Automated License Plate Readers (ALPR)

447.1 PURPOSE AND SCOPE

This procedure shall be applicable to the squad(s) equipped with of Automated License Plate Reader (ALPR) technology and is intended to provide guidance on the use of the ALPR and the data collected by the system (Minn. Stat. § 626.8472).

447.1.2 POLICY

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

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

447.1.3 ADMINISTRATION

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates. It is used by the Grand Rapids Police Department 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 Captains. The Captains will assign members under their command to administer the day-to-day operation of the ALPR equipment and data.

447.2 OPERATIONS

Use of an ALPR is restricted to the purposes outlined below. Office 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) 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.

(d) No member of this office shall operate ALPR equipment or access ALPR data without first completing office-approved training.

(e) No ALPR operator may access confidential office, state or federal data unless authorized to do so.

(f) If practicable, the officer should verify an ALPR response through the Minnesota Justice Information Services (MNJIS) and National Law Enforcement Telecommunications System (NLETS) databases before taking enforcement action that is based solely upon an ALPR alert.

447.3 RESTRICTIONS, NOTIFICATIONS AND AUDITS

The Grand Rapids Police Department will observe the following guidelines regarding ALPR use (Minn. Stat. § 13.824):

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

1. License plate numbers.
2. Date, time and location of data captured.
3. 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.

447.4 DATA COLLECTION AND RETENTION

A. ALPR Data Collection and Retention

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 Grand Rapids Police Department Captains are 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 office procedures.

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):

1. 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.

2. 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 in AXON evidence.com.

447.5 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.

447.6 ACCOUNTABILITY

All saved data will be closely safeguarded and protected by both procedural and technological means. The Grand Rapids Police Department 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 office-related civil or administrative action.

(c) Biennial audits and reports shall be completed pursuant to Minn. Stat.§ 13.824, Subd.
6.

(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) 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).

447.7 RELEASING ALPR DATA AMONG LAW ENFORCEMENT AGENCIES

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, if they have a legitimate, specific and documented purpose, using the following procedures (Minn. Stat.§ 13.824):

(a) The agency makes a written request for the ALPR data that includes:

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

(b) The request is reviewed by a Captain or Shift Sergeant and approved before the request is fulfilled.

1. A release must be based on a reasonable suspicion that the data is pertinent to an active criminal investigation and documented.

(c) The approved request is retained on file.

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

447.8 NOTIFICATION TO BUREAU OF CRIMINAL APPREHENSION

Notify the Bureau of Criminal Apprehension of that installation or use and of any fixed location of a stationary automated license plate reader within ten days of the installation or current use of an automated license plate reader or the integration of automated license plate reader technology into another surveillance device.

447.9 BIENNIAL AUDIT REQUIRMENT

The Department is required to arrange for an independent, biennial audit of records to determine whether the data are properly classified, how the data is used, whether the data was destroyed pursuant to statutory guidelines, and to verify compliance with the required data access policies. A report summarizing the results of each audit must be provided to the commissioner of Administration and the Legislature within 30 days of the audit's completion.

445.6 ADMINISTERING ACCESS TO PORTABLE AUDIO/VIDEO RECORDING DATA

(a) Data subjects. Under Minnesota law, the following are considered data subjects for purposes of administering access to Portable Audio/Video Recorder data:

1. Any person or entity whose image or voice is documented in the data.
2. The officer who collected the data.
3. Any other officer whose voice or image is documented in the data, regardless of whether that officer is or can be identified by the recording.

(b) Portable Audio/Video Recorder data is presumptively private. Portable Audio/ Video Recorder recordings are classified as private data about the data subjects unless there is a specific law that provides differently. As a result:

1. Portable Audio/Video Recorder data pertaining to people is presumed private, as is Portable Audio/Video Recorder data pertaining to businesses or other entities.
2. Some Portable Audio/Video Recorder data is classified as confidential (see C. below).
3. Some Portable Audio/Video Recorder data is classified as public (see D. below).

(c) Confidential data. Portable Audio/Video Recorder data that is collected or created as part of an active criminal investigation is confidential. This classification takes precedence over the "private" classification listed above and the "public" classifications listed below.

(d) Public data. The following Portable Audio/Video Recorder data is public:

1. Data documenting the discharge of a firearm by a peace officer in the course of duty, other than for training or the killing of an animal that is sick, injured, or dangerous.
2. Data that documents the use of force by a peace officer that result in substantial bodily harm.
3. Data that a data subject requests to be made accessible to the public, subject to redaction. Data on any data subject (other than a peace officer) who has not consented to the public release must be redacted [if practicable]. In addition, any data on undercover officer must be redacted.
4. Data that documents the final disposition of a disciplinary action against a public employee.
5. However, if another provision of the Data Practices Act classifies data as private or otherwise not public, the data retains that other classification. For instance, data that reveals protected identities under Minn. Stat. § 13.82, sub. 17 (e.g., certain victims, witnesses, and others) should not be released even if it would otherwise fit into one of the public categories listed above.

Portable Audio/Video Recorders

(e) Access to Portable Audio/Video Recorder data by non-employees. Officers shall refer members of the media or public seeking access to Portable Audio/Video Recorder data to Grand Rapids Police Department Records Division, who shall process the request in accordance with the MGDPA and other governing laws. In particular:

1. An individual shall be allowed to review recorded Portable Audio/Video Recorder data about him- or herself and other data subjects in the recording, but access shall not be granted:

   (a) If the data was collected or created as part of an active investigation.

   (b) To portions of the data that the office would otherwise be prohibited by law from disclosing to the person seeking access, such as portions that would reveal identities protected by Minn. Stat. § 13.82, subd. 17.

2. Unless the data is part of an active investigation, an individual data subject shall be provided with a copy of the recording upon request, but subject to the following guidelines on redaction.

   (a) Data on other individuals in the recording who do not consent to the release must be redacted.

   (b) Data that would identify undercover officers must be redacted.

   (c) Data on other officers who are not undercover, and who are on duty and engaged in the performance of official duties, may not be redacted.

(f) Access by peace officer and law enforcement employees. No employee may have access to the department's Portable Audio/Video Recorder data except for legitimate law enforcement or data administration purposes:

1. Officers may view stored Portable Audio/Video Recorder video only when there is a business need for doing so. When preparing written reports, members should review their recordings as a resource (See the Officer Involved Shootings and Deaths Policy for guidance in those cases). However, members shall not retain personal copies of recordings. Members should not use the fact that a recording was made as a reason to write a less detailed report

   (a) Officers are prohibited from reviewing Portable Audio/Video Recorder footage following a police-citizen critical incident that results in great bodily harm or death to a citizen prior to giving a voluntary statement to the investigating authority.

   (b) Under rare circumstances, when a given fact-set calls for clarification of a critical incident, and with unanimous agreement of the Chief or his/ her designee, the investigating authority, and the prosecuting authority, an involved officer may be authorized to review video prior to or during an investigatory interview of an incident. In the event that pre-statement Portable Audio/Video Recorder footage viewing is authorized, the Chief or his/her designee shall make pre-statement review authorization and the reason for the authorization publicly available upon request.

2. Office personnel shall document their reasons for accessing stored Portable Audio/Video Recorder data in the Evidence.com cloud at the time of each access. Office personnel are prohibited from accessing Portable Audio/Video Recorder data for non-business reasons and from sharing the data for non-law enforcement related purposes, including but not limited to uploading data recorded or maintained by this agency to public and social media websites.

3. Employees seeking access to Portable Audio/Video Recorder data for nonbusiness reasons may make a request for it in the same manner as any member of the public.

(g) Other authorized disclosures of data. Officers may display portions of Portable Audio/ Video Recorder footage to witnesses as necessary for purposes of investigation as allowed by Minn. Stat. § 13.82, subd. 15, as may be amended from time to time. Officers should generally limit these displays in order to protect against the incidental disclosure of individuals whose identities are not public. Protecting against incidental disclosure could involve, for instance, showing only a portion of the video, showing only screen shots, muting the audio, or playing the audio but not displaying video. In addition,

1. Portable Audio/Video Recorder data may be shared with other law enforcement agencies only for legitimate law enforcement purposes that are documented in writing at the time of the disclosure.

2. Portable Audio/Video Recorder data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law.

445.6.1 SPECIAL CONSIDERATIONS OF DATA PRIOR TO RELEASE

Prior to release of data, a supervisor shall determine if a file is appropriate for release if it contains subjects who may have rights under the MGDPA limiting public disclosure of information about them. These individuals include:

(a) Victims and alleged victims of criminal sexual conduct.

(b) Victims of child abuse or neglect.

(c) Vulnerable adults who are victims of maltreatment.

(d) Undercover officers.

(e) Informants.

(f) When the video is clearly offensive to common sensitivities.

(g) Victims of and witnesses to crimes, if the victim or witness has requested not to be identified publicly.

(h) Individuals who called 911 and services subscribers whose lines were used to place a call to the 911 system.

(i) Mandated reporters.

(j) Juvenile witnesses, if the nature of the event or activity justifies protecting the identity of the witness.

(k) Juveniles who are or may be delinquent or engaged in criminal acts.

(l) Individuals who make complaints about violations with respect to the use of real property.

(m) Officers and employees who are the subject of a complaint related to the events captured on video.

(n) Other individuals whose identities the officer believes may be legally protected from public disclosure.

Prior to release of Portable Audio/Video Recorder data, the Records Division will consult with the officer/investigator to ensure that any of the above listed persons are potentially on any footage captured by the Portable Audio/Video Recorder.

445.7 DATA SECURITY SAFEGUARDS

(a) All safeguards in place by Evidence.com will meet or exceed required security parameters. In addition:

(b) Personally owned devices, including but not limited to computers and mobile devices, shall not be programed or used to access or view agency Portable Audio/Video Recorder data.

(c) Officers shall not intentionally edit, alter, or erase any Portable Audio/Video Recorder recording unless otherwise expressly authorized by the Chief or his/her designee.

(d) As required by Minn. Stat. § 13.825, subd. 9, as may be amended from time to time, this agency shall obtain an independent biennial audit of its Portable Audio/Video Recorder program.

445.8 OFFICE USE OF DATA

(a) Supervisors will randomly review Portable Audio/Video Recorder usage by each officer to ensure compliance with this policy

(b) In addition, supervisors and other assigned personnel may access Portable Audio/ Video Recorder data for the purposes of reviewing or investigating a specific incident that has given rise to a complaint or concern about officer misconduct or performance.

(c) Nothing in this policy limits or prohibits the use of Portable Audio/Video Recorder data as evidence of misconduct or as a basis for discipline.

(d) Officers should contact their supervisors to discuss retaining and using Portable Audio/Video Recorder footage for training purposes. Officer objections to preserving or using certain footage for training will be considered on a case-by-case basis. Field training officers may utilize Portable Audio/Video Recorder data with trainees for the purpose of providing coaching and feedback on the trainees' performance.

445.9 DATA RETENTION

(a) All Portable Audio/Video Recorder data shall be retained for a minimum period of 90 days. There are no exceptions non-evidentiary data.

(b) Data documenting the discharge of a firearm by an officer in the course of duty, other than for training or the killing of an animal that is sick, injured, or dangerous, must be maintained for a minimum period of one year.

(c) Certain kinds of BWC or portable audio/video records data must be retained for six years:

1. Data that documents the use of deadly force by an officer, or force of a sufficient type or degree to require a use of force report or supervisory review.

2. Data documenting circumstances that have given rise to a formal complaint against an officer.

(d) Other data having evidentiary value shall be retained for the period specified in the Records Retention Schedule. When a particular recording is subject to multiple retention periods, it shall be maintained for the longest applicable period.

(e) Subject to Part F (below), all other Portable Audio/Video Recorder footage that is classified as non-evidentiary, becomes classified as non-evidentiary, or is not maintained for training shall be destroyed after 90 days.

(f) Upon written request by a Portable Audio/Video Recorder data subject, the office shall retain a recording pertaining to that subject for an additional time period requested by the subject of up to 365 days. The agency will notify the requestor at the time of the request that the data will then be destroyed unless a new written request is received.

(g) Unintentionally recorded data will not be retained only after the following review.

(1) A sergeant is notified by the employee who collected the material.
(2) The sergeant will then approach a Police Captain and the Police Chief who will then review the request based on the material, referencing definitions provided in 445.1.1 and considering if the material poses any legitimate law enforcement value. Ultimately, the Police Chief will authorize not retaining the recorded data.

445.10 COMPLIANCE

Supervisors shall monitor for compliance with this policy. The unauthorized access to or disclosure of Portable Audio/Video Recorder data may constitute misconduct and subject individuals to disciplinary action and criminal penalties pursuant to Minn. Stat. § 13.09 and/or Minn. State Statute 262.8473.