344 Automated License Plate Reader (ALPR)

344.1 PURPOSE AND SCOPE

To provide rules and guidance for capturing, storing, and using digital data obtained through Automated License Plate Reader systems.

344.2 DEFINITIONS

(a) **AUTOMATED LICENSE PLATE READER (ALPR) –** A camera system that automatically photographs and stores license plate numbers, date, time, and location information. ALPRs may be permanently fixed, portable trailer-mounted, or vehicle-mounted.

(b) **CHIEF SECURITY OFFICER –** Responsible for receiving daily alerts on login attempts, limiting access to the license plate database for only permissible use, and/or regularly monitoring access to data stored under this General Order.

(c) **HOT LIST -** A cross-reference from vehicle license plate scans with information associated with vehicles of interest. This list includes but is not limited to license plates listed as stolen, B.O.L.O., SILVER and AMBER alerts, or wanted individuals with a Class A offense or greater warrant.

344.3 PROCEDURE

344.3.1 MANAGEMENT OF ALPR

(a) The Auto Theft Interdiction Unit will manage the ALPR program.
    1. The Chief Security Officer is the Sergeant of the Auto Theft Unit.
(b) Operators encountering problems with ALPR equipment or programs will notify the Chief Security Officer.

344.3.2 ASSIGNMENT, USE, AND LOCATIONS OF ALPR SYSTEMS

(a) Real time Crime Center (RTCC) personnel will monitor all ALPR systems. All RTCC personnel will be trained on using and interpreting ALPR systems.
    1. RTCC will either dispatch alerts received, generally broadcast (GB) them, or notify patrol.
(b) An ALPR alert alone, including an alert sent by RTCC, does not create reasonable suspicion to justify a traffic stop or the detention of an individual. Before making a stop or detention, the officer will:
    1. Make a visual confirmation that the license plate actually matches the information captured by the ALPR and reported in the corresponding alert.
    2. Confirm the license plate information with the National and Texas Crime Information Centers (NCIC/TCIC).
    3. In the absence of exigent circumstances and if it is safe and reasonable under the circumstances, a second officer will verify that the license plate matches the hit before officers take enforcement action.
        (a) Investigators conducting follow-up investigations shall always use a second officer to verify the license plate match before taking any action.
    4. Officers conducting a traffic stop based on a confirmed ALPR alert will consider the level of risk associated with the nature of the offense and ensure that their response complies with all applicable laws and General Orders.
(c) The Chief Security Officer will work with the Police Technology Unit (PTU) and Research and Planning to ensure all permanent ALPR cameras are located at various points throughout the city to ensure the deployment of permanent ALPR cameras will not be placed in places more likely to target any group or segment of our community disproportionately.

344.4 SAFEGUARDS

(a) Prohibited use:
   1. When using ALPR systems, officers will not target any person based on their actual or perceived race, color, religion, creed, sex, gender, gender identity, sexual orientation, age, national origin, ethnicity, disability, veteran status, marital status, partnership status, pregnancy status, political affiliation or beliefs, and, to the extent permitted by law, alienage or citizenship status.
   2. Users will not employ ALPR systems to intimidate or harass any individual or group.
   3. Employees shall not obtain, attempt to obtain, or convert any data obtained with ALPR for their personal use or the unauthorized use of another person. Department personnel will only access and use the ALPR system for official and legitimate law enforcement purposes consistent with this General Order.
   4. Unless there is a criminal nexus, officers will not use the ALPR system or use, retain, or transmit license plate reader data to investigate persons who are, or were, exercising their First Amendment right, including freedom of speech, assembly, association, and exercise of religion, such as attending political rallies, organizational meetings, public demonstrations, and religious gatherings.
   5. Operators will not use or operate ALPR systems or ALPR data for warrant round-up operations, operations focused on collecting past due traffic fines, Class C Misdemeanors, or any other similar purpose of generating revenue or collecting money owed by the public.
   6. APD personnel will not use ALPR systems or ALPR data for the purpose of conducting criminal investigations regarding a person's immigration status or access to reproductive health services, to the extent legally possible.
   7. Any alleged misuse or inappropriate application of ALPR operations, information, data, or software will be investigated pursuant to GO 902 Administrative Investigations and subject to appropriate disciplinary action if the allegation is substantiated.

(b) If any officer or employee reasonably believes that another law enforcement agency has used or is using APD ALPR systems or data in a manner that violates the "Prohibited Uses" identified herein, the officer or employee will report that information to the Auto Theft Interdiction Unit Lieutenant. The Lieutenant will review the possible violation and determine if sharing ALPR data with the outside agency will continue.

(c) The Chief Security Officer shall oversee access to the ALPR database and will limit roles and access depending on the user's role and need for access. The Chief Security Officer shall closely coordinate with CTM to ensure the implementation of the best data security and storage practices for all ALPR data. APD will store all collected ALPR data on a designated ALPR server unless investigators retain and save the data for a criminal investigation.

(d) Server operators will purge ALPR data from the designated ALPR server 30 days after an ALPR collects it. The retention period for ALPR data will comply with state law. All logins and transactions are logged within the ALPR system and audited to ensure proper use and whether there is a criminal predicate.

(e) For ALPR data related to ongoing criminal investigations or criminal investigations that contain ALPR as evidence, investigators must download and record the relevant ALPR data into the case file.

(f) The Department shall retain all ALPR data related to an endangered, missing person, or criminal investigation for a period consistent with the City of Austin's Records Management Ordinance, Chapter 2-11, and any applicable City Records Control Schedules and/or the State Local Government Retention Schedules.

(g) When an officer takes any action due to an ALPR alert, but it is later discovered that the action they took was against the wrong vehicle due to any error in data entry, fictitious or swapped license plates, or interpretation of the license plate, the officer will email the incident details to their supervisor and Risk Management before the end of their shift. Risk Management will include this data in the next quarterly audit, per GO 344.6 Audit.

344.5 RELEASE OF DATA

(a) ALPR data shall not be distributed, sold, or transferred to any non-law enforcement entities.

(b) Data sharing with other law enforcement agencies will only occur for vehicles on the hot list due to locating missing or endangered persons or due to a documented ongoing criminal investigation.

(c) Requests for ALPR data shall be processed in accordance with Texas Government Code, Chapter 552, and General Order 116 (Security and Release of Records and Information). If required by law to share or disclose this data, APD will supply the requested information for a specific case or investigation only to the extent legally required.

(d) The Chief of Police, or a designee, will be promptly notified if a request for information is broader than a specific case or investigation. This notification will enable APD to fulfill its obligation to report that request to the Office of Police Oversight, Mayor, and Council prior to sharing any information.

344.6 AUDIT

The Risk Management Unit will conduct audits of the ALPR system. They will present the audit results to the Chief of Police or their designee, which may be public information as allowed by law. At minimum:

(a) The Risk Management Unit will perform a quarterly random audit of the system to ensure compliance with policies and procedures.

(b) This audit shall include, but is not limited to:

1. The number of license plates scanned.
2. The names of the lists against which captured plate data were checked, and the number of confirmed matches and the number of matches that, upon further investigation, did not correlate to an alert.
3. The number of matches that resulted in the arrest, prosecution, or location of a missing or endangered person.
4. The number of preservation requests received broken down by the number of requests by a governmental entity versus by a defendant.
5. The number of data sharing requests received, granted, and denied broken down by agency.
6. The number of data sharing requests resulting in arrest, prosecution, or the location of a missing or endangered person.
7. The number of manually-entered license plate numbers under Section 1, broken down by reason justifying the entry, and the number of confirmed matches and the number of matches that, upon further investigation, did not correlate to an alert broken down by user access roles.
8. Any changes in Austin Police Department policy that affect privacy concerns.
9. License plate hits, categorized by zip code and sector, and the type of camera that captured the data.
10. Data gathered during a detention that does not result in an investigation, per this order 344.4 (g).
11. Information regarding the race and gender of the driver of any vehicle detained as a result of ALPR action.
12. Information regarding the race and gender of the victim of the crime reported resulting in the ALPR action.
13. Information regarding the offense under investigation regarding any ALPR action taken.

(c) The Risk Management Unit will assist the City Auditor or an external party directed by the City Auditor with Audits. Information shared for the purposes of this audit is not subject to section 344.5 (a) above.

344.7 TRAINING

(a) Any personnel who will be utilizing the ALPR system must complete annual training on the policies and restrictions regarding ALPR use, data handling, and processing requests for ALPR data. Among other topics, this training will cover:
   1. Appropriate use and collection of ALPR data and emphasize the requirement to document the reason for the inquiry;
   2. APD Policy 344.4 Safeguards;
   3. Examples of negative consequences resulting from misuse; and
   4. A clear explanation and warning that the current driver of any vehicle may not be the person who is wanted by law enforcement in connection with the license plate being included in a hotlist.

(b) No employee shall access, use, view, or otherwise participate in the ALPR program unless and until the employee completes this annual training. Employees who have previously completed the training but fail to timely complete subsequent annual training shall have their access to ALPR systems revoked until they complete the required training.