PROCEDURE MANUAL
07-13

MICHIGAN STATE POLICE

License Plate Reader Systems

Purpose: This manual provides procedures that govern the use of automated License Plate Reader (LPR) technology by members.

Effective Date: June 20, 2023

Table of Contents

Definitions:

Access: For the purposes of this policy, access is the ability to receive notifications and perform inquiries in an LPR system.

Administrators: Administrators are those defined as having full access to all features of an LPR system.

Credentials: As used herein, the term credentials means login information that corresponds with a sole individual's access to an LPR system. This information is personal in nature and is held to the same requirements as found in directives regarding information security, the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy and the State of Michigan (SOM) Technical Standard, 1340.00.130.02 Acceptable Use of Information Technology.

Crime: As used herein, the term crime means an act or the commission of an act that is forbidden or the omission of a duty that is commanded by a public law and that makes the offender liable to punishment by that law. The term crime includes acts of terrorism.

Dispatchers: Dispatchers are those defined as having access to and the ability to receive notifications from an LPR system while working under the direction of a supervisor.

Historical LPR Data: Historical LPR Data consists of the dates, times, and locations of individually identifiable motor vehicles that is stored for future use and includes any LPR Data.

Historical LPR Data is not maintained by the Michigan State Police and will only be accessed through the organization maintaining the LPR system.

Jurisdiction: The geographical territory within which a law enforcement agency may exercise its power to enforce the law. This territory is defined as being within the state of Michigan.

Law Enforcement Information Network (LEIN)/National Crime Information Center (NCIC) Alert List: LEIN/NCIC Alert List means the list of license plates and certain other data extracted from the LEIN Alert Files and combined with the NCIC LPR Alert List.

LPR Alert Entry: An LPR Alert entry is entering a known license plate with a criminal predicate into an LPR system.

LPR Data: LPR Data is information, which is provided to a law enforcement official, including notifications that a license plate number contained in an LPR system has been detected in the vicinity of an LPR Unit.

LPR Data Notifications: Consists of license plate numbers and letters selected for inclusion on a particular list to facilitate the identification of vehicles displaying those license plate numbers. LPR Data notifications may be referred to as "alert lists" within this manual.

LPR Images: LPR Images consist of the optical appearance of the license plate and the surrounding area of the front and/or rear of a motor vehicle. LPR Images include information that is not rendered into an electronically readable format.

LPR System: LPR systems consists of the LPR Units, communications network components, data server hardware, software including any Optical Character Recognition (OCR) and algorithms, all operating in an organized and coordinated manner to collect license plate information and create notifications based on entered data.

LPR Units: LPR Units consist of the imaging hardware which captures the image of the license plates, regardless of the types of cameras used or the deployment of the unit.

Memorandum of Understanding (MOU): Refers to any agreement between the department and other law enforcement agencies.

Query: A query consists of the data provided by an LPR system in response to a transaction initiated by an authorized user.

Real-time: As used herein, the term "real-time" means a system in which input data is processed so that it is available virtually immediately.

Statistical Summary Data: Statistical Summary Data consists of a summary set of observations concerning LPR Data, which includes, but is not limited to:

(1) Measures from location(s), (e.g., average location, average number of license plate scans, average number of alert list hits).

(2) Raw counts of LPR Image captures. Statistical Summary Data shall not contain any license plate numbers.

Supervisors: Supervisors are those who have access to and the ability to receive notifications from an LPR system.

Users: Users are those defined as having access to an LPR system.

Section 1: License Plate Reader (LPR) Systems

1.1 Purpose for Collecting LPR Data

a. LPR Data may be collected:

i. To support crime analysis techniques.

ii. To alert law enforcement officials of the proximity of a vehicle displaying a license plate number that is included on an alert list.

iii. To locate vehicles displaying license plate numbers and letters that have a known relationship to an individual who is reasonably suspected of having committed a crime.

iv. To help law enforcement officials detect unreported and previously undetected crimes.

v. To help law enforcement assist in locating missing or endangered persons and/or juveniles.

1.2 Collection of LPR Data

a. LPR Units may be deployed within the department's jurisdiction in any one or all the following manners:

i. In a Fixed Deployment, by being mounted in a fixed location, whether overtly or covertly.

ii. In a Portable Deployment, by being semi-permanently placed, whether overtly or covertly.

iii. In a Mobile Deployment, by being mounted to a mobile vehicle, whether overtly or covertly.

iv. All LPR equipment requires bureau approval before acquiring and deploying such equipment.

b. Elements of LPR Data

i. Each piece of LPR Data collected by the department must include:

1. The LPR image.

2. The license plate number derived by the system's OCR software.

3. The Global Positioning System (GPS) coordinates or other location information of the observation.

4. The date and time of the observation; and

5. The deployment configuration of the LPR Unit that captured the LPR image.

ii. Each piece of LPR Data collected by the department may include other information that aids in the identification of vehicles including, but not limited to, the nonelectronically readable information contained in the LPR image (e.g., color, make, model, truck cap, etc.).

iii. LPR Data is not considered personal identifying information.

c. LPR data obtained for prosecution shall be maintained as evidence and documented as such within the original incident report.

1.3 Credentials and Dissemination of LPR Data

a. Department credentials to an LPR system shall follow the below listed guidelines.

i. Members shall not have access granted through any other department's LPR system at any time.

ii. LPR access for members is reserved only for the department's LPR subscription(s) and credentials or access may be granted in accordance with guidelines defined below.

iii. Once a member has transferred or ended employment, those granted access or credential rights shall be terminated.

1. Administrators are responsible for maintaining the list of users who have terminated following employment.

iv. Users shall not share any credential or access login information as this information is personal in nature and is held to the same requirements as found in directives regarding information security, the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy and the State of Michigan (SOM) Technical Standard, 1340.00.130.02 Acceptable Use of Information Technology.

b. Unless a request for an elevated designation has been submitted through the chain of command for approval by a bureau commander, or a bureau commander's designee, the access designations will be assigned to the corresponding departmental positions as follows:

i. Users: Members who are in a position where job functions necessitate access to an LPR system.

ii. Supervisors: MSP Operations Lieutenants.

iii. Administrators: Administrators will be selected by a bureau commander or their designee.

c. Anyone not employed by the department and not identified above, shall not be granted credentials to an LPR system. LPR Data can be shared upon written request to supervisors, as listed above, with confirmation of an ongoing criminal investigation. Federal agencies can access LPR data through their federal identified database.

i. Non-department members who are working under the direction of a department member may be granted user access to LPR systems.

1. These individuals shall review this directive prior to being granted access.

d. Users may access LPR Data for any official law enforcement investigative purpose.

i. Members shall provide an incident number as a reason for each inquiry of LPR systems.

1. Dispatchers inquiring for non-department entities shall provide that entity's incident number.

ii. Members shall document all LPR inquires on their eDaily or within the original incident report.

iii. LPR Data may be accessed in emergency circumstances when members are actively investigating life threatening felonies, or if there is imminent risk of loss of life.

e. Members with LPR system credentials may access LPR Data:

i. To conduct crime analysis.

ii. To identify and track the movement of vehicles displaying license plates reasonably related to a crime that has already been committed.

iii. To identify and track the movement of vehicles displaying license plate numbers contained in an alert list.

iv. To identify and track the movement of vehicles displaying license plates reasonably related to individuals when there is articulable suspicion linking the individual to having committed a crime.

v. To generate investigative leads for the investigation of a felony.

vi. To detect instances of criminal conduct not previously observed or reported to the department; and

vii. To otherwise investigate crimes and criminal conduct.

viii. Where the head law enforcement official or the elected prosecutor of a jurisdiction reasonably determines that an individual or vehicle poses a threat of substantial harm to the public, LPR Data may be released to the public, including, but not limited to, private security personnel.

1. A determination that the public safety exception above applies must be documented in writing and sent to an administrator to be retained in an electronic centralized storage location.

2. The release of LPR Data must be limited to information that could reasonably protect the public from the harm justifying the dissemination of the data.

ix. LPR Images may be used in a photo line-up to further a specific investigation for which the LPR Image was requested.

f. Dissemination of data, other than as set forth in this manual is prohibited.

g. Administrative rights may be granted through a formal request to the commander of the Field Services Bureau. Administrative rights shall be limited to persons identified within the Michigan Intelligence Operation Center, Field Operations Bureau, and/or the Information Technology Division, and should be limited to areas of work that are identified in the request.

1.4 Retention of LPR Data

a. Historical LPR data shall not be retained. All historical LPR data will be maintained by the LPR provider in which the department subscribes to obtain the LPR data.

b. The Memorandums of Understanding between the department and the provider shall request that LPR providers not retain data obtained from department hardware longer than 30 days.

c. In instances where LPR Data has the potential to be used in criminal investigations, members shall capture that information as manufactured/digital evidence to include:

1. License plate information

2. Date and location where LPR Data was captured

3. Related camera information

d. Members shall capture LPR Data using the features provided by the LPR System when accessible. In the event an LPR System does not provide a standard function for information download, members shall document the relevant information in the original incident report. Mechanisms for documentation include but are not limited to:

    1. Screen shots
    2. Metadata logs
    3. Dispatched information

1.5 Quality of LPR Data

a. The Information Technology Division (ITD) shall monitor the quality of the LPR Data it uses, analyzes, and disseminates regardless of its source.

    i. Members, using LPR Data, who identify an inconsistency between the LPR Image, and the license plate number derived from the LPR Image by the software shall take steps to correct the LPR Data.

    ii. Members using LPR Data shall visually confirm, either from the LPR Image or the license plate itself, that the license plate which caused an LPR system to generate an alert or notification matches the information contained in an alert list prior to taking any enforcement action other than following the vehicle.

b. ITD shall ensure the most recent or most trusted software is installed and used by an LPR system provider.

c. ITD shall conduct routine data quality audits to measure the accuracy of the output derived from LPR Images.

d. Individuals have no right to access or challenge LPR Data unless otherwise authorized by law.

1.6 LPR Data Notifications

a. Prior to detaining a vehicle or individual based upon an alert or notification that the vehicle's license plate number is on an alert list, the law enforcement official shall verify that the vehicle's license plate number, obtained from a visual inspection of the plate or the LPR Image, matches the information contained on an alert list.

b. Prior to detaining a vehicle or individual based upon an alert or notification that a vehicle’s license plate number is on the LEIN/NCIC alert list, the law enforcement official shall run the license plate number in LEIN and NCIC to ensure the vehicle/license plate is an active record.

    i. Alert list data connected to an investigation shall be retained as part of the investigation record consistent with Section 1.4.c.

c. Alert List Data used to detain an individual shall be retained as part of the investigation and in accordance with the department’s retention and disposal schedule.

    i. Members shall document this LPR Data in the original incident.

d. Members using alert lists who identify an inconsistency between the license plate number contained on an alert list and the records supporting that license plate number's inclusion on the Alert List shall take steps to correct an alert list.

1.7 Accountability for LPR Data

a. Supervisors, as defined in section 1.3(b) shall monitor the use of an LPR system, including but not limited to alert list changes, individual searches, LPR data access, and the dissemination of LPR Data.

b. Policy Awareness and Training

   i. Training shall be provided to individuals prior to accessing, maintaining, analyzing, or otherwise using the department's LPR Data on the following topics:

      1. The requirements contained in this procedure manual and the importance of complying with its terms.

      2. The types of errors LPR software can make when extracting electronically readable information from an LPR Image.

      3. LPR Data relates only to a vehicle's license plate information whereabouts and not necessarily the whereabouts of its registered owner; members shall follow the operational guidelines as set in this policy.

      4. A license plate number is not a proxy for an individual's name or other personally identifying information; and

      5. Any additional subjects the department considers significant to ensure LPR Data is appropriately accessed, analyzed, and disseminated.

   ii. Use of LPR systems shall be limited to members who have completed training in accordance with this section and provide documentation of successfully completing that training.

   iii. Administrators, as defined in section 1.3(b), shall maintain appropriate records confirming personnel that access or use LPR Data have completed training in accordance with this Section.

c. The LPR Coordinator shall monitor relevant legislative and regulatory activity impacting the administration of LPR systems or the collection, analysis, and dissemination of LPR Data and communicate changes needed to this written directive accordingly.

1.8 Security of LPR System and Data

a. The site security, system integrity, personnel security, and system security of an LPR system and data shall be maintained in accordance with directives regarding information security, the FBI CJIS Security Policy, the FBI CJIS Security Policy Michigan Addendum, and SOM Policy 1340.00 Information Technology Information Security.

Review Responsibility:	Field Operations Bureau; Field Support Bureau, Information Technology Division
Accreditation Standards:	CALEA 41.3.9