

	HEATH DEPARTMENT OF PUBLIC SAFETY	
	Policy 7.18 Automated License Plate Readers (ALPRs)	
	Effective Date: 11/07/2024	Review Date: 07/29/2026
	Approved: _____ <i>[Signature]</i> Director of Public Safety	
	Reference:	

I. POLICY

The Heath Department of Public Safety utilizes Automated License Plate Reader (ALPR) technology to support legitimate law enforcement purposes while recognizing and respecting the privacy, civil rights, and civil liberties of the public. ALPR data shall be collected, accessed, retained, disseminated, and audited only in accordance with applicable federal and state law, Criminal Justice Information Services (CJIS) requirements, and department policy.

All data captured by the ALPR system is the property of this department and shall be used solely for official law enforcement purposes. Access to ALPR data is restricted to authorized personnel with a legitimate law enforcement need. ALPR data may contain confidential or sensitive law enforcement information and shall be protected from unauthorized access, disclosure, or dissemination. Any release of ALPR data shall be governed by applicable law and department policy.

II. PURPOSE

The purpose of this policy is to establish procedures and accountability measures governing the authorized use, access, collection, retention, dissemination, storage, and auditing of ALPR data by members of this department. The department utilizes ALPR technology, including fixed and trailer-mounted systems, as a law-enforcement tool to enhance public safety, support patrol operations, assist criminal investigations, and improve the department's ability to identify vehicles associated with criminal activity, missing persons, AMBER Alerts, BOLO notifications, and other legitimate law enforcement purposes.

The ALPR system utilizes specialized cameras and Optical Character Recognition (OCR) technology to capture and convert license plate images into searchable text data that may be compared against designated law enforcement databases, including NCIC and TCIC. The system may collect and store license plate numbers, vehicle images, dates, times, locations, and related vehicle information; however, it does not identify the driver or occupants of a vehicle. All ALPR operations shall be conducted in a lawful, ethical, and professional manner.



HEATH DEPARTMENT OF PUBLIC SAFETY

GENERAL ORDERS MANUAL

III. DEFINITIONS

- A. Automated License Plate Reader (ALPR): A computer-based law enforcement system utilizing specialized cameras and software, including OCR technology, to capture digital images of license plates and compare the information against designated law enforcement databases.
- B. ALPR Administrator: The Director of Public Safety or designee responsible for the oversight, administration, management, auditing, security, and compliance of the department's ALPR program and systems.
- C. ALPR Operator: A department member who has successfully completed Department approved ALPR training and is authorized to access, operate, monitor, query, or utilize ALPR systems and associated data for legitimate law enforcement purposes.
- D. Detection / Read: Data Captured by an ALPR system consisting of digital images of license plates, vehicles, and associated metadata including but not limited to date, time, geographic location, camera location, and vehicle descriptors obtained during an ALPR scan.
- E. Law Enforcement Database: A database or list of license plates associated with vehicles or persons of law enforcement interest compiled from authorized local, state, federal, or regional law enforcement sources, including but not limited to NCIC, TCIC, BOLO notifications, stolen vehicle files, wanted person files, AMBER Alerts, and missing persons databases.
- F. Vehicle of Interest: A vehicle associated with criminal activity or law enforcement investigation, including but not limited to stolen vehicles, vehicles displaying stolen license plates, vehicles linked to wanted or missing persons, or vehicles identified through authorized law enforcement investigations.

IV. ALPR ADMINISTRATOR

- A. The Operations Captain shall be responsible for ensuring compliance with all requirements governing the department's ALPR program, including but not limited to the following:
 - 1. Ensuring that only properly trained and authorized personnel are permitted access to ALPR systems, equipment, or ALPR data.
 - 2. Ensuring all required training is completed and documented for authorized ALPR users prior to system access.



HEATH DEPARTMENT OF PUBLIC SAFETY

GENERAL ORDERS MANUAL

3. Ensuring appropriate oversight, monitoring, and auditing of ALPR systems to maintain the security, integrity, and lawful use of ALPR information in compliance with applicable privacy laws and the department's ALPR policy.
4. Ensuring procedures are established and followed regarding ALPR operations, data access, retention, dissemination, and audit logging.
5. Ensuring this policy and related procedures are available for public review in accordance with applicable law and Department transparency practices.

V. OPERATIONS

- A. The use of ALPR technology is restricted to legitimate law enforcement purposes. Department members shall not use, access, or permit others to use ALPR equipment, systems, or data for any unauthorized, personal, commercial, or non-law enforcement purpose.
 1. ALPR technology may be used in conjunction with criminal investigations, intelligence gathering, BOLO notifications, missing person investigations, suspect interdiction, stolen vehicle investigations, and other lawful law enforcement activities. Reasonable suspicion or probable cause is not required for the general operation or use of ALPR systems.
 2. Partial license plates, vehicle descriptors, and other identifying information associated with major crimes or significant incidents may be searched in the ALPR system in an effort to identify vehicles associated with criminal activity.
 3. No department member shall operate ALPR equipment or access ALPR data without first completing department-approved training.
 4. ALPR alerts should be considered informational and investigative in nature. An ALPR alert alone shall not constitute probable cause or reasonable suspicion for enforcement action. Prior to initiating a traffic stop, detention, arrest, or other law enforcement intervention based upon an ALPR alert, officers shall:
 - a. Verify the alert through NCIC, TCIC, Communications, MDC, or other authorized law enforcement databases.



HEATH DEPARTMENT OF PUBLIC SAFETY GENERAL ORDERS MANUAL

- b. Visually confirm that the observed plate, issuing state, and vehicle descriptors match the information associated with the ALPR alert.
 - c. Develop the legal basis for enforcement action by establishing probable cause and ensuring adherence to constitutional requirements.
- 5. Because an ALPR alert may be associated with a vehicle and not necessarily the driver or occupants, officers shall make reasonable efforts to confirm the identity of any wanted or involved person prior to initiating enforcement action.
- 6. Law enforcement databases utilized by the ALPR program shall be approved and managed by the ALPR Administrator and may include information obtained from local, state, regional, and federal law enforcement databases. Department personnel shall recognize that law enforcement database information may not reflect real-time updates and that occasional OCR or database errors may occur.
- 7. All ALPR users shall utilize individually assigned login credentials and secure two-factor authentication procedures. Access to ALPR systems and data shall be fully auditable and restricted to authorized personnel only.

VI. DATA COLLECTION AND RETENTION

- A. The Director of Public Safety, or designee, is responsible for ensuring that appropriate systems, procedures, and safeguards are in place for the lawful collection, retention, storage, security, auditing, and disposal of ALPR data. All ALPR data collected by the department shall be maintained in accordance with applicable federal and state law, department records retention policy, vendor agreements, and the City of Heath's records retention schedule.
- B. ALPR data may be stored by a department-approved vendor providing ALPR services and data hosting. The vendor shall be responsible for maintaining administrative, technical, and physical safeguards to protect ALPR data from unauthorized access, disclosure, alteration, or destruction. Vendor-retained ALPR data will only be shared with other law enforcement agencies upon the approval of the ALPR Administrator. The Department may separately retain ALPR records, reports, images, or evidentiary data obtained from the ALPR system in accordance with applicable records retention schedules, criminal justice



HEATH DEPARTMENT OF PUBLIC SAFETY

GENERAL ORDERS MANUAL

requirements, evidentiary needs, court orders, public information requests, or ongoing investigations.

- C. ALPR data that has reached the applicable retention period shall be purged or deleted unless the data has become, or it is reasonably anticipated that the data may become, evidence in a criminal or civil proceeding, is subject to a litigation hold, discovery request, public information request, court order, or other lawful requirement for retention.
- D. Information collected through the ALPR system shall not be sold, traded, commercially distributed, or used for any purpose other than legitimate law enforcement or criminal justice purposes authorized by law and department policy.

VII. ACCOUNTABILITY AND SAFEGUARDS

- A. All ALPR data should be protected through appropriate administrative, technical, and physical safeguards designed to prevent authorized access, disclosure, alteration, misuse, or destruction. The department shall maintain security measures and auditing procedures sufficient to ensure compliance with applicable law, CJIS requirements, and recognized privacy protections.
 - 1. Access to ALPR systems and data shall be restricted to authorized personnel through individually assigned login credentials and secure two-factor authentication methods. System access shall be capable of documenting user activity, including the user's identity, date, time, and actions performed within the system.
 - 2. Personnel authorized to access ALPR data may do so only for legitimate law enforcement investigations authorized by law and defined in this policy.
 - 3. ALPR data may be shared with authorized and verified law enforcement agencies or criminal justice entities for legitimate law enforcement purposes. The sharing of ALPR information with other governmental law enforcement agencies shall be considered an authorized intergovernmental exchange of criminal justice information and not a public release of information.



HEATH DEPARTMENT OF PUBLIC SAFETY GENERAL ORDERS MANUAL

4. Every ALPR query, search, detection browsing inquiry, or historical data search shall be documented within the ALPR system and associated with a case or incident number, administrative investigation number, or other documented law enforcement purpose that clearly justifies the inquiry.
5. Access to and use of ALPR data shall be subject to periodic audit and review to ensure compliance with this policy, applicable law, and authorized use requirements. Any suspected misuse, unauthorized access, disclosure, or policy violation, shall be reported through the chain of command and investigated in accordance with department procedures.
6. Security incidents, unauthorized disclosures, data breaches, or other information security concerns involving ALPR data shall be handled in accordance with the applicable CJIS security policy requirements, and any other applicable department procedures.

VIII. DATA AUDITS

- A. The Operations Captain shall be responsible for ensuring periodic audits of ALPR system usage to verify compliance as defined in this policy, applicable law, authorized use requirements, and privacy protections.
- B. At a minimum, a semi-annual audit shall be conducted reviewing ALPR detection browsing inquiries, historical searches, and other system activity occurring during the preceding six-month period. The audit shall include a random sample of at least ten ALPR inquiries conducted by department personnel to determine whether each inquiry was made for legitimate law enforcement purposes and properly documented in accordance with this policy. The audit shall evaluate, at a minimum:
 1. Whether the inquiry was conducted by an authorized user.
 2. Whether the inquiry was associated with a legitimate law enforcement or criminal justice purpose.
 3. Whether the required case number, incident number, or documented reason for the inquiry was provided.
 4. Whether access to ALPR data was consistent with the requirements established in this policy and applicable law.



HEATH DEPARTMENT OF PUBLIC SAFETY GENERAL ORDERS MANUAL

5. Whether any unauthorized access, misuse, dissemination, or policy violations occurred.
- C. Audit findings shall be documented in a written report submitted to the Director of Public Safety. The report shall identify any policy violations, training deficiencies, system errors, or data integrity concerns and include recommendations for corrective action when appropriate.
1. All audit reports and related documentation shall be retained for the minimum period required under the Texas State Library and Archives Commission's Local Schedule and shall not be destroyed until all applicable retention periods or other legal requirements have been satisfied.
- D. Following review by the Director of Public Safety, audit reports and associated documentation shall be retained in accordance with department records retention policy and all applicable legal requirements. Any identified misuse of the ALPR system shall be investigated and addressed through appropriate administrative, disciplinary, training, and corrective actions consistent with established department procedures.

IX. RELEASE AND DISSEMINATION OF ALPR DATA

- A. ALPR data, records, images, alerts, and associated information may be shared only with authorized law enforcement agencies, prosecutorial agencies, criminal justice entities, or other governmental agencies as permitted by law and for legitimate law enforcement or criminal justice purposes. The sharing of ALPR information with authorized governmental entities shall be considered an intergovernmental exchange of information and not a release of information to the public.
- B. Requests for ALPR related records shall be processed in accordance with applicable federal and state law, the Texas Public Information Act, and any relevant court orders. Information may be withheld from public disclosure when authorized by law, including circumstances where release would interfere with the detection, investigation, or prosecution of crime, jeopardize public safety, reveal sensitive law enforcement techniques, or otherwise qualify for an exception to disclosure.



HEATH DEPARTMENT OF PUBLIC SAFETY GENERAL ORDERS MANUAL

- C. ALPR data shall not be sold, traded or commercially distributed. ALPR data shall not be released to unauthorized persons or entities.

X. PERMITTED AND IMPERMISSIBLE USES

- A. The ALPR system, all associated equipment, and all data collected through its operation are the property of the Heath Department of Public Safety. Department personnel shall access and utilize ALPR systems and ALPR data only for official and legitimate law enforcement or public safety purposes consistent with this policy, applicable law, and department procedures.
- B. The following uses of the ALPR system are specifically prohibited:
1. Except as authorized by law or court order, department personnel shall not utilize ALPR technology to capture or monitor vehicles or license plates located in areas where there is a reasonable expectation of privacy. ALPR systems shall only collect information from vehicles exposed to public view, including public roadways, public rights-of-way, and locations accessible to the general public.
 2. Department personnel shall not use ALPR systems or data to harass, intimidate, monitor, or retaliate against any individual or group.
 3. Department personnel shall not use ALPR technology, scan files, or associated data solely on the basis of a person's or group's race, color, ethnicity, national origin, religion, gender, gender identity, sexual orientation, disability, political affiliation, or any other protected characteristic recognized by law.
 4. Department personnel shall not access or use ALPR systems, scan files, or ALPR data for personal, non-law enforcement, commercial, or unauthorized purposes.
 5. Department personnel shall not use ALPR technology or associated data for the purpose of interfering with, discouraging, or infringing upon any individual's rights protected by the First Amendment of the United States Constitution, including lawful speech, assembly, association, religion, or expression.
- C. Any unauthorized access, misuse, dissemination, or impermissible use of the ALPR system or associated data shall result in an investigation by the department and may lead to criminal prosecution, civil liability, disciplinary action,



HEATH DEPARTMENT OF PUBLIC SAFETY

GENERAL ORDERS MANUAL

revocation of system access, and/or administrative sanctions up to and including termination.

XI. ALERTS FROM ALPR SYSTEMS

- A. An alert alone does not create probable cause to justify a traffic stop or detention of an individual. An officer may not detain an individual based solely on an alert from the ALPR system unless the officer has reasonable suspicion or probable cause that such person is involved in criminal activity.
- B. Officers shall obtain visual confirmation that the license plate matches the license plate on the alert.
- C. Each incident should be weighed according to the totality of circumstances presented therein.
 - 1. Stolen Vehicles and Stolen License Plates – Any stolen vehicle or stolen license plate alerts shall be verified through TCIC/NCIC before an investigative detention, unless reasonable suspicion exists that the operator is involved in criminal activity.
 - 2. Wanted Person – A wanted person alert may be utilized as reasonable suspicion after verifying the warrant through TCIC/NCIC unless the officer has information that the wanted subject is not inside the vehicle, in which case the hit shall be treated as information only.
 - 3. Hot List Alerts – This alert is information only for officers, and reasonable suspicion does not exist based on the alert alone. The narrative of the alert will assist officers in determining the level of reasonable suspicion in addition to the totality of the circumstances. Independent reasonable suspicion may or may not be required to detain. Officers shall articulate the reason for the investigative stop if an arrest is made.
- D. Upon being notified of an ALPR alert, officers may respond, or coordinate a response, to the area of the capture and look for the suspect vehicle. If the vehicle is located, proper traffic stop procedures shall be followed based upon the type of hit, officer observations, and other factors present.
- E. Hotlist alerts should include specific instructions for personnel. Example: "stop only with probable cause and ID occupants if possible".



HEATH DEPARTMENT OF PUBLIC SAFETY GENERAL ORDERS MANUAL

- F. Upon receiving an ALPR alert of a critical missing person, the Officer should notify dispatch of the alert and coordinate a response to search for the vehicle.
- G. Any search results or "Hit" from an ALPR system that leads to an arrest or incident report shall be treated as evidence and noted in the narrative and images/information uploaded into the case file.
- H. The Operations Captain shall be notified via email of any search results or "Hit" from an ALPR system that leads to an arrest or incident report.

XII. CUSTOM HOTLIST

The Department may maintain a custom hotlist based on the specific law enforcement need. Custom hotlists contain a list of license plates that are associated with serious criminal activity that occurs within the City of Heath but are not entered into TCIC/NCIC.

- A. Only authorized members are allowed to enter vehicle information onto the custom hotlist. Members shall receive approval from the Operations Captain before entering a vehicle into any hotlist.
- B. The Operations Captain will determine if the hotlist entry will be shared with only this agency or other area law enforcement
- C. Members shall only enter vehicle information onto the custom hotlist for a criminal law enforcement investigation or critical missing person alert.
- D. Once a vehicle is entered into the custom hotlist, the member entering the vehicle shall forward the information to all department staff via email.
- E. The criminal investigations division may generate an intelligence bulletin, relaying relevant information to other law enforcement personnel.
- F. Members shall not enter partial license plates onto the custom hotlist. Only complete license plate numbers will be entered into the system.
- G. Every custom hotlist entry will be required to follow certain criteria and must have the following:
 - 1. The name and ID of the individual entering the hotlist alert.
 - 2. The full license plate of the vehicle.
 - 3. The case or incident number related to the entry.



HEATH DEPARTMENT OF PUBLIC SAFETY GENERAL ORDERS MANUAL

4. A short narrative explaining the circumstances behind the reason for the entry including the existence of reasonable suspicion or probable cause if applicable. Example, “this is information only and the officer should develop their own probable cause”. If the reason for entry is an attempt to identify a criminal suspect, detailed descriptors of the suspect(s) are required if known at the time of entry.
- H. Once any member of the department is made aware that the hotlist alert is no longer valid or necessary, they will immediately request the license plate be removed from the hotlist.
- I. Removal requests are made through the Operations Captain.
- J. Once a vehicle on the custom hot list is stopped or detained, the detaining officer shall notify the Operations Captain to remove the vehicle from the hotlist. The officer shall complete a supplement to the incident number, which provides investigators relevant details about the vehicle stop.

XIII. TRAINING

- A. The Operations Captain shall ensure that all personnel authorized to access, operate, administer, manage, or utilize the ALPR system successfully complete department-approved training prior to being granted access to the system.
- B. Refresher training or remedial training may be required as determined by the Director of Public Safety, changes in law, policy updates, audit findings, or operational needs.

XIV. PRIVATELY OWNED/FUDNED ALPR SYSTEMS

- A. The department recognizes that residents, homeowner’s associations, businesses, or other private entities may choose to purchase privately owned ALPR systems and voluntarily share data with the department. All private systems shared with the department must be approved by the Director of Public Safety. All data received by the department is subject to all provisions of this policy.
- B. Department personnel shall not possess or use login credentials that provide direct access to any privately owned ALPR system. Access to privately owned data shall occur only through data shared with or provided to the department in accordance with law and policy.

PRIOR ORDERS



HEATH DEPARTMENT OF PUBLIC SAFETY GENERAL ORDERS MANUAL

From and after the effective date of issuance of this order, it shall be in full force and shall govern the operations of this department with regard to its subject matter. Former orders, policies, directives, and memoranda relating to this subject matter are hereby specifically revoked and they shall be of no force and effect from and after the date of issuance of this order.