



LAW ENFORCEMENT BULLETIN



AUTOMATED LICENSE PLATE READERS – NEW SAMPLE POLICY SUPPORTS RESPONSIBLE USE AND COMPLIANCE

Automated License Plate Reader (ALPR) technology remains an important crime-fighting tool for law enforcement agencies. When properly governed, ALPR systems can assist with identifying stolen vehicles, locating wanted people, supporting active investigations, recovering missing persons, and enhancing public safety. However, because ALPR systems collect and retain vehicle location data, their use must be carefully managed through policy, training, supervision, documentation, and auditing.

For New Jersey law enforcement agencies, maintaining a comprehensive ALPR policy is essential to meeting the requirements of New Jersey Attorney General Law Enforcement Directive No. 2022-12, which updated statewide rules governing ALPR technology. In light of recent scrutiny involving improper access to, or misuse of, license plate reader systems, chiefs of police must also ensure their policies provide enhanced operational guidance, clearly define oversight responsibilities, require frequent audits, and reinforce safeguards designed to prevent misuse, protect privacy, maintain system integrity, and safeguard constitutional rights by limiting access to ALPR data to legitimate law enforcement purposes that are properly documented and subject to meaningful review.

An Automated License Plate Reader Sample Policy is now available in the [Law Enforcement Accreditation Plus Sample Policy Portal](#). The policy does not restrict lawful ALPR use; instead, it provides a strong framework to preserve system integrity, support responsible crime-fighting and public safety efforts, and protect agencies, officers, the community, and the public through provisions that include:

- Providing key definitions to ensure consistent understanding and application of ALPR-related terms.
- Requiring documentation of the specific reasons ALPR systems are deployed, especially when units are temporarily placed at particular locations.
- Mandating prompt reporting of system errors or malfunctions that may affect accuracy, reliability, or investigative use.
- Defining prohibited uses to prevent improper access, misuse, or inquiries unrelated to a legitimate law enforcement purpose.
- Requiring documentation for access to, or inquiries of, BOLO lists, BOLO queries, and crime scene queries.
- Establishing required training for authorized users before they access ALPR systems or data.
- Enhancing system and user audits to confirm authorized access, validate the purpose of inquiries, detect potential misuse, and support accountability.

Chiefs of police are encouraged to review their current ALPR policy, compare it against the updated sample policy, and ensure that supervisors and authorized users understand their responsibilities. A current, well-implemented ALPR policy is not merely an administrative requirement; it is a critical risk-management tool that protects the agency, supports officer accountability, addresses public concerns, and helps preserve the lawful use of ALPR technology.

If you have any questions, please contact your Law Enforcement Risk Control Consultant, or if you need assistance in accessing the Law Enforcement Accreditation Plus Portal, contact the J.A. Montgomery Law Enforcement Team at lawenforcementteam@jamontgomery.com