



POLICY

It is the policy of the DCJIS to utilize the technology only in furtherance of official and legitimate law enforcement operations and public safety. Recognizing privacy implications, it is further the policy of DCJIS to ensure the protection of data. Thus, all users of the Central Repository are expected to abide by the guidelines set forth herein when using the Central Repository.

ACRONYMS AND DEFINITIONS

Agency ALPR Administrator: An employee of a Participating Agency designated by that agency to be responsible for the management of its authorized users and the user accounts at the Participating Agency.

Authorized User: An individual designated by a law enforcement agency and properly trained in the use and operational protocols of the ALPR. Only authorized employees who have an approved login and password will be allowed to access or use information in the Central Repository.

Contributing Agency: An agency that contributes ALPR data to the Central Repository.

Non-Contributing Agency: An agency that may access, but does not contribute data to, a data application or system maintained or operated within the DCJIS network or system.

Participating Agency: Either a contributing or non-contributing party that utilizes the Central Repository.

Source Agency: The agency that originally recorded and contributed data to a data application or system maintained or operated within the DCJIS network or system.

PROCEDURES

1. Standard of Use

Central Repository ALPR data shall be accessed and used only for official and legitimate law enforcement operations and public safety and may only be used based on specific and articulable facts of a concern for safety, wrongdoing, criminal investigations, Department-related civil investigations, or pursuant to a court order.

Searches of historical Central Repository ALPR data shall be done in accordance with this policy.



Only users who have been designated by their law enforcement department and properly trained in the use and operational protocols of the ALPR systems shall be permitted to use the Central Repository. DCJIS administrators shall ensure that any changes in hardware, software or law are communicated to all participants. Only authorized employees who have an approved login and password (Central Repository Authorized Users) will be allowed to access or use information in the Central Repository.

When a enforcement action, investigation, or prosecution results from the Repository ALPR data, the information contained in it will be preserved by the agency accessing the information.

Requests for searches of Central Repository ALPR data may be made by authorized members of the Contributing Party or Non-Contributing party subject to the provisions of this policy.

2. Login Application Process

- a) Each Contributing and Non-contributing Party shall designate an Agency ALPR administrator to be responsible for management of user accounts at that agency. All authorized users shall be limited to current employees who are legally authorized to review criminal justice information for crime prevention and detection purposes. Each potential user shall submit a request for a login and password to the Agency ALPR Administrator. The Agency ALPR Administrator shall have discretion to deny or revoke individual access.

3. Login Assignment

- a) Each Authorized User will be issued a user login and a default password by the Agency ALPR Administrator. Upon logging into the Repository for the first time, each Authorized User shall change the default password to another DCJIS-compliant password.
- b) Each Agency ALPR Administrator is responsible for the timely removal of any login accounts as Authorized Users leave their agency.
- c) An Authorized User shall not access the Central Repository by using a name and password that was assigned to another user. An Authorized User shall not give his or her password to another person, including another user, to access the system.

4. ALPR Central Repository Data Query Logs

- a) An automated log will be maintained for each transaction, which will include the name of the individual accessing the data, along with the date and time of access.



- b) Requests to review stored ALPR data and search results will be recorded and maintained in appropriate case files.
- c) ALPR Data Query Logs shall be maintained and secured.
- d) Audits of the ALPR systems and the central repository shall be conducted by the DCJIS.

5. ALPR Data Sharing and Dissemination

- a) Each Contributing Agency authorizes the release of its information as outlined in this Policy to any other criminal justice agency that may participate in the Central Repository in the future.
- b) A Contributing Party that does not want certain information from its ALPR system to be shared is responsible for filtering out such information before entering it into the Central Repository.
- c) The information contributed to the Central Repository is limited to ALPR data.
- d) Central Repository ALPR data can be accessed, retrieved, or shared for official and legitimate law enforcement operations or public safety purposes only.

6. Ownership of Data

- a) Each Contributing Party will retain sole responsibility, ownership, management control, and disposition over the information it contributes or allows access to. All system entries will be identifiable to the Contributing Party, and the content of the contributed information remains the sole responsibility of the Contributing Party and is under that Contributing Party's management control.
- b) It shall be the responsibility of the party requesting or using the data to confirm the accuracy of the information with the Source Agency before taking any enforcement-related action.

7. Retention of Data

- a) Data from field ALPRs will be transferred/uploaded to the Department's server at a time to be determined by the Agency ALPR Administrator.
- b) ALPR data shall be stored in the Central Repository for a period of one year except in the following circumstances:



- i) Alert data associated with an enforcement action, investigation, or prosecution shall be maintained for one year or until a final disposition has been reached in the particular case, whichever is longer.
- ii) Alert data associated with an arrest will be maintained in the criminal case file and retained for the maximum period of time associated with such record.
- iii) Alert data associated with criminal investigations will be maintained in the criminal case file and retained for the maximum period associated with such record.
- iv) If it is reasonable to believe and the ALPR data will become evidence in a criminal or civil action, the record will be maintained until it is no longer reasonable to believe it will become evidence in a criminal or civil action.
- v) Whenever otherwise directed by the ALPR Administrator.

CONFIDENTIALITY OF INFORMATION

Information in the Central Repository is confidential and is not subject to public disclosure, except as required by law. Only Authorized Users are allowed to view and use the information, otherwise, the information shall be kept confidential.

ACKNOWLEDGEMENT OF TERMS AND CONDITIONS OF USE

The Agency ALPR Administrator shall provide a copy of the terms and conditions of the Massachusetts Public Safety Information Sharing Global Policy and this ALPR Central Repository Companion System Policy to all Authorized Users when they are issued a login ID for the system. Each Authorized User shall sign an acknowledgement stating, "I have received a copy of the terms and conditions of usage of the Central Repository. I agree to comply with the terms and conditions and I understand that any violation of the terms and conditions may lead to disciplinary action and/or criminal prosecution." The Agency ALPR Administrator shall maintain the signed acknowledgements at all times.

POLICY REVIEW

The Commissioner of the Department of Criminal Justice Information Services is responsible for the annual review of this policy.