Number:	Subject:	Issue Date:	Effective Date:	Review Date:
10D.6	Automated License Plate Recognition Program	2/24/2020		

Per Order of:	TLEA References:	TCA References:
James A. Hambrick, Chief of Police	None	55-10-302

This Policy is for departmental use only and does not apply in any criminal or civil proceeding. This Policy should not be construed as creation of a higher legal standard of safety or care in an evidentiary sense with respect to third party claims. Violations of this General Order will only form the basis for departmental administrative sanctions. Violations of law will form the basis for civil and criminal sanctions in a recognized judicial setting.

1. **Purpose**

   The purpose of this policy is to establish a standard operating procedure for deployment, utilization, maintenance and training associated with the use of the Automated License Plate Recognition (ALPR) program, termed Guardian Shield.

2. **Definitions**

   a. Hardware: Automatic License Plate Recognition (ALPR) systems include a set of cameras that capture images of license plates. These cameras are typically affixed to the outside of the operational License Plate Recognition (LPR) vehicle or mounted to fixtures in other locations. This system also includes a separate computer processor which processes the camera images against the "Hot List".

   b. Hit: The notification that a scanned motor vehicle license plate matches one that has been entered into a "Hot List".

   c. Hot List: Data files that are provided through the Tennessee Bureau of Investigation / National Crime Information Center (TBI/NCIC) extracted from the law enforcement databases which contain a listing of stolen license plates, stolen vehicles, wanted persons, and other vehicles and/or persons actively being sought by a law enforcement agency. Hot Lists are also created by authorized personnel with enough evidence related to a criminal investigation.

   d. Automated License Plate Recognition (ALPR) System: A complete system by which advanced camera technology and software captures images of vehicle license plates and instantaneously compares them with a large file of records (Hot Lists) to identify vehicles of interest. The ALPR merely accomplishes, more efficiently, the same task a police officer may accomplish by reading a license plate and manually entering the number into a database for comparison.

   e. Guardian Shield Administrator: The Chief of Police's designee who administers the overall Guardian Shield program.

   f. OCR: Optical character recognition.

3. **Policy**

   a. Training

      i. Prior to the use of Guardian Shield equipment or computer portal, officers must complete department approved training.

ii. The Guardian Shield Administrator will ensure that any changes in hardware, software, applicable laws or training are relayed to the department.

b. Response to Guardian Shield Alerts

i. Officers shall investigate all LPR alerts to include, but not limited to stolen vehicles, wanted subjects, or other suspected criminals to determine the validity of the alert.

ii. The officer will visually verify that the scanned plate matches the alert information with regard to plate letters, numbers and issuing state.

iii. Once the state and all characters have been verified as accurate, the following information should be utilized by an officer in determining whether or not reasonable suspicion exists:

1. Expired Tags, Other Suspensions: Officers should verify the status of the tag on NCIC to establish reasonable suspicion.

2. Stolen Vehicles and Stolen License Plates: Officer should verify the status through NCIC, or other local government system or database.

3. Wanted Person: A wanted person alert may be utilized when obtaining reasonable suspicion, unless the officer has information the subject is not in the vehicle, when added to personally observed or known information.

4. BOLO Only: This alert is information only for officers. The narrative of the alert will assist officers in obtaining reasonable suspicion.

5. Officer Safety, Suspected Gang Member, Sexual Offender, Past Offender, Associate Only, and Information Only or Other Non-Specified Alerts: These alerts are "information only" for officers. Reasonable suspicion must be obtained in order to detain.

iv. Due to the increased potential for a vehicle pursuit involving a Guardian Shield alert, officers shall communicate with their supervisors. Officers shall use good judgement when planning contact and interception of the alert vehicle. They shall also use extreme caution and good judgement when staging and deploying pursuit termination devices as set out in the department's pursuit policy.

v. Alerts leading to pursuits or arrests shall be saved as a PDF and attached to the incident report.

c. Local Data Entry / Hot List Creation

i. In order to enter a tag into a Local Hotlist, an officer should have reasonable suspicion to believe the car is directly associated with the person sought (owner, regular driver, regular passenger, driver or passenger involved in previous criminal activity in said vehicle, etc.), based on officer information or recent criminal activity.

ii. When entering the tag into a hotlist, the entry into Guardian Shield should be noted in the active case or dispatch notes for the assigned case number.

iii. Once the officer has sufficient evidence based on the above, an entry into the Local Hotlist may be made through the management function of Guardian Shield. If a tag has been, or will be entered into NCIC, it may be entered into the Local Hotlist for a period of seven days only.

iv. Only complete tag numbers will be entered into the system.

v. Officers should set a reasonable expiration for tags entered into the Hotlist. Reasonableness is based upon articulable facts and the totality of the circumstances.

vi. Once the entering officer is made aware that the alert is no longer valid, he/she should immediately remove the tag from the system.

vii. Any officer, who is made aware of an alert that is no longer valid, should immediately notify the entering officer, and all potentially affected personnel.

d. Data Security and Access

i. Personnel who are granted access to Guardian Shield devices and/or databases will be issued a username and password specific to each individual by the System Administrator.

ii. All operators of Guardian Shield will be responsible for maintaining a secure login and password. This password will not be shared with anyone else.

iii. The database may be accessed for law enforcement purposes only.

iv. When conducting investigative queries into Guardian Shield, a requestor, case number (if applicable) and reason will be entered and associated with the search.

v. Personnel will not release any information obtained by the Guardian Shield to non-law enforcement personnel unless required by law.

vi. Sample audits will be conducted at least annually to ensure the removal of appropriate data is completed as required by TCA 55-10-302.

vii. All investigative queries into collected Guardian Shield data by personnel are logged and available for auditing and review by the Agency. Any perceived policy violation or other misuse of the system will result in further investigation and appropriate disciplinary action if warranted.

e. Data Storage, Retention, & Sharing

i. Data gathered is automatically uploaded to Guardian Shield vendor database.

ii. Release of data gathered by Guardian Shield is restricted in the same manner as CJIS information and unauthorized to non-law enforcement personnel.

iii. When sharing of captured plate data generated by Guardian Shield the agency with which data is shared must be listed on the city's website within fifteen (15) days after sharing data (Governmental entity as defined by Tennessee Code Annotated 55-10-302 (a) (3)).

iv. License Plate reads will only be stored for a maximum period of thirty (30) days, unless the data is retained or stored as part of an ongoing investigation, and in that case, the data shall be destroyed at the conclusion of either:

1. An investigation that does not result in any criminal charges being filed; or

2. Any criminal action undertaken in the matter involving the captured plate data.

v. The collected Guardian Shield data contains no Personally Identifiable Information that may be used to connect license plate detection to an individual. It is only with permissible purpose that an investigator may make this connection (using other systems).

TLEA Standards

None