



# INDEPENDENT AUDITOR'S REPORT

---

Mankato Department of Public Safety



SEPTEMBER 4TH, 2026  
RAMPART AUDIT LLC

## **Automated License Plate Reader Audit Report**

Dear Director Clifton:

We have audited the Mankato Department of Public Safety's (MDPS) Automated License Plate Reader (ALPR) program for the period of July 24, 2025, through August 5, 2026.

The purpose of this audit is to evaluate MDPS'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 Mankato Department of Public Safety. Our responsibility is to express an opinion on the operations of this program based on our audit. MDPS personnel have advised us that it is their intent to obtain annual audits for the first three years of the ALPR program's operation in order to enhance transparency, and this is also noted in the ALPR policy itself.

On August 6, 2026, Rampart Audit, LLC (Rampart) met with Commander Justin Neumann, Records Supervisor Kay Schultz, Systems Administrator Jason Black and IT Director Doug Storm, who provided information about MDPS's ALPR program and facilitated access to MDPS 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 8/06/2026 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**

Commander Neumann advised us that MDPS operates both mobile and stationary ALPRs. The mobile ALPRs were implemented on July 24, 2025, while the first stationary ALPRs came online on November 20, 2025.

Mankato Department of Public Safety employs the Axon Fleet mobile ALPR system, which utilizes optical character recognition (OCR) technology built into the existing in-car cameras installed in MDPS squads.

At the time of our audit, MDPS had deployed 24 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. The screen will remain active until the officer provides a response to the hit.

In most instances, the officer is able to dismiss the 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 alerts that result from scans that occur while responding to higher priority calls. When an alert is not dismissed, 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. MDPS 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 until manually purged.

Mankato Department of Public Safety also employs a total of seven (7) Milestone Systems stationary ALPRs. These cameras are positioned at four (4) intersections within the city and operate continuously.

Data from stationary ALPR scans upload wirelessly to an in-house server maintained by City of Mankato IT staff. While settings in the XProtect software on the Milestone server allow ALPR data to be retained for a maximum of 60 days, in practice data is purged more frequently due to the server’s limited storage capacity. Any stationary ALPR data to be retained beyond 60 days is exported through a manual process to the same Evidence.com database as mobile evidentiary ALPR data and is retained until manually purged. The Milestone system is able to provide hit notifications through email and text message;

however, it is not currently linked to any license plate data files. As a result, while the data it collects can be searched manually, it does not identify hits.

At the time of our audit, MDPS retained records of 617,106 mobile ALPR reads, which included 6,377 hits during the preceding 60 days. While attempting to obtain a count of stationary ALPR reads during the audit, the Milestone system locked up at 50,000 entries. While IT staff were unable to resolve the issue during the on-site portion of our audit, they had previously reported a count of 154,895 stationary ALPR reads. The auditor verified that no data was retained beyond 60 days in either ALPR database.

## **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 Mankato Department of Public Safety's ALPR policy and compared it to the requirements and prohibitions contained in Minn. Stat. §13.824. In our opinion, MDPS's ALPR policy addresses all of the mandatory elements identified in the statute, including the employee discipline standards for unauthorized access to ALPR data. A copy of the policy has been attached to this report as Appendix A.

## **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 Milestone systems. We reviewed the sample data against the list of permitted data elements above. We noted that while both systems collected the elements from the list, the Milestone system recorded a short video segment as part of each scan. Because these videos consist of a series of sequential images of "license plates, vehicles and areas surrounding the vehicles," and because §13.824 Subd. 2 authorizes the collection of the plural term "pictures," it is our opinion that these brief recordings are consistent with statute.

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, Milestone's ALPR system employs artificial intelligence (AI) to analyze the photos and identify vehicle characteristics such as the vehicle's make, model, body style and color. As with the Axon VAR data, we noted that these 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.

While MDPS's ALPR policy does not explicitly state this, the access requirements and controls documented in the policy are appropriate for private or nonpublic data. In addition, MDPS personnel provided a copy of the agency's Public Safety Data Inventory, which documents the various types of data maintained by MDPS, including the classification of each data type and the controlling statute. This inventory references §13.824 Subd. 2 and identifies ALPR data as private, unless it is part of an active investigation, in which case it would be classified as confidential.

In order to obtain access to MDPS data, a requesting agency is required to submit a written request using an ALPR-specific form that includes the following:

- The name of the agency.
- The name of the person requesting the data.
- The intended purpose of the data.
- A record of the factual basis for the access and any associated case number, complaint or incident that is the basis for the access.
- A statement that the request is authorized by the head of the requesting law enforcement agency or his/her designee.

Such requests are normally reviewed by a member of MDPS command staff, though supervisors at the rank of sergeant or above are authorized to respond to requests that are exigent in nature. If approved, the supervisor creates an agency assist case or call for service in MDPS's Records Management System

(RMS) and documents the information listed above. In addition, MDPS retains a copy of the written request. In some instances, MDPS could require that the requesting agency obtain a warrant for the data.

We noted that the ALPR form includes a written reminder of the receiving agency's data privacy responsibilities under the governing statute, which we recommend.

Commander Neumann advised us that MDPS had received four (4) law enforcement requests during the period covered by this report. Rampart reviewed these requests, verifying that each one followed the procedures identified in MDPS' ALPR policy manual.

Requests for ALPR data from data subjects are submitted to the MDPS 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. Commander Neumann advised us that MDPS received four (4) requests for ALPR data from members of the public during the period covered by this report.

## **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 Mankato Department of Public Safety stationary ALPRs is available on the Minnesota Bureau of Criminal Apprehension website. All of the stationary ALPRs are operational at all times. The Milestone 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. Commander Neumann advised us that the MDPS shift schedule is currently used to determine this information.

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 MDPS's "transparency portal" for each system, which provides information similar to that which is required by the public log of use, as well as additional information about how ALPR data is, and is not, used. 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 on a monthly basis in order to avoid the loss of summary data. Commander Neumann advised us that MDPS had already adopted this practice prior to the audit.

#### **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 earlier in this report, Mankato Department of Public Safety had deployed seven (7) stationary ALPRs at the time of our audit. As part of this audit, Commander Neumann furnished a list of stationary ALPR locations. Rampart compared this list 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 MDPS'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. Commander Neumann advised us that none of the agency's 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. Commander Neumann advised us that he has retained both the notification emails to the BCA regarding the placement of each of MDPS' stationary cameras, as well as the response confirming the BCA's receipt of each, and will continue to do so.

### **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.

MDPS 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 supervisors and system administrators.

Access is granted to new MDPS officers as part of the field training process, which includes a requirement that the officer read and sign off on the MDPS ALPR policy.

### **ALPR DATA AUDIT TRAIL**

MDPS 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 MDPS to request that Axon develop a more user-friendly audit trail report.

The auditor reviewed a sample of searches recorded in the audit trail, verifying the listed case number and search reason for each against the corresponding case in the MDPS RMS system. The auditor determined the searches were clearly documented and appeared to be appropriate.

### **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 described earlier in this report. Mankato Department of Public Safety's policy specifies a 60-day retention policy for ALPR data. 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.

MDPS personnel advised us that the in-house server used to house Milestone ALPR data lacks sufficient storage to retain a full 60 days' worth of data; consequently, Milestone data is automatically purged prior to the end of the retention period as needed.

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

Rampart also reviewed an evidentiary export 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, Commander Neumann advised us that all officers have access to respond to hits and conduct searches in the ALPR systems, while hotlist updates are limited to supervisors. In addition, there are two MDPS system administrators with full access rights to the Axon system, while three City of Mankato IT staff have system administrator access to the Milestone system. ALPR 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.

Users conducting searches in either ALPR system are required by policy to provide both the associated case number and a search reason. While the Axon software physically enforces these requirements, the Milestone system does not; however, keystroke logging is utilized and the user ID and specific computer used is recorded each time data is accessed.

Commander Neumann advised us that access is logged and reviewable in the audit trails of both ALPR systems. He and the Administrative Records Clerk review access to the Axon system, while he and Senior Network Technician Black review Milestone access. Commander Neumann advised us that internal reviews are completed monthly and documented via email to Director of Public Safety Clifton and Deputy Chief of Police Baukol to create an internal ALPR audit log. As part of our audit, Commander Neumann provided an example of one of these emails. We noted that the email contained the following elements:

- The identities of MDPS 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 recommend that a minimum of two administrators or supervisors conduct periodic reviews or internal audits to review data access, and document such reviews 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. As noted above, MDPS follows this practice.

We recommend conducting the following internal audit tests, 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 noted that the internal audit memorandum provided by Commander Neumann indicated that the tests conducted addressed each of these recommendations.

We also recommend ensuring that audit log data are retained for a minimum of thirty (30) months, to accommodate biennial audits. Commander Neumann advised us that the Milestone system specifies a retention period of 144 years for audit logs, while Axon’s retention period is indefinite.

## AUDIT RESULTS

Based on our review of Mankato Department of Public Safety’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 MDPS’s ALPR program is compliant with the requirements of Minn. Stat. §13.824 and §626.8472



Rampart Audit, LLC

9/04/2026

# APPENDIX A:

Policy

**427**

Mankato Department of Public Safety

Mankato Dept of PS Policy Manual

---

## **Automated License Plate Readers (ALPR)**

### **427.1 PURPOSE AND SCOPE**

The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology (Minn. Stat. § 626.8472).

### **427.2 POLICY**

The policy of the Mankato Department of Public Safety is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

Operators shall take reasonable precautions to avoid inadvertently recording or transmitting images of areas where there is a reasonable expectation of privacy.

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

### **427.3 ADMINISTRATION**

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates. It is used by the Mankato Department of Public Safety to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. It may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction and stolen property recovery.

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Director of Public Safety or designee. The Director of Public Safety or designee will assign

members under his/her command to administer the day-to-day operation of the ALPR equipment and data.

#### **427.4 DEFINITIONS**

**Alert:** An indication (either visual and/or audible) from the ALPR that the plate read, matches a license plate listed in the Minnesota License Plate Data File or the Manual Hot List.

**Automated License Plate Reader (ALPR):** Per Minn. Stat. § 13.824, Automated License Plate Reader means 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.

**Be on the Lookout (BOLO):** A determination by a law enforcement agency that there is a legitimate and specific law enforcement reason related to an active criminal investigation to identify or locate a particular vehicle.

**Manual Hot List:** A compilation of license plates or partial license plates for which a BOLO situation exists and that information is programmed by a user into the ALPR system so that an officer will receive an alert if the ALPR reads a license plate that matches a license plate included on the list.

**Manual Hot Plate Entry:** A determination by a law enforcement agency that there is a legitimate and specific law enforcement reason related to an active criminal investigation to identify or locate a particular vehicle.

**Minnesota License Plate Data File:** A data file provided by the Minnesota Department of Public Safety, Bureau of Criminal Apprehension that contains FBI and Minnesota license plate-related Hot File data on stolen and felony vehicles, wanted persons, and attempts to locate. The FBI Hot File records represent all 50 states, the District of Columbia, certain United States Territories, and Canada. The file also contains license plate-related data on Minnesota Driver and Vehicle Services registered vehicles where an operator's license was withdrawn (suspended, canceled, disqualified or revoked.) This file contains no live data.

**Read:** The process by which the ALPR focuses on, photographs, and converts a picture of a license plate to digital text that comes within range of the ALPR that then may be compared against the Minnesota License Plate Data File or Manual Hot List.

**Real-Time Criminal Justice Information Services (CJIS):** A query of the CJIS system that includes the most up to date data available at the time of the query. CJIS includes any system to process, store, or transmit criminal justice information.

#### **427.5 OPERATIONS**

Use of an ALPR is restricted to the purposes outlined below. Department members shall not use, or allow others to use, the equipment or database records for any unauthorized purpose.

- (a) An ALPR shall only be used for official law enforcement business.
- (b) An ALPR may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not necessary before using an ALPR.
- (c) An ALPR must 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.
- (d) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas around homicides, shootings and other major incidents.
- (e) No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.
- (f) No ALPR operator may access confidential department, state or federal data unless authorized to do so.
- (g) Officers may only search previously collected ALPR data when reasonable suspicion exists that the data is relevant to an active criminal investigation. A factual basis for the search must be documented in the audit trail, the officer's report, or both.
- (h) If practicable, the officer should verify an ALPR response through the Minnesota Justice Information Services (MNJIS), National Law Enforcement Telecommunications System (NLETS), or other appropriate systems before taking enforcement action. Officers should also visually confirm that the plate number, state, and vehicle type reasonably match the alert.
- (i) Whenever ALPR data contributes to a stop, detention, citation, arrest, or investigative action, the use of ALPR should be documented in the corresponding IBR or investigative report.
- (j) When reviewing an ALPR alert, officers are expected to classify each hit as correct read, wrong state, incorrect read, or dismissed.

#### 427.5.1 RESTRICTIONS, NOTIFICATIONS AND AUDITS

The Mankato Department of Public Safety will observe the following guidelines regarding ALPR use (Minn. Stat. § 13.824):

- (a) Data collected by an ALPR will be limited to:

- (a) License plate numbers.
- (b) Date, time and location of data captured.
- (c) Pictures of license plates, vehicles and areas surrounding the vehicle captured.
- (b) ALPR data may only be matched with the Minnesota license plate data file, unless additional sources are needed for an active criminal investigation.
- (c) ALPRs shall not be used to monitor or track an individual unless done so under a search warrant or because of exigent circumstances.
- (d) The Bureau of Criminal Apprehension shall be notified within 10 days of any installation or use and of any fixed location of an ALPR.
- (e) Any person whose conduct constitutes the knowing unauthorized acquisition of not public data, as defined in Minn Stat § 13.055 sub 1 may be subject to criminal charges (Minn Stat § 13.09).

#### **427.6 DATA COLLECTION AND RETENTION**

The Director of Public Safety or designee-is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred from vehicles to the designated storage in accordance with department procedures.

ALPR data received from another agency shall be maintained securely and released in the same manner as ALPR data collected by this department (Minn. Stat. § 13.824).

ALPR data not related to an active criminal investigation must be destroyed no later than 60 days from the date of collection with the following exceptions (Minn. Stat. § 13.824):

- (a) Exculpatory evidence - Data must be retained until a criminal matter is resolved if a written request is made from a person who is the subject of a criminal investigation asserting that ALPR data may be used as exculpatory evidence.
- (b) Address Confidentiality Program - Data related to a participant of the Address Confidentiality Program must be destroyed upon the written request of the participant. ALPR data already collected at the time of the request shall be destroyed and future related ALPR data must be destroyed at the time of collection. Destruction can be deferred if it relates to an active criminal investigation.

All other ALPR data should be retained in accordance with the established records retention schedule.

When ALPR data is relevant to an active investigation or enforcement action, associated files (such as ALPR-generated images, PDFs, or alert records) shall be retained as part of the case file and uploaded to the corresponding IBR record when applicable.

When accessing ALPR software to perform a license plate search, users must enter the associated case number and may enter the type of incident and/or a brief description of the reason for the search. All information entered will be captured in the audit trail and is subject to review.

#### 427.6.1 LOG OF USE

A public log of ALPR use will be maintained that includes (Minn. Stat. § 13.824):

- (a) Specific times of day that the ALPR collected data.
- (b) The aggregate number of vehicles or license plates on which data are collected for each period of active use and a list of all state and federal public databases with which the data were compared.
- (c) For each period of active use, the number of vehicles or license plates related to:
  - 1. A vehicle or license plate that has been stolen.
  - 2. A warrant for the arrest of the owner of the vehicle.
  - 3. An owner with a suspended or revoked driver's license or similar category.
  - 4. Active investigative data.
- (d) For an ALPR at a stationary or fixed location, the location at which the ALPR actively collected data and is installed and used.

A publicly accessible list of the current and previous locations, including dates at those locations, of any fixed ALPR or other surveillance devices with ALPR capability shall be maintained. The list may be kept from the public if the data is security information as provided in Minn. Stat. § 13.37, Subd. 2.

#### 427.7 ACCOUNTABILITY

All saved data will be closely safeguarded and protected by both procedural and technological means. The Mankato Department of Public Safety will observe the following safeguards regarding access to and use of stored data (Minn. Stat. § 13.824; Minn. Stat. § 13.05):

- (a) All ALPR data downloaded to the mobile workstation and in storage shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.
- (b) Members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.
- (c) Biennial audits and reports shall be completed pursuant to Minn. Stat. § 13.824, Subd

6. In addition, the Mankato Department of Public Safety will conduct annual audits of ALPR user access, search logs, and system utilization for the first three years. Results of these audits will be reported to the City Council.

- (d) Breaches of personal data are addressed as set forth in the Protected Information Policy (Minn. Stat. § 13.055).
- (e) 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.
- (f) When supported by the ALPR system, a valid case number shall be entered to ensure accountability and auditability.
- (g) Any member who violates Minn. Stat. § 13.09 through the unauthorized acquisition or use of ALPR data will face discipline and possible criminal prosecution (Minn. Stat. § 626.8472).

#### **427.8 RELEASING ALPR DATA**

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures (Minn. Stat. § 13.824):

- (a) Law enforcement agencies requesting access to ALPR data must submit a completed ALPR Data Request Form to the Director of Public Safety or designee. The form must document a legitimate law enforcement purpose and include the following: :
  - (a) The name of the agency.
  - (b) The name of the person requesting.
  - (c) The intended purpose of obtaining the information.
  - (d) A record of the factual basis for the access and any associated case number, complaint or incident that is the basis for the access.
  - (e) A statement that the request is authorized by the head of the requesting law enforcement agency or his/her designee.
- (b) The review and approval process is as follows:
  - (a) If the request does not involve an exigent need, it will be reviewed and processed by the Records Supervisor or other records staff.
  - (b) If the request is made after hours and is determined to involve an exigent need, it must be reviewed and approved by Agency Command.
  - (c) An "Assist Other Agency" ICR shall be created in the records management system for all approved ALPR data releases. The completed ALPR Data Request Form must be

scanned and included with the IBR record, and a notation must be made in the software applications audit trail documenting that the request was made, reviewed, approved, and fulfilled.

- (d) Any release of ALPR data must be based on reasonable suspicion that the data is pertinent to an active criminal investigation.
- (e) All approved ALPR data requests and associated documentation shall be retained on file in accordance with the department's records retention schedule.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy.

#### **427.9 MANUAL HOT LIST CONTENT AND USE**

The ALPR is capable of alerting to license plates entered by the law enforcement agency in the ALPR system and not listed in the Minnesota License Plate Data File. Entries into the ALPR system shall comply with the following procedures and Minn. Stat. § 13.824:

- (a) A license plate number or partial license plate number shall only be entered in the Mankato Department of Public Safety Manual Hot List when there is a legitimate and specific law enforcement reason related to an active criminal investigation to identify or locate that particular vehicle or any person reasonably associated with that vehicle.
- (b) The Manual Hot List shall be reviewed as frequently as practical and entries shall be updated or removed as appropriate. Any entry must be removed as soon as the justification for its inclusion no longer exists.
- (c) If an officer receives an alert based on a Manual Hot List entry, they must follow 426.5(g) or utilize any other applicable databases to confirm that current legal justification exists to take action on the alert.
- (d) A Manual Hot List entry may not be used as a substitute for an entry into any other databases such as Minnesota or FBI Hot Files, Nation Crime Information Center (NCIC), or Keeping Our Police Safe (KOPS) files, if appropriate.