GRANITE CITY POLICE DEPARTMENT

**Title: AUTOMATED LICENSE PLATE READERS (ALPR) Procedure: 6.001**

**Date Issued: 04/28/20**

**Revised:**

**I. PURPOSE**

A. Automated License Plate Reader (ALPR) technology, also known as License Plate Recognition, provides automated detection of license plates. ALPRs are used by the Granite City 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. ALPRs may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction and stolen property recovery, and suspect interdiction.

**II. POLICY**

1. Use of an ALPR is restricted to the purposes outlined below. Department personnel shall not use, or allow others to use, the equipment or database records for any unauthorized purpose.
   * 1. No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.
     2. An ALPR shall only be used for official and legitimate law enforcement business.
     3. An ALPR may be used in conjunction with any patrol operation or official department investigation. Reasonable suspicion or probable cause is not required before using an ALPR.
     4. 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. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.
     5. The officer should verify through dispatch an ALPR response through the Illinois Law Enforcement Agencies Data System (LEADS) before taking enforcement action that is based solely upon an ALPR alert.
2. No ALPR operator may access LEADS unless otherwise authorized to do so

**III. PROCEDURES/GENERAL**

1. All installation and maintenance of ALPR equipment, as well as ALPR data retention and access shall be managed by the designated administrator. The designated administration will assign personnel under his/her command to administer the day-to-day operation of the ALPR equipment and data.
2. LPR will be installed in squad cars and department computers
   1. Dispatch is required to log in and monitor LPR at the beginning of every shift.
   2. Officers are required to log in and monitor in squad
3. When a hit is received
   1. Dispatch will monitor HITS
      1. If the HIT occurs on Eastbound McKinley and/or any Granite City LPR, Dispatch will do further inquiry.
      2. Dispatch will confirm that the picture of the plate matches what the program read it to be, and then confirm that it matches what the plate is on the actual entry, ensuring that all 3 match.
      3. If the HIT is a LEADS or REJIS Stolen vehicle hit, Dispatch will run the plate.
      4. Dispatch will provide 10-68 information to patrol units via radio, informing them if the vehicle is stolen or not.
   2. Officer will monitor HITS
      1. It is the Officer’s responsibility to verify HIT information prior to taking action.
         1. Officers will confirm that the picture of the plate matches what the program read it to be, and then confirm that it matches what the plate is on the actual entry, ensuring that all 3 match.
         2. Officers will identify reason for entry into other department’s hotlist.
      2. Prior to making a traffic stop, Officers will develop independent PC.
         1. Running a plate and receiving valid LEADS/NCIC hit can constitute PC
4. Entering a vehicle in Granite City Hotlist
   1. Only vehicles associated with a felony case are authorized for entry into the Granite City hotlist.
   2. Under special circumstances, OIC may use discretion to enter a vehicle to the hotlist for a misdemeanor offense, or AMBER/SILVER Alerts.
   3. If a vehicle is to be entered on the Granite City hotlist, there must be sufficient PC to seize and tow the vehicle if located.
   4. Officers will get supervisor approval prior to entry being made.
   5. Entry into hotlist will be made by a supervisor only.
   6. Vehicles entered into LEADS as stolen may be entered into the Granite Police hotlist.
   7. Vehicles entered shall have sufficient detail for reason of entry and will request dispatch contact upon being located (Contact GCPD Dispatch 877-6111).
5. Removing vehicle from hotlist
   1. Upon dispatch receiving a notification of a Granite City hotlist vehicle being located, dispatch notify the OIC.
   2. OIC will contact the Detective supervisor to advise of the vehicle being located, and to receive further instructions regarding the vehicle.
   3. OIC will remove the vehicle from the Granite City hotlist.
   4. In the case of a stolen vehicle being located, OIC should check the Granite City hotlist, and remove the vehicle if it had been entered.
   5. Supervisors will conduct a weekly audit of the hotlist
      1. Supervisors will investigate vehicles entered by their squad and verify the entry is still valid.
      2. Supervisors will remove any entries which are no longer needed.

**IV. ALPR DATA COLLECTION AND RETENTION**

1. All data and images gathered by an ALPR are for the official use of the Granite City Police Department and because such data may contain confidential LEADS information, it is not open to public review
   * + 1. ALPR information gathered and retained by this department may be used and shared with prosecutors or others only as permitted by law.

**V. ACCOUNTABILITY AND SAFEGUARDS**

All saved data will be closely safeguarded and protected by both procedural and technological means. The Granite City Police Department will observe the following safeguards regarding access to and use of stored data:

* + 1. All ALPR data downloaded to the mobile workstation and server shall be accessible only through a login/password protected system capable of documenting all access of information by name, date and time.
    2. 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 relate to a specific criminal investigation or department-related civil or administrative action.