| | BRUNSWICK COUNTY SHERIFF'S OFFICE<br>**GENERAL ORDER** | NO.<br>**E-07** | LAST REVISION DATE<br>**09/01/2026** | LAST REVIEW DATE<br>**09/01/2026** |
|---|---|---|---|---|
| SUBJECT<br>Automated License Plate Readers | | AMENDS | | |
| REFERENCE | | RESCINDS | | |
| PREPARED BY<br>BCSO Policy Review Committee | | APPROVED BY: SHERIFF BRIAN CHISM | | |

**Purpose**:

This directive establishes procedures and guidelines for the use and oversight of the agency's fixed and mobile Automated Licenses Plate Reader (ALPR) technology.

## I. Definitions:

**A. Automated License Plate Reader (ALPR) –** A device that uses cameras and computer technology to compare digital images of license plates to lists of known plates of interest. ALPR's may be deployed in different configurations including fixed and mobile cameras. Both configurations operate in the same manner for the same purpose.

1. Fixed ALPR locations use cameras that are engineered to focus on the rear license plate of vehicles passing by the camera location. The camera image is sent by cellular data signal to an off-site server where the image is compared with license plates entered into the National Crime Information Center (NCIC) and hot lists as defined below. Only license plates that match an NCIC entry of hot list entry will trigger an alert. The images of the license plates of the vehicles passing by the camera are retained for no longer than 30 days.
2. Mobile ALPR systems work in the same manner. The cameras may be mounted on a vehicle or on a mobile trailer. The ALPR users who are logged in to monitor that particular camera will receive an alert if a captured image matches an NCIC entry or hot list entry.

B. **Hot List** – a digital database of specific license plate numbers and vehicles of interest that ALPR cameras scan against in real time to generate alerts. Sources of Hot List entries include:

1. National databases including records from the National Crime Information Center (NCIC) for stolen vehicles, wanted suspects, or national AMBER Alerts.
2. Custom lists created by local law enforcement agencies for active local investigations, missing persons, or BOLOs (Be On the Lookout).

C. **Scan File Data** – Information obtained by an ALPR of license plates within public view that were read by the device, including images of the plate and vehicle on which it was displayed, and information regarding the location of the patrol vehicle or stationary camera position at the time the information was captured. Information stored includes a photo of the registration plate showing the rear of the vehicle, or an image of the vehicle if no plate is identified by fixed camera systems, a date and time stamp of when the registration plate was read by the ALPR and a GPS coordinate to identify the location the registration plate was read by the ALPR.

## II. Procedure:

### A. Overview

1. The ALPR works by comparing hot list data with the scan file. The device will alert the user of potential matches. The user must take steps to validate the alert itself. Deputy should be mindful that the ALPR may produce erroneous alerts due to damaged license plates, misidentification of a plate, or the variety of license plate types, etc.
2. Any traffic stops based on the alert from the ALPR must comply with all laws and procedures for a traffic stop.
3. Upon receiving an ALPR alert generated from an NCIC file, officers must confirm the status of the NCIC hit prior to taking any enforcement action.
4. If the ALPR alert is from a custom hot list, officers will follow the instructions in the reason code of the notification. If there are no instructions in the reason code, or if the NCIC hit cannot be verified, officer will need to develop reasonable suspicion independently of the ALPR alert prior to taking enforcement action.
5. There may be alerts that will not always require action, such as NCIC Nationwide Domestic Violence Protection Orders.

**B. Development of the Hot List**

1. Information will be submitted to ALPR servers in the following ways:

   a) Available NCIC extract downloads occur periodically and will transfer that hot list data to the ALPR servers.

   b) Authorized users of the ALPR may only enter additional vehicles of interest to the hot list for official and legitimate law enforcement purposes.

2. Hot lists will primarily be compiled from vehicles associated with NCIC entries for the following categories:

   a) Stolen Vehicles

   b) Gang or Suspected Terrorists

   c) Missing Persons

   d) Stolen License Plates

   e) Wanted Persons with Warrants Entered into NCIC

3. Hot lists may also include vehicles from any on-going investigation.

4. Hot lists **shall not** include license plates associated with only regulatory motor vehicle violations (i.e. expired registration, inspection violations, driver's license violations).

**C. Usage/Limitations/Security**

1. Only authorized personnel trained in the use of ALPR shall operate the system. All authorized personnel will complete the required training.

2. Scan file data will, on an ongoing basis, be automatically uploaded from the ALPR servers.

3. Department personnel are responsible for the security of the ALPR data and may only access, use, release and/or disseminate hotlist and scan file data for official and legitimate law enforcement purposes:

   a) As with other similar data, the department will ensure that the storage, use and transmission of scan file and hot list data is as secure as reasonably possible. Access to both shall be restricted only to sworn law enforcement personnel and designated non-sworn personnel.

   b) Hot list data will be considered confidential information. Security of the hot list data will be the responsibility of the officer using the ALPR or personnel accessing the data.

a) Scan file data will be considered confidential information. Access to agency's ALPR's scanned files will be secured and controlled by a login/password accessible system capable of documenting who accessed the information by identity, date and time. Authorized personnel may only access data stored in the ALPR servers based upon a reasonable belief that the scanned file data may be related or useful as part of a specific official action or investigation.

c) This section also applies to shared data obtained by ALPR systems not operated by this agency.

4. Authorized personnel may retain ALPR data beyond 30 days for criminal investigative reasons only. If the data needs to be maintained beyond 30 days, a copy of the information should be acquired and placed into the case management system and documented via the investigative report or a supplement report. The ALPR systems automatically purge all stored data after 30 days.

**D. Program Oversight/Evaluation/Audit Review**

1. All requests for shared data access from other law enforcement agencies and/or invitations to access data from private ALPR systems shall be forwarded to the Sheriff or his designee for approval.

2. Damage or other malfunctions to equipment shall be immediately reported to the personnel's supervisor.

3. To ensure manual entries are removed when no longer of interest the personnel who created the entry shall be responsible for removal of the entry.

4. The Sheriff, or his designee, shall conduct an audit of the ALPR systems at least once every 30 days to ensure compliance with all applicable policies and laws.

5. Anyone becoming aware of possible violations of this policy, including but not limited to the unauthorized access, use, release and/or dissemination of ALPR data, shall refer the matter to their supervisor.