



<b>Automated License Plate Readers (ALPR)</b>	Related Policies:
<i>This policy is for internal use only and does not enlarge an employee’s civil liability in any way. The policy should not be construed as creating a higher duty of care, in an evidentiary sense, with respect to third party civil claims against employees. A violation of this policy, if proven, can only form the basis of a complaint by this department for non-judicial administrative action in accordance with the laws governing employee discipline.</i>	
Applicable Indiana Statutes:	
CALEA Standard:	
Date Implemented: September 2022	Review Date: September 2024

I. **Purpose:** The purpose of this policy is to provide guidance for the capture, storage, and use of digital data obtained using Automated License Plate Reader (ALPR) technology. The primary purpose of the Muncie Police Department Automated License Plate Readers (ALPR) system is to provide a tool for use by Patrol and Criminal Investigations personnel. This tool assists in the detection and apprehension of vehicles and/or persons traveling through the jurisdiction of the Muncie Police Department in a vehicle that has license plates that have been entered either into the National Crime Index Computer or on the MPD ALPR Hotlist. The ALPR system can also be utilized by MPD Detectives to assist in the development of leads that can eventually identify suspects who have committed crimes within the city.

LPR cameras can be mobile (mounted on vehicles) or fixed (mounted to a structure) as determined by the agency that owns the cameras.

II. **Policy:** The policy of this agency 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 agency. Because such data may contain confidential information, it is not open to public review.

The ALPR technology, allows for the automated detection of license plates along with the vehicle make, model, color and unique identifiers through the agency’s ALPR system. The technology is used to convert data associated with vehicle license plates and vehicle descriptions for official law enforcement purposes.

III. **Terms, defined. For purposes of the Automatic License Plate Reader Privacy Act:**

A. **Alert** means data held by the Bureau of Motor Vehicles, each criminal justice information system maintained in this state, the Federal Bureau of Investigation

National Crime Information Center, the Federal Bureau of Investigation Kidnappings and Missing Persons list, the Missing Persons Information Clearinghouse, and license plate numbers that have been manually entered into the automatic license plate reader system upon a law enforcement officer's determination that the vehicles or individuals associated with the license plate numbers are relevant and material to an ongoing criminal or missing persons investigation

- B. Automatic license plate reader system** means one or more mobile or fixed automated cameras used in combination with computer algorithms to convert images of license plates into computer-readable data
- C. Captured plate data** means global positioning system coordinates, date and time information, photographs, license plate numbers, and any other data captured by or derived from any automatic license plate reader system
- D. Governmental entity** means a department or agency of this state, the federal government, another state, or a political subdivision or an individual acting for or as an agent of any of such entities
- E. ALPR Operator:** Trained agency members who may utilize ALPR system/equipment. ALPR operators may be assigned to any position within the agency, and the ALPR Administrator may order the deployment of the ALPR systems for use in various efforts.
- F. ALPR Administrator:** The Chief of Police or his designee, serves as the ALPR Administrator for the agency.
- G. Hot List:** A list of license plates associated with vehicles of interest compiled from one or more data bases including, but not limited to, NCIC, Local BOLO's, etc.
- H. Vehicles of Interest:** Including, but not limited to vehicles which are reported as stolen; display stolen license plates or tags; vehicles linked to missing and/or wanted persons and vehicles flagged by the Indiana Bureau of Motor Vehicles Administration or law enforcement agencies.
- I. Detection:** Data obtained by an ALPR of an image (such as a license plate) within public view that was read by the device, including potential images (such as the plate and description of vehicle on which it was displayed), and information regarding the location of the ALPR system at the time of the ALPR's read.
- J. Hit:** Alert from the ALPR system that a scanned license plate number may be in the National Crime Information Center (NCIC) or other law enforcement database for a specific reason including, but not limited to, being related to a stolen car, wanted person, missing person, domestic violation protective order or terrorist-related activity.

#### **IV. Prohibited acts; exceptions.**

- A. An automatic license plate reader system may be used when such use is:
  - a. By a law enforcement agency of a governmental entity for the purpose of identifying:
    - 1. Outstanding parking violations;
    - 2. A vehicle registered to an individual for whom there is an outstanding warrant
    - 3. A vehicle associated with a missing person
    - 4. A vehicle that has been reported as stolen
    - 5. A vehicle that is relevant and material to an ongoing criminal investigation
  - b. By a parking enforcement entity for regulating the use of a parking facility
  - c. For the purpose of controlling access to a secured area

**V. Procedures:**

- A. Only properly trained sworn officers, and police dispatchers are allowed access to the ALPR system or to collect ALPR information. No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.
- B. To ensure proper operation and facilitate oversight of the ALPR system, all users will be required to have individual credentials for access and use of the systems and/or data, which can be fully audited.
- C. Department members shall not use or allow others to use the equipment or database records for any unauthorized purpose.
- D. ALPR Administrator shall monitor to ensure the security of the information and compliance with applicable privacy laws.
- E. An ALPR system database and capture information are to be used for official law enforcement purposes only. Personnel shall only access the database for investigative/administrative purposes only and treat all data as confidential.
- F. An ALPR may be used in conjunction with any routine patrol operation or criminal investigation; reasonable suspicion or probable cause is not required before using an ALPR.

- G.** Partial license plates and unique vehicle descriptions reported during major crimes can be entered into the ALPR system to identify suspect vehicles.
- H.** If practical, the officer should verify ALPR information before taking enforcement action that is based solely on an ALPR alert. Once an alert is received, the operator should confirm that the observed license plate from the system matches the license plate of the observed vehicle before any law enforcement action is taken because of an ALPR alert, the alert will be verified through an inquiry via MDT or through Dispatch. Officers will not take any police action that restricts the freedom of any individual based solely on an ALPR alert unless it has been validated. Because the ALPR alert may relate to a vehicle and may not relate to the person operating the vehicle, officers are reminded that they need to have reasonable suspicion and/or probable cause to make an enforcement stop of any vehicle. (For example, if a vehicle is entered into the system because of its association with a wanted individual, officers should attempt to visually match the driver to the description of the wanted subject prior to making the stop or should have another legal basis for making the stop.)
- I.** Hot lists shall be obtained or compiled from sources consistent with the purposes of the ALPR system set forth in this policy. Personnel will not enter any license plates into the MPD “Hotlist” unless the vehicle is currently wanted/suspected in criminal activity. Occasionally, there may be errors in the ALPR system’s read of a license plate. Therefore, an alert alone should not be a basis for police action (other than following the vehicle of interest). Prior to initiation of a stop of a vehicle or other intervention based on an alert, officers shall undertake the following:
- a.** An officer must receive confirmation, from Communications Center or other department computer device, that the license plate is still stolen, wanted, or otherwise of interest before proceeding (absent exigent circumstances).
  - b.** Officers shall visually verify that the license plate of interest matches identically with the image of the license plate number captured (read) by the ALPR, including both the alphanumeric characters of the license plate, state of issue, and vehicle descriptors before proceeding. Officers alerted to the fact that an observed motor vehicle's license plate is entered as a Hot Plate (hit) in a specific BOLO (be on the lookout) list are required to make a reasonable effort to confirm that a wanted person is in the vehicle and/or that a reasonable basis exists before an officer would have a lawful basis to stop the vehicle.
  - c.** Officers will clear all stops from hot list alerts by indicating the positive ALPR Hit, i.e., with an arrest or other enforcement action.
  - d.** General Hot Lists will be automatically downloaded into the ALPR system a minimum of once a day with the most current data overwriting the old data.
  - e.** All entries and updates of specific Hot Lists within the ALPR system will be documented by the requesting department member within the appropriate general offense report.



- J. All Hot Plates and suspect information entered the ALPR system will contain the following information at a minimum:
- a. Entering department member's name.
  - b. Related case number.
  - c. Short synopsis describing the nature of the originating call.

**K. Communications Personnel**

- a. The Communications Center shall be responsible for monitoring the ALPR system. All hits received will sound an alert in the Communications Center. Upon receiving an alert, on-duty dispatch personnel will immediately verify the captured plate (photo) with the wanted/suspect plate number displayed as the wanted plate from either NCIC, or the department Hotlist. Upon visual verification of the plate/tag the dispatcher will manually verify the wanted plate with NCIC to determine if it is still outstanding as wanted.
- b. Verified NCIC hits will result in an immediate dispatch of an officer, if possible
- c. Stolen License Plates – On all stolen license plate hits, dispatch personnel will check the stolen plate through BMV records. Should the stolen plate come back to a vehicle with the same make, model, and color of the vehicle that the stolen plate is currently being displayed on, the dispatched units shall be immediately advised of that fact.
- d. Hotlist Alerts may include specific instructions to field personnel. Those instructions will also be relayed to on - duty personnel at the time of dispatch.
- e. Communications personnel shall be responsible for notification of the NCIC information submitting jurisdiction of the recovery of wanted stolen vehicles and the status of any arrests. Notification shall be as per NCIC protocols.

**L. Officers**

- a. Patrol Officers shall be responsible for monitoring ALPR cameras on their assigned beat. Upon receipt of an ALPR notification, on duty personnel will respond to the area of the capture and look for the suspect vehicle. If the vehicle is located, proper traffic stop procedures should be followed based upon the type of hit, officer observations and other factors present.
- b. Officers may utilize ALPR data to assist in the identification of suspects involved in criminal activity.
- c. Officers may have search access enabling them to search the database for vehicles and/or persons of interest.

- d. When Investigative personnel utilize ALPR data to assist in identification of a suspect or vehicle linked to criminal activity, the ALPR data can be downloaded from the system and attached to the investigative report as evidence.

**M. ALPR Uses** - The ALPR system, and all data collected, is the property of the agency. Trained agency personnel may only access and use the ALPR system for official and legitimate law enforcement purposes consistent with this policy. The following uses of the ALPR system are specifically prohibited:

- a. **Invasion of Privacy:** Except when done pursuant to a court order such as a search warrant, it is a violation of this policy to utilize the ALPR to record license plates except those of vehicles that are exposed to public view (e.g., vehicles on a public road or street, or that are on private property but whose license plate(s) are visible from a public road, street, or a place to which members of the public have access, such as the parking lot of a shop or other business establishment).
- b. **Harassment or Intimidation:** It is a violation of this policy to use the ALPR system to harass and/or intimidate any individual or group.
- c. **Use Based on a Protected Characteristic:** It is a violation of this policy to use the ALPR system or associated scan files or hot lists solely because of a person's, or group's race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law.
- d. **Personal Use:** It is a violation of this policy to use the ALPR system or associated scan files or hot lists for any personal purpose.
- e. **First Amendment Rights:** It is a violation of this policy to use the ALPR system or associated scan files or hot lists for the purpose or known effect of infringing upon First Amendment rights.
- f. Anyone who engages in an impermissible use of the ALPR system or associated scan files, or hot lists may be subject to disciplinary action.

**Retention of captured plate data; limitation; updates; use; limitations.**

1. Any manual entry must document the reason for the entry; and
2. ALPR data will be purged after 30 days unless it has become, or it is reasonable to believe it will become, evidence in a criminal, administrative, civil or other lawful action.
3. Information gathered or collected, and records retained by the ALPR system will not be sold, accessed, or used for any purpose other than legitimate law enforcement or public safety purposes.

**N. Accountability and Safeguards** - All data will be closely safeguarded and protected by both procedural and technological means. The agency will observe the following safeguards regarding access to and use of stored data:

- a. All ALPR data downloaded to a mobile device, computer or MDT shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date, and time.
- b. Persons 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 relates to a specific criminal investigation or department-related civil or administrative action.
- c. ALPR data may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes. MPD may enter into data-sharing agreements with other law enforcement agencies as determined by the Chief of Police.
- d. Every ALPR Detection Browsing Inquiry must be documented by either the associated agency case number or incident number, and/or a reason for the inquiry.

**O. ALPR Data Detection Browsing Audits**

- a. The Department will audit a sampling of the ALPR system utilization from the prior 12-month period to verify proper use in accordance with this policy. The audit results shall be communicated to the Chief of Police or his/her designee.

**P. Data not considered public record;**

- a. Captured plate data held by a governmental entity is not considered a public record

**Q. PRIVATELY OWNED/FUNDED ALPR SYSTEMS**

Muncie residents may want to purchase privately owned ALPR systems and link them to the MPD network of systems. All private systems linked to the MPD system must be approved by the Chief of Police. All data received by the MPD shall become MPD data and subject to all provisions of this policy. The MPD must be provided search capabilities to any linked ALPR system. The MPD shall not be responsible for any costs associated with a privately funded ALPR system.

- a. Privately owned ALPR systems must meet all local government right of way ordinances, rules and regulations.
- b. The MPD will not actively monitor any privately-owned ALPR
- c. A private ALPR shall only be used for official law enforcement business