INDEPENDENT AUDITOR'S REPORT

Duluth Police Department

SEPTEMBER 26TH, 2026

RAMPART AUDIT LLC

Automated License Plate Reader Audit Report

Dear Chief Ceynowa:

We have audited the Duluth Police Department's (DPD) Automated License Plate Reader (ALPR) program for the period of February 1, 2025, through August 12, 2026.

The purpose of this audit is to evaluate DPD's compliance with Minn. Stat. §13.824, which sets forth requirements and prohibitions governing the use of ALPRs and the collection, use, management and destruction of ALPR data, and Minn. Stat. §626.8472, which mandates that the chief law enforcement officer (CLEO) of any agency that maintains an ALPR system in Minnesota establish and enforce a written policy governing the use of the system, and also sets forth minimum requirements for the ALPR system policy.

Minn. Stat. §13.824 Subd. 6 requires that an agency shall arrange for an independent, biennial audit of its ALPR records "to determine whether data currently in the records are classified, how they are used, whether they are destroyed as required… and to verify compliance with [Minn. Stat. §13.824] Subdivision 7," which governs authorization to access data. This program and its associated data are the responsibility of the Duluth Police Department. Our responsibility is to express an opinion on the operations of this program based on our audit.

On August 13, 2026, Rampart Audit, LLC (Rampart) met with Lieutenant Joel Olejnicak, Investigator Morgan Cekalla and Digital Evidence Specialist Erik Isakson, who provided information about DPD's ALPR program and facilitated access to DPD ALPR data by running reports and retrieving sample data at the direction of Rampart. Please note that all ALPR data access undertaken for the purpose of this audit occurred between the hours of 1:00 PM and 2:30 PM on 8/13/2026 and was logged in the ALPR system with a reason code of "Rampart ALPR audit." No direct system access was granted to the auditors, nor was any data downloaded by the auditors.

ALPR PROGRAM

Duluth Police Department personnel advised us that DPD operates both mobile and stationary ALPRs, and that the systems were implemented during February of 2025.

DPD employs the Axon Fleet mobile ALPR system, which utilizes optical character recognition (OCR) technology built into the existing in-car cameras installed in DPD squads. At the time of our audit, DPD had deployed 49 Axon Fleet ALPRs. We note that the number of mobile ALPRs deployed may vary temporarily as squads are retired from service and replaced.

The Axon ALPR system compares each scanned license plate to two databases. The Minnesota License Plate Data File contains a limited version of the Minnesota DVS database, including a list of those vehicles registered to individuals whose driving status is identified as suspended, revoked, canceled or disqualified. This file also contains FBI NCIC data related to stolen and felony vehicles, wanted persons and attempts to locate. The Manual Hot List File contains a list of license plates related to active investigations which have not been entered into the Minnesota License Plate Data file. While these databases may be updated multiple times per day, they are not considered "live" data.

The Axon system integrates with the squad's mobile data terminal (MDT), and is normally active whenever the camera is powered on. The ALPR software runs in the background and the vast majority of license plate reads require no action on the part of the officer. When the ALPR identifies a possible match to a license plate listed in one of the databases listed above, or "hit," it triggers an audible alert and activates a window on the MDT to display information about the alert, including the nature of the hit and two images: a close-up of the license plate, and a wide-angle view that shows portions of the vehicle and the area immediately surrounding the vehicle. If an officer is unable to review a hit when it occurs, it is placed into a queue and is available for review at a later time.

In most instances, the officer is able to dismiss a hit alert without taking further action. Common reasons for hit dismissals include scans of parked vehicles indicating that the registered owner lacks a valid driving status, state mismatches and misread plate numbers. Officers will also dismiss or ignore alerts that result from scans that occur while responding to higher priority calls. Officers are required to confirm the hit information through the appropriate live database (DVS or NCIC) before taking enforcement action.

Data from mobile ALPR scans, including hit data, upload wirelessly to Axon's secure cloud storage service, Evidence.com. DPD retains mobile ALPR data for 60 days, after which it is permanently deleted. ALPR data is retained beyond 60 days only when classified as active investigatory data, or when so requested in writing by an individual who is the subject of a criminal investigation and who identifies the data as potential exculpatory evidence. Any ALPR data to be retained beyond 60 days is exported through a manual process to a separate Evidence.com database and is retained as evidence. Evidentiary ALPR data is retained until manually purged, unless the officer fails to assign a category, in which case it is purged after 90 days.

Duluth Police Department also employs a total of ten Flock Safety stationary ALPRs. These cameras are positioned at nine (9) intersections within the city and operate continuously; however, DPD personnel advised us during the audit that all of these cameras had been turned off as of the date of our audit.

Data from stationary ALPR scans, including hit data, upload wirelessly to Flocksafety.com, which utilizes Amazon Web Service's GovCloud for secure CJIS storage. Stationary ALPR data is retained for 30 days, though recent news media reporting has indicated that Flock intends to reduce its ALPR retention to a default period of seven (7) days. Any stationary ALPR data to be retained beyond the standard retention period is exported through a manual process to the same Evidence.com database as mobile evidentiary ALPR data and is retained until manually purged, unless the officer fails to assign a category to the data,

in which case the data is purged after 90 days. The Flock system is able to provide hit notifications through email and text message, based on each user's preference.

At the time of our audit, DPD retained records of 2,820,611 mobile ALPR reads over the preceding 60 days, and 586,800 stationary ALPR reads over the preceding 30 days. These reads included a combined total of 89,527 hits.

ALPR POLICY

As noted above, Minn. Stat. §626.8472 states:

> The chief law enforcement officer of every state and local law enforcement agency that maintains an automated license plate reader shall establish and enforce a written policy governing use of the reader. Use of an automated license plate reader without adoption of a written policy under this section is prohibited. At a minimum, the policies and procedures must incorporate the requirements of section 13.824, and the employee discipline standards for unauthorized access to data contained in section 13.09.

Rampart reviewed a copy of Duluth Police Department's ALPR policy, a copy of which is attached to this report as Appendix A, and compared it to the requirements and prohibitions contained in Minn. Stat. §13.824 and Minn. Stat. §626.8472. In our opinion, DPD's ALPR policy addresses all of the mandatory elements identified in the statute, except for the employee discipline standards for unauthorized access to ALPR data, which is a requirement specified in Minn. Stat. §626.8472. Prior to the completion of this report, Duluth Police Department submitted a revised ALPR policy that addresses that requirement. A copy of the policy is attached to this report as Appendix B.

DATA COLLECTION

Minn. Stat. §13.824 Subd. 2 limits ALPR data collection to the following elements:

1. License plate numbers;
2. Date, time and location data on vehicles; and
3. Pictures of license plates, vehicles and areas surrounding the vehicles.

Rampart selected a random sample of license plate scans from both the Axon and Flock systems. We reviewed the sample data against the list of permitted data elements above and verified that both systems collected only the elements listed.

Axon's ALPR system employs artificial intelligence (AI) to analyze the photos and develop what it terms Vehicle Attribute Recognition (VAR) data. This includes details such as the vehicle's make, model, body style and color, as well as the license plate's state of issuance. Each element is given a probability score, Axon's estimate as to the reliability of its analysis. This data is retained along with the §13.824 Subd. 2

data. We noted that these VAR elements are not "collected," but rather are the product of AI analysis that is applied to the photographs collected under Subd. 2.

Similar to the Axon system, Flock's ALPR system employs artificial intelligence (AI) to analyze the photos and develop what it terms Vehicle Fingerprint (VF) data. This includes details such as the vehicle's make, model, body style and color; unique elements such as roof racks, stickers or damage; as well as the license plate's state of issuance. In addition, Flock Safety's website describes its system as possessing at least limited ability to identify vehicles based on VF elements, even in the absence of a license plate. As with the Axon VAR data, we noted that these VF elements are not "collected," but rather are the product of AI analysis that is applied to the photographs collected under Subd. 2.

Both ALPR systems also record the identity of the camera conducting each read, and the Axon system records any response to a hit entered by a user. We noted that these details are not data collected by the license plate reader itself, but rather could be deemed metadata – that is, additional data about the ALPR read or hit data that are necessary for auditing and classification purposes.

DATA CLASSIFICATION

Minn. Stat. §13.824 Subd. 2(b) states:

> All data collected by an automated license plate reader are private data on individuals or nonpublic data unless the data are public under section 13.82, subdivision 2, 3, or 6, or are active criminal investigative data under section 13.82, subdivision 7.

The Data Classification section of DPD's ALPR policy identifies ALPR data as "private or non-public, unless the data is part of an active criminal investigation," in which case it would be classified as confidential, or as public data if it meets one of the exceptions listed Minn. Stat. §13.824 Subd. 2, 3 or 6.

In order to obtain access to DPD ALPR data, a requesting agency is normally required to submit a written request using the department's records request portal, though email, phone or in-person requests are accepted when exigent circumstances exist, or when DPD personnel are actively assisting with the requesting agency's investigation.

Written requests are reviewed by the Data Release Coordinator, though supervisors at the rank of sergeant or above are authorized to respond to requests that are exigent in nature. In addition, investigators are authorized to share relevant data when actively assisting another agency. In some instances, DPD could require that the requesting agency obtain a warrant for the data. We recommend that DPD retain copies of all written requests for audit purposes, and that verbal requests be documented in a CFS or incident report as appropriate.

Because both Axon and Flock evidentiary downloads are stored in Axon's Evidence.com, data from both systems is shared with other Axon customers via the case sharing function, while a downloadable link is provided for non-Axon customers. DPD's Axon data sharing mechanisms include a written reminder for

the receiving agency of that agency's data privacy responsibilities under the governing statute, which we recommend.

Requests for ALPR data from data subjects are submitted to the DPD Records department. Requests submitted in person require a photo ID, while requests submitted online require a signed and notarized request form in order to release private data. These requirements are intended to ensure that private data are released only to the data subject.

PUBLIC LOG OF USE

Minn. Stat. §13.824 Subd. 5(a) requires that "[a] law enforcement agency that installs or uses an automated license plate reader must maintain a public log of its use…" and requires that the agency maintain the following data as part of the log:

1. Specific times of the day that the reader actively collected data;
2. The aggregate number of vehicles or license plates on which data were collected for each period of active use;
3. A list of all state and federal databases with which the data were compared, unless the existence of the database itself is not public;
4. For each period of active use, the number of vehicles or license plates in each of the following categories:
    a. The vehicle or license plate has been stolen;
    b. There is a warrant for the arrest of the owner of the vehicle;
    c. The owner of the vehicle has a suspended or revoked driver's license or similar category; or,
    d. The data are active investigatory data
5. For fixed or stationary readers, the location at which the reader is installed and used and actively collected data.

A complete list of Duluth Police Department's stationary ALPRs is available on the Minnesota Bureau of Criminal Apprehension website. All of the stationary ALPRs are operational at all times. The Flock system captures the remaining elements from the list above.

The Axon system also captures the required data elements; however, as of the date of our audit, it was not clear whether Axon offered a pre-programmed report capable of providing information about the specific times of the day that each ALPR actively collected data. We noted that this requirement might require clarification from the legislature as to whether the log would need to list the time of each individual scan, or whether a summary report listing the times of the first and last scan of each day would suffice. Alternatively, because Patrol squads are shared, it may suffice to note that the Axon readers are effectively in continuous operation.

We noted that the statute provides limited guidance to the agency for creating the public log of use. While it identifies the required data elements, it doesn't specify how frequently the log should be

produced or how long it should be retained. We did note that the General Records Retention Schedule for Minnesota Cities recommends that an ALPR public log of use be retained for two years.

As part of the audit, Rampart reviewed DPD's "transparency portal" for each system, which provides information similar to that which is required by the public log of use. While the transparency portal data does not satisfy all of the requirements specified for the public log of use, those remaining data elements are captured by the systems. Because ALPR data is purged on a daily basis as the retention period expires, we recommend archiving a copy of each system's transparency portal periodically in order to avoid the loss of summary data.

NOTIFICATION TO THE BCA OF THE LOCATION OF ANY FIXED/STATIONARY ALPRs

Minn. Stat. §13.824 Subd. 5(b) requires that:

> The law enforcement agency must maintain a list of the current and previous locations, including dates at those locations, of any fixed stationary automated license plate readers or other surveillance devices with automated license plate reader capability used by the agency. The agency's list must be accessible to the public, unless the agency determines that the data are security information as provided in section 13.37, subdivision 2. A determination that these data are security information is subject to in-camera judicial review as provided in section 13.08, subdivision 4.

As noted in the preceding section, Duluth Police Department had deployed 10 stationary ALPRs at the time of our audit. As part of this audit, DPD personnel reviewed the map of stationary ALPR locations in their Flock software with our auditor. Rampart compared this map to the list published on the Minnesota Bureau of Criminal Apprehension website and verified that both were identical.

We noted that while both state statute and DPD's ALPR policy require that the agency maintain a list of previous locations, the statute does not indicate how long the list of previous locations must be maintained. In the absence of authoritative guidance, Rampart recommends that such data be maintained for two years. DPD personnel advised us that none of the agency's stationary ALPRs have been moved since their initial placement. We recommend retaining copies of the emails used to notify the BCA of the initial placement, as well as copies of any emails documenting the future movement of ALPRs, to ensure historical location information is available for at least two years.

ALPR DATA ACCESS CONTROLS

Minn. Stat. §13.824 Subd. 7(c) requires that:

> The ability of authorized individuals to enter, update, or access automated license plate reader data must be limited through the use of role-based access that corresponds to the official duties or training level of the individual and the statutory authorization that grants access for that purpose. All queries and responses, and all actions in which data are entered, updated,

accessed, shared, or disseminated, must be recorded in a data audit trail. Data contained in the audit trail are public, to the extent that the data are not otherwise classified by law.

DPD advised us that ALPR system access is role-based, as required by statute, and we reviewed a list of the available roles as part of this audit. All officers have access to search and respond to hits, while hotlist update access is limited to administrators.

Access to mobile ALPR data is granted to new DPD officers as part of the field training process, which includes a requirement that the officer read and sign off on the DPD ALPR policy. In addition, officers complete CJIS training, PATROL online training and City of Duluth online training. Access to stationary ALPR data is limited to lieutenants, sergeants and investigators, as well as one (1) analyst and six (6) administrators, and requires the completion of additional Flock-specific training courses that address searches, alerts and data administration.

ALPR DATA AUDIT TRAIL

DPD personnel ran an Audit Trail Report for each ALPR system. While both systems were able to produce an audit log, we noted that the Axon audit trail is currently unrefined and difficult to read. The log we reviewed consisted of an Excel download with many of the data elements for each entry concatenated into a long alphanumeric string. This is consistent with Axon logs we have reviewed as part of other audits and appears to be a limitation of the system. While we were able to use the log in its current form to review activity, we encouraged DPD to request that Axon develop a more user-friendly audit trail report.

The Axon system requires an officer to enter either a case number or a search reason prior to searching ALPR data, while the Flock system requires either an offense type or a search reason. The auditor reviewed a sample of searches recorded in the audit trail, verifying the listed case number and/or search reason for each against the corresponding case in the DPD records management system. The auditor determined that the searches were adequately documented and appeared to be appropriate.

DPD personnel also advised us that the Flock system includes an internal audit function that flags certain types of activity, such as repeated searches for a particular license plate. This alert requires supervisory review of the searches before the flag can be cleared. DPD personnel advised us that they have received three (3) such alerts, and that supervisors reviewed all three to verify that the searches were both appropriate in nature and related to active cases.

ALPR DATA DESTRUCTION

Minn. Stat. §13.824 Subd. 3(a) requires that ALPR data be destroyed no later than 60 days from the date of collection, subject to certain exceptions. Duluth Police Department's policy specifies a 60-day retention policy for ALPR data, though Flock Safety's default retention period is 30 days. (As noted earlier in this report, Flock has recently announced its intention to reduce this retention period to seven [7]

days.) Software settings in both systems automatically delete permanently any data contained in the respective ALPR database once it reaches the corresponding data retention limit. As discussed earlier in this report, by statute ALPR data can be retained beyond 60 days only when identified as active investigatory data, or when requested in writing as potential exculpatory evidence. In such cases, the ALPR data is then manually exported to a separate evidentiary database within Evidence.com.

As part of the audit, DPD personnel ran reports to list any retained ALPR data within the two ALPR systems' databases that was more than 60 days old. The reports showed no retained data beyond each system's corresponding retention period. Any ALPR data retained as evidence is stored in a separate evidentiary database, as described above.

Rampart also reviewed three evidentiary exports to confirm both the retained data elements and the separate storage location. The auditor also reconciled the retained data to the corresponding ICR.

INTERNAL CONTROL RECOMMENDATIONS

As noted above, DPD personnel advised us that all officers have access to respond to hits and conduct searches in the ALPR systems, while hotlist updates are limited to administrators. Mobile ALPR data access is granted as part of the field training process after the officer signs off on the ALPR policy and completes training on its use and requirements, while stationary ALPR data access requires additional training modules.

Users conducting searches in either ALPR system are required by policy to provide "the factual basis for the access and any associated case number, complaint, or basis for the access." Both systems force the user to provide a case number and/or search reason before performing a search. DPD personnel advised us that access is logged and reviewable in the audit trails of both ALPR systems.

DPD personnel advised us that the Flock system enforces internal audit reviews when certain conditions are met, such as repeated searches of the same license plate, but that internal audits are not otherwise conducted.

We recommend that a minimum of two administrators or supervisors conduct periodic reviews or internal audits to review data access, and document such reviews in the ALPR system with a reason code of "admin audit" or a similar meaningful description. Doing so will avoid requiring an employee to review his or her own activity.

We recommend conducting the following internal audit tests periodically, subject to the limitations of the audit trail report of each ALPR system:

1. Review any license plates that are searched multiple times.
2. Conduct random reconciliations of license plate searches to the case number listed in the audit log as the reason for the search, to ensure the search was appropriate.
3. Conduct random reviews of individual users' use to evaluate the appropriateness of access, as well as verifying the completeness of the data elements associated with each search.

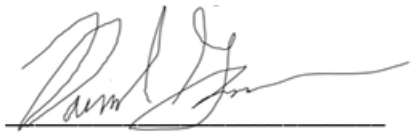
We recommend documenting these tests via email or other writing to create an internal ALPR audit log. We recommend that the documentation include the following elements:

- The identities of DPD staff conducting the internal audit.
- The purpose of the audit.
- The tests conducted and the purpose of each test.
- The results of the audit.

We also recommend ensuring that audit log data are retained for a minimum of thirty (30) months, to accommodate biennial audits.

AUDIT RESULTS

Based on our review of Duluth Police Department's ALPR policy and operations, as well as the on-site tests conducted and data reviewed as part of our audit, it is our opinion that DPD's ALPR program is compliant with the requirements of Minn. Stat. §13.824 and §626.8472



Rampart Audit, LLC

9/26/2026

APPENDIX A:

DULUTH PD MN Policies and Data Library

DULUTH POLICE DEPARTMENT POLICY MANUAL

Automated License Plate

Readers Policy#: 3.5.9

Effective Date: 5/18/2026

I. PURPOSE

This policy is intended to provide guidance on the use of an Automated License Plate Reader (ALPR) and the maintenance and use of the data collected by these systems.

II. DEFINITIONS

AUTOMATED LICENSE PLATE READER (ALPR) (defined by Minn. Stat. § 13.824. subd. 1(b).)

- an electronic device mounted on a law enforcement vehicle or positioned in a stationary location that is capable of recording data on or taking a photograph of a vehicle or its license plate and comparing the collected data and photographs to existing law enforcement databases for investigative purposes. Automated License Plate Reader includes a device that is owned or operated by a person who is not a government entity to the extent that data collected by the reader are shared with a law enforcement agency. Automated license plate reader does not include a traffic safety camera system.

III. GUIDELINES

A. Installation or Integration of an ALPR

1. Within ten (10) days of the installation or current use of an ALPR or the integration of automated license plate reader technology into another surveillance device, the Chief or the Chief's designee shall notify the Bureau of Criminal Apprehension (BCA) of that installation or use and of any fixed location of a stationary ALPR. Minn. Stat. § 13.824, subd. 8 (g)..

B. Authorization and Use of an ALPR

1. Only department personnel trained in the proper use of the ALPR system may access and operate the system. Access to the ALPR system shall be authorized by the Chief or the Chief's designee, prior to personnel obtaining access.
2. The ALPR system shall only be used for official and legitimate law enforcement purposes.
3. Operators receiving an alert on the ALPR system shall obtain independent verification of the information associated with the alert prior to taking any enforcement action.
4. An ALPR shall not be used to monitor or track an individual who is the subject of an active criminal investigation unless authorized by a warrant, issued upon probable cause, or exigent circumstances justify the use without obtaining a warrant. Minn. Stat. § 13.824, subd 2 (g)_,_
5. Documentation
    a. All data queries shall include the factual basis for the access and any associated case number, complaint, or basis for the access.
    b. The department will maintain a public log of use. Any ALPR use shall be documented in the log, unless the department determines the data is exempt pursuant to Minn. Stat. § 13.37, subd. 2. Documentation in the log shall include:

        Specific times and dates when ALPR data was collected;

The aggregate number of vehicles or license plates

on which data was collected for each period of active use and a list of all state and federal databases which the data was compared to, unless the existence of the database is not public;

The number of vehicles or license plates identified by an ALPR where the ALPR alet1ed to each of the following categories: stolen vehicle or license plate, warrant for the arrest of the owner of the vehicle, an owner with a suspended or revoked driver's license or similar category, or an active investigation alert (KOPS); and

For stationary ALPR's, the location where the ALPR was installed and used while collecting data, including a list of current and previous locations documenting dates at those locations for use.

C. Data Collection

1. Pursuant to Minn. Stat. § 13.824, subd. 2(g), data collected from an ALPR shall be limited to:
   a. License plate numbers;
   b. Date, time and location data on vehicles; and
   c. Pictures of license plates, vehicles and areas surrounding the vehicles.

D. Data Classification

1. All data collected by an ALPR shall be classified as private and nonpublic, unless the data is part of an active criminal investigation, under Minn. Sta. § 13.82, subd. *2,* or is within a specific exception as provided in Minn. Stat. § 13.82, subds.2, 3, or Q.

E. Data Distribution

1. ALPR information gathered and retained by the department may be used and shared with prosecutors and other law enforcement agencies for legitimate law enforcement purposes, or as otherwise permitted by law, in compliance with Minn. Stat. § 13.824, subd. 4.

2. ALPR data that is not related to an active criminal investigation may not be shared with, disseminated to, sold to or traded with other individuals or entity unless explicitly authorized by law.

F. Data Retention and Destruction

1. Data collected by an ALPR that is not related to an active criminal investigation must be destroyed no later than sixty (60) days from the date of collection, unless otherwise prescribed by law. Minn. Stat. § 13.824, subd. 3(g).

2. Upon written request from an individual who is the subject of a pending criminal charge or complaint, along with the case or complaint number and a statement that the data may be used as exculpatory evidence, ALPR data otherwise subject to destruction must be preserved by the department until the criminal charge or complaint is resolved or dismissed. Minn. Stat. § 13.824, subd. 3(b).

G. Records and Audits

1. The department shall maintain a list of the current and previous locations, including dates at those locations, of any fixed stationary ALPR or other surveillance device with ALPR capability used by the department. Minn. Stat. § 13.824, subd. S(b).. This list shall be accessible to the public, unless the department determines that the data constitutes security information as provided by Minn. Stat. § 13.37, subd. 2.

2. The department shall maintain records showing the date and time ALPR data was collected and the applicable classification of the data.

3. The department shall arrange for an independent, biennial audit of the records to determine whether data currently in the records are classified, how the data are used, whether they are destroyed as required by statute, and to verify compliance with all rules and regulations. Minn. Stat. § 13.824, subd 6 ( ).

4. A report summarizing the results of each audit shall be provided to the commissioner of administration, to the chairs and ranking minority members of the committees of the house of representatives and the senate with jurisdiction over data practices and public safety issues and to the Legislative Commission on Data Practices and Personal Data privacy no more than thirty (30) days following completion of a biennial audit. Minn. Stat. §13.824, subd. 6 ( )..

© 2026 DULUTH PD MN Policies and Data Library· by MAGNUSIONE • Categories • 19.gin • All Rights Reserved

APPENDIX B:

DULUTH POLICE DEPARTMENT POLICY MANUAL
Automated License Plate Readers

Policy #: 3.5.9
Effective Date: 5/18/2026

I. PURPOSE

This policy is intended to provide guidance on the use of an Automated License Plate Reader (ALPR) and the maintenance and use of the data collected by these systems.

II. DEFINITIONS

AUTOMATED LICENSE PLATE READER (ALPR) (defined by Minn. Stat. § 13.824, subd. 1(b)) – an electronic device mounted on a law enforcement vehicle or positioned in a stationary location that is capable of recording data on or taking a photograph of a vehicle or its license plate and comparing the collected data and photographs to
existing law enforcement databases for investigative purposes. Automated License Plate Reader includes a device that is owned or operated by a person who is not a government entity to the extent that data collected by the reader are shared with a law enforcement agency. Automated license plate reader does not include a traffic safety camera system.

III. GUIDELINES

A. Installation or Integration of an ALPR

1. Within ten (10) days of the installation or current use of an ALPR or the integration of automated license plate reader technology into another surveillance device, the Chief or the Chief's designee shall notify the Bureau of Criminal Apprehension (BCA) of that installation or use and of any fixed location of a stationary ALPR. Minn. Stat. § 13.824, subd. 8 (a).

B. Authorization and Use of an ALPR

1. Only department personnel trained in the proper use of the ALPR system may access and operate the system. Access to the ALPR system shall be authorized by the Chief or the Chief's designee, prior to personnel obtaining access.

2. The ALPR system shall only be used for official and legitimate law enforcement purposes.

3. Operators receiving an alert on the ALPR system shall obtain independent verification of the information associated with the alert prior to taking any enforcement action.

4. An ALPR shall not be used to monitor or track an individual who is the subject of an active criminal investigation unless authorized by a warrant, issued upon probable cause, or exigent circumstances justify the use without obtaining a warrant. Minn. Stat. § 13.824, subd 2 (d).

5. Documentation

    a. All data queries shall include the factual basis for the access and any associated case number, complaint, or basis for the access.

    b. The department will maintain a public log of use. Any ALPR use shall be documented in the log, unless the department determines the data is exempt pursuant to Minn. Stat. § 13.37, subd. 2. Documentation in the log shall include:

        i. Specific times and dates when ALPR data was collected;

        ii. The aggregate number of vehicles or license plates on which data was collected for each period of active use and a list of all state and federal databases which the data was compared to, unless the existence of the database

is not public;

iii. The number of vehicles or license plates identified by an ALPR where the ALPR alerted to each of the following categories: stolen vehicle or license plate, warrant for the arrest of the owner of the vehicle, an owner with a suspended or revoked driver's license or similar category, or an active investigation alert (KOPS); and

iv. For stationary ALPR's, the location where the ALPR was installed and used while collecting data, including a list of current and previous locations documenting dates at those locations for use.

C. Unauthorized Use

1. Personnel shall access, use, and disseminate ALPR data only as authorized by this policy and Minn. Stat. ch. 13.

2. A willful violation of Minn. Stat. ch. 13, of any rule adopted under that chapter, or of the provisions of this policy implementing that chapter, by any department employee constitutes just cause for suspension without pay or dismissal. Minn. Stat. § 13.09(b).

3. Any employee who willfully violates Minn. Stat. ch. 13 or rules adopted under it, or whose conduct constitutes the knowing unauthorized acquisition of not public data, is guilty of a misdemeanor. Minn. Stat. § 13.09(a). Suspected criminal violations may be referred to the appropriate prosecuting authority, and administrative discipline shall proceed independently of any referral or charge.

D. Data Collection

1. Pursuant to Minn. Stat. § 13.824, subd. 2(a), data collected from an ALPR shall be limited to:

   a. License plate numbers;

   b. Date, time and location data on vehicles; and

   c. Pictures of license plates, vehicles and areas surrounding the vehicles.

E. Data Classification

1. All data collected by an ALPR shall be classified as private and nonpublic, unless the data is part of an active criminal investigation, under Minn. Sta. § 13.82, subd. 2, or is within a specific exception as provided in Minn. Stat. § 13.82, subds.2, 3, or 6.

F. Data Distribution

1. ALPR information gathered and retained by the department may be used and shared with prosecutors and other law enforcement agencies for legitimate law enforcement purposes, or as otherwise permitted by law, in compliance with Minn. Stat. § 13.824, subd. 4.

2. ALPR data that is not related to an active criminal investigation may not be shared with, disseminated to, sold to or traded with other individuals or entity unless explicitly authorized by law.

G. Data Retention and Destruction

1. Data collected by an ALPR that is not related to an active criminal investigation must be destroyed no later than sixty (60) days from the date of collection, unless otherwise prescribed by law. Minn. Stat. § 13.824, subd. 3(a).
2. Upon written request from an individual who is the subject of a pending criminal charge or complaint, along with the case or complaint number and a statement that the data may be used as exculpatory evidence, ALPR data otherwise subject to destruction must be preserved by the department until the criminal charge or complaint is resolved or dismissed. Minn. Stat. § 13.824, subd. 3(b).

H. Records and Audits

1. The department shall maintain a list of the current and previous locations, including dates at those locations, of any fixed stationary ALPR or other surveillance device with ALPR capability used by the department. Minn. Stat. § 13.824, subd. 5(b). This list shall be accessible to the public, unless the department determines that the data constitutes security information as provided by Minn. Stat. § 13.37, subd. 2.

2. The department shall maintain records showing the date and time ALPR data was collected and the applicable classification of the data.

3. The department shall arrange for an independent, biennial audit of the

records to determine whether data currently in the records are classified, how the data are used, whether they are destroyed as required by statute,
and to verify compliance with all rules and regulations. Minn. Stat. § 13.824, subd 6 (a).

4. A report summarizing the results of each audit shall be provided to the commissioner of administration, to the chairs and ranking minority members of the committees of the house of representatives and the senate with
jurisdiction over data practices and public safety issues and to the Legislative Commission on Data Practices and Personal Data privacy no more than thirty
(30) days following completion of a biennial audit. Minn. Stat. §13.824, subd. 6 (c).