POLICY/PURPOSE:
The purpose of this procedure is to implement practices for the proper use, maintenance, and deployment of the department’s License Plate Reader (LPR) and its software.

The availability and use of the LPR system provides opportunities for enhanced productivity, effectiveness, and officer safety.

All information in the LPR systems will be considered confidential and law-enforcement sensitive. Employees will be held accountable for and must be able to articulate the legitimate law enforcement purpose for the use and dissemination of received information.

DEFINITIONS:
Active LPR Data – Information provided to an Operator in real-time in the form of alerts that a license plate number contained in the hot list is near an LPR unit.

Administrator – Personnel responsible for setting up Users, installs, and maintaining the system.

Alert – A visual and/or auditory notice triggered when the LPR system receives a potential “hit” on a license plate.

Evidentiary Hit - A hit resulting in either law enforcement action (i.e. arrest or traffic stop) or documentation related to an active investigation. This LPR information may be downloaded and treated as evidence.

Hit – A read matched to a license plate that has previously been registered on the department’s “hot list” of vehicle plates or on the local “hot list” on the LPR’s computer that has been added by a User.

Historical LPR Data – A database containing the dates, times, and locations of individually identifiable motor vehicles.

Hot List – A database of license plate numbers of interest to law enforcement. This database may include the following:

- Stolen license plates or license plate numbers of stolen vehicles
- Vehicles associated with wanted subjects or registered sex offenders
- Vehicles associated with missing/endangered persons or AMBER alerts
- Vehicles associated with federal probationers
POLICY TITLE: License Plate Reader (LPR)  
STANDARD/REF #: 41.3.9

APPROVED BY: Wayne Jerman, Chief 
REVIEWED DATE: 1/17/2019

REQUIRED REVIEWERS: Special Operations Commander, CID Captain 
REVISED DATE: 1/17/2019

- Nationwide Domestic Violence Protection Orders
- NCIC violent gang and terrorist files
- Vehicles associated with suspended, revoked, or barred drivers
- Vehicles associated with active criminal investigations
- Vehicles with expired registration
- Any additional databases utilized must be approved by the Chief of Police and be consistent with this policy

Sources of information include but are not limited to the National Crime Information Center (NCIC), Amber Alerts, Department of Homeland Security Watch lists, Iowa Department of Transportation, or local information added manually by members of the department trained in the proper use of the LPR.

NOTE – Local warrants and no contact orders require manual submissions when not entered into NCIC.

LPR – License Plate Recognition/License Plate Reader.

Non-Encounter Alert – An alert indicating the officer not to stop the vehicle based on provided information alone. The officer should observe the vehicle and report pertinent information to the requesting member agency.

Operations Center Software – Software that serves as a repository of all data collected by the deployed LPR systems. This software acts as a data warehouse that can be queried for information pursuant to a law enforcement or public safety function.

Operator – Officers who will use the system in the field.

Read – The capture of digital images or license plates and vehicles with associated metadata (date, time, GPS coordinates with vehicle image capture).

User – Personnel who operate the information side of the system, query data or create/use hot lists.

AUTHORIZED USAGE: 
Use of the LPR system and/or Operations Center software is restricted to the law enforcement or public safety functions of the department. Information obtained from the LPR and/or Operations Center
software will not be used for personal reasons or for reasons inconsistent with the law enforcement/public safety functions of the department.

Misuse or abuse of any part of the LPR system will result in discipline up to and including termination in accordance with department directive, Disciplinary System.

Information obtained from any or all LPR system components will only be disseminated to other law enforcement agencies for legitimate law enforcement purposes consistent with this procedure upon the expressed permission of the Chief of Police or his designee. Information may also be disseminated to comply with a court-related request or subpoena.

**PROHIBITED USAGE:**
Prohibited uses of the LPR system, active LPR data, historical LPR data, and hot lists include, but are not limited to the following:

- To record plates on vehicles on private property that are not exposed to public view;
- To harass or intimidate any person/group;
- For personal use;
- Solely on the basis of a protected characteristic. Protected characteristics that are an impermissible basis for LPR use include:
  
  - A person’s race
  - Gender
  - Religion
  - Political affiliation
  - Nationality
  - Ethnicity
  - Sexual orientation
  - Disability
  - Any other classification protected by law

- For the purpose of or known effect of infringing on First Amendment Rights. For example, collecting information about an individual’s lawful associations, lawful political and religious affiliations or activities, etc., is improper.

**TRAINING REQUIREMENTS** [41.3.9c]
All Operators shall receive training prior to operating the LPR system. Only personnel that have successfully completed approved departmental training are allowed to operate the LPR equipment or
system. Operators will use the LPR equipment and system in accordance with their training and this directive.

PROCEDURE:
The Program Administrator will oversee general access to the LPR hot lists.

Prior to manually entering vehicle information to a hot list, Users will complete a LPR Submission Request (CRPD #782) and receive supervisor approval for the submission.

Administrators can manually add license plates to LPR hot lists by entering complete license plate information, the reason for the entry, any pertinent information (i.e. officer safety issues), and contact information. An inactive time of 90 days will be set unless further information is received to extend this timeframe.

Quarterly, members of CAU will audit the general access hot lists to ensure they are up to date.
- Manual entries remaining in the system in excess of 90 days will be deleted unless otherwise noted.

Guidelines: [41.3.9a]
Hot list data and collected hits are automatically refreshed within the system.

LPR “hits” alone do not constitute reasonable suspicion or probable cause for a stop. Officers receiving an alert will develop independent reasonable suspicion for the stop or immediately confirm the status of the vehicle by visually confirming the license plate matches the image and running the license plate manually via the MDC or request verification from CAU; unless compelling circumstances or officer safety issues make it unsafe to do so. In such cases, officers will confirm the status of the associated vehicle as soon as practical.

Vehicle occupants may not be the subject associated with the license plate. Officers must develop a reasonable belief the operator/occupant is the person of interest included in the hot list prior to initiating a traffic stop.

License plates may be entered manually for inclusion to a hot list for law enforcement purposes only (i.e. Attempt to Locates, stolen vehicles, etc.).

All enforcement action taken in response to a hit will be documented on an incident report, supplemental report, and will follow all reporting procedures outlined in department directives.
Downloading hit information from the general access hot lists will be requested through authorized Users. This information will be downloaded into document form and submitted with the officer’s report.

Officers will adhere to the department’s Department Motor Vehicle Operation and Pursuit directives when attempting to contact an LPR alert vehicle.

**Administrative Reporting:**
Monthly, the Program Administrator will submit a report of LPR usage to the Criminal Investigative Division (CID) and Patrol Commanders. The report will include:
- The number of manual submissions
- The number of hits
- The number of successful uses of the LPR
- Data purging information
- Data dissemination information
- Procedure compliance

The summary of the monthly LPR reports will be included in the department’s Annual Report.

**Data Storage & Retention:** [41.3.9b,d]
All LPR “Reads” data will remain on the server with Vigilant Solutions (current vendor) for a period of 180 days. All “Evidentiary Hits” are to be held in storage for a period of no less than five (5) years from the time of the event, after which time the data may be disposed of:
- If the hit is deemed of evidentiary, it will be printed and turned in as part of the case file.

**Maintenance:**
Under no conditions will an Operator modify the LPR equipment or software operating system without permission from an Administrator.

Damaged LPR equipment mounted to cars will follow procedures in Police Vehicle – Equipment and Inspection directive. Damage will be immediately reported to the Administrator, Watch Commander, and documented using the following:
- Vehicle Damage book located in the Command Center
- Police Vehicle Damage form (CRPD #729)
- Email to “Police Vehicle Defect”

The Administrator will be responsible for coordinating repairs with the appropriate vendor.
LPR camera lenses may be cleaned with non-alcohol/non-ammonia based glass cleaner or mild soap and water and a soft, nonabrasive cloth.

LPR camera lenses must not be scraped to clear snow or ice. Lenses must be gently warmed until clear to avoid damage.

Anytime the LPR unit is disconnected, un-mounted, or removed from the vehicle, it will be placed in the protective storage case and secured.