vehicle has been recovered, a wanted or missing person has been located, an investigative interest has ended, or the information supporting the entry is determined to be inaccurate.
- H. Receipt of an alert generated from a manually entered hot-list record remains subject to the verification requirements of Section 41.16.5. A manual hot-list entry does not independently establish reasonable suspicion or probable cause.
- I. Manual hot-list entries, renewals, removals, and associated user activity shall be maintained in system audit logs when supported by the ALPR system and are subject to supervisory review and the auditing requirements established by this policy.

- J. Hot lists received automatically from LEADS, NCIC, or other authorized criminal justice information systems shall be governed by the originating system's requirements and applicable law. Department members are not responsible for independently reviewing or renewing individual records contained in externally maintained hot lists.

41.16.9 ALPR System—ECC Responsibilities

- A. Authorized ECC telecommunicators may access the ALPR system for the purpose of receiving ALPR alerts, assisting field personnel, conducting authorized searches when requested, and performing other functions consistent with their assigned duties and this policy.
- B. Upon receipt of an ALPR alert or confirmed hit appropriate for field notification, ECC may disseminate the information to field personnel through a BOLO. The BOLO should include the information contained within the ALPR alert that is reasonably necessary to assist officers, including, when available, the license plate and state of issuance, vehicle description, location, direction of travel, time of the alert, basis for the alert, and relevant officer-safety information.
- C. ALPR information disseminated by ECC is an investigative lead. ECC dissemination of an ALPR alert does not constitute independent verification of the vehicle or license plate and does not establish reasonable suspicion or probable cause for enforcement action. Officers receiving an ALPR alert or BOLO remain responsible for independently evaluating and verifying the information in accordance with Section 41.16.5 before taking enforcement action whenever reasonably practical.
- D. When requested by an officer, ECC may query LEADS or another authorized criminal justice information system to assist in confirming the current status of a license plate, vehicle, wanted person, or other information associated with an ALPR alert. When information contained within the ALPR system conflicts with current information contained within LEADS, officers and ECC personnel shall rely upon the current LEADS information for purposes of determining the status of the associated record.
- E. ECC may disseminate informational ALPR alerts or BOLOs when the information may reasonably assist field personnel in locating a vehicle or person associated with a legitimate law enforcement or public safety purpose. The receipt of an ALPR BOLO does not require an officer to respond or take enforcement action. Officers shall exercise discretion based upon their current assignment, the nature of the alert, available resources, and the totality of the circumstances.
- F. When multiple ALPR alerts are received involving the same vehicle or incident, ECC should update the existing BOLO with relevant subsequent information, including updated location, time, or direction of travel, rather than creating unnecessary duplicate BOLOs.
- G. When an ALPR alert results from a Department-created manual hot-list entry, ECC may, when requested or when reasonably appropriate based upon information contained within the alert, notify the Department member or investigative unit associated with the entry.
- H. ECC shall communicate relevant officer-safety information associated with an ALPR alert when such information is available, including information concerning wanted persons, stolen vehicles, weapons, violent offenses, or other known safety considerations.
- I. Authorized ECC personnel may conduct historical ALPR searches at the request of an officer or other authorized Department member when the search is reasonably related to a legitimate law enforcement or public safety purpose. Historical searches conducted by ECC personnel are subject to the same documentation, access, training, and auditing requirements established in Sections 41.16.7, 41.16.10, and 41.16.11.
- J. ECC personnel shall not independently modify or disposition ALPR alerts or manual hot-list entries unless specifically authorized by Department procedure. Responsibility for dispositioning actionable alerts remains with the officer taking action, and responsibility for maintaining manual hot-list entries shall be governed by Section 41.16.8.

41.16.10 Training

- A. All authorized users of ALPR systems shall receive Department-approved initial training before operating ALPR equipment or accessing ALPR data. Training shall include, at minimum:
 - 1. Proper use of ALPR systems, equipment, search functions, and operational protocols.
 - 2. Applicable LEADS training and certification requirements.
 - 3. Authorized and prohibited uses of ALPR technology and data.
 - 4. Legal and constitutional considerations, including privacy, First Amendment protections, and the requirement to independently verify alerts before enforcement action.

5. Search documentation, data handling, dissemination, retention, security, and audit requirements.
- B. The Training Division, in coordination with the ALPR System Administrator, shall ensure significant changes in hardware, software, law, Department policy, or identified audit trends are addressed through in-service training, bulletins, or other appropriate instruction.

41.16.11 ALPR Auditing and Accountability

- A. The ALPR System Administrator, or designee, shall conduct and document monthly audits of ALPR system use to ensure compliance with applicable law and Department policy.
- B. Monthly audits shall include a review of a representative sample of user searches and, when available, system-generated alerts or indicators of unusual or potentially unauthorized activity. The audit shall include review of:
 1. The identity of the authorized user conducting the search.
 2. The associated incident, CAD, or case number, or documented emergency justification.
 3. The stated law enforcement or public safety purpose for the search.
 4. Whether the search was reasonably related to the documented purpose.
 5. The search criteria utilized and, when appropriate, the scope and duration of the search.
 6. Any dissemination of ALPR information to another criminal justice agency.
 7. Any unusual, anomalous, or potentially unauthorized search activity identified through system audit tools or other means.
 8. Any emergency search conducted before an incident, CAD, or case number was available.
- C. In addition to random or representative sampling, the ALPR System Administrator, or designee, shall conduct targeted reviews when activity reasonably warrants additional scrutiny, including unusual search volumes or patterns, searches lacking adequate documentation, repeated searches involving the same vehicle, or other activity inconsistent with normal Department operations.
- D. Any apparent misuse, unauthorized access, unauthorized dissemination, or other potential violation identified during an audit shall be documented and referred to the appropriate supervisor or command officer for review and, when warranted, further investigation.
- E. The ALPR System Administrator shall ensure an annual comprehensive audit of the Department's ALPR program is conducted. The annual audit shall include, at minimum, a review of:
 1. User access and permissions.
 2. Training and certification requirements.
 3. Data retention and deletion practices, including whether the established retention period remains appropriate.
 4. Data sharing and dissemination practices, including agencies with ongoing or system-level access to Department ALPR data.
 5. System security, authentication, and access controls.
 6. Compliance with Department policy and applicable law.
 7. Manual hot-list practices, when applicable.
 8. Any identified misuse, policy violations, corrective actions, or training needs.
 9. The operational effectiveness and legitimate law enforcement use of the ALPR program.
 10. Vendor compliance with applicable contractual, security, retention, and data-protection requirements.
- F. ALPR audit logs and documentation of completed audits shall be maintained in accordance with applicable records-retention requirements and Department procedures.
- G. The ALPR System Administrator shall report significant audit findings, identified trends, policy concerns, or recommended corrective actions to the Chief of Police or designee.