

AUTOMATED LICENSE PLATE READERS (ALPR)

434.1 PURPOSE AND SCOPE

The purpose of this policy is to establish clear guidelines for the lawful, ethical, and transparent use of the Automated License Plate Reader (ALPR) technology by the Warden Police Department. ALPR systems enhance public safety, support criminal investigations, locate wanted persons and vehicles, and improve officer situational awareness. All use of ALPR technology shall comply with ESSB 6002, Washington State privacy laws, and applicable department policies.

This policy applies to all personnel who operate, access, manage, or supervise ALPR equipment or data.

434.2 ADMINISTRATION OF ALPR SYSTEMS AND DATA

The ALPR program shall be overseen by the ALPR Program Administrator, appointed by the Chief of Police. The administrator is responsible for:

- Installation, maintenance and repair of ALPR equipment
- Insuring proper data retention, transfer, access control, and storage
- Assigning trained personnel to manage day-to-day ALPR operations
- Conducting audits and insuring compliance with state law and department policy

Supervisors shall insure that ALPR-equipped vehicles and systems are functioning properly and that all use complies with this policy.

434.3 AUTHORIZED USES

ALPR technology shall be used only for official and legitimate law enforcement purposes, including:

- Locating stolen, wanted, or missing vehicles and license plates
- Identifying felony, gross-misdemeanor, or other active criminal cases
- Enhancing officer safety
- canvassing major crime scenes when appropriate
- Identifying vehicles associated with felony and gross-misdemeanor warrants

ALPR systems may be used in conjunction with patrol operations, lawful investigations, and major-incident response. Reasonable suspicion or probable cause is not required to initiate ALPR scanning.

434.4 PROHIBITED USES

ALPR systems shall not be used for:

AUTOMATED LICENSE PLATE READERS (ALPR)

- General surveillance without a law enforcement purpose
- Immigration enforcement
- Personal or non-law enforcement activities
- Any use not explicitly authorized by this policy

434.5 DATA COLLECTION AND VERIFICATION

ALPR systems automatically capture images and metadata. Personnel shall not alter or intentionally modify ALPR data.

Officers must verify any ALPR alert ("hit" through the Centralized Computerized Enforcement Services System (ACCESS) or other reliable investigative methods before taking enforcement action, unless independent factors justify immediate action.

No ALPR operator may retrieve ACCESS data unless properly authorized.

434.6 DATA RETENTION, STORAGE, AND TRANSFERS

Consistent with ESSB 6002:

- Passive ALPR data not tied to a criminal investigation shall be retained no longer than 90 days
- Data linked to an active investigation, legal requirement, lawful hold, or court order may be retained longer as permitted by law
- ALPR data stored in vehicles shall be transferred to secure department servers on a regular basis, not to exceed 30 days between transfers
- All ALPR data shall be stored securely, protected from unauthorized access, and preserved according to legal requirements

434.7 ACCESS, RELEASE, AND INFORMATION SHARING

Access to ALPR data is restricted to authorized personnel for legitimate law-enforcement purposes. Any access shall be logged, including user, date, and time.

ALPR data may only be released:

- As required by law
- in response to a valid public records request (subject to exemptions)

AUTOMATED LICENSE PLATE READERS (ALPR)

- To verified law enforcement agencies for criminal justice purposes

Partner agencies receiving ALPR data must comply with ESSB 6002-aligned retention, usage, and privacy protections. All sharing agreements shall be documented and reviewed annually.

434.8 TRAINING REQUIREMENTS

All personnel who operate ALPR systems or access ALPR data must complete department-approved training addressing:

- Proper operation of the ALPR technology
- Legal requirements under ESSB 6002
- Data handling, retention, and privacy protections
- Verification standards for ALPR alerts
- Prohibited uses of ALPR systems

Refresher training will be provided annually

434.9 AUDITING, ACCOUNTABILITY, AND MISUSE

The ALPR Program Administrator shall conduct regular audits, including:

- Verification that ALPR access is authorized
- Compliance with retention and privacy rules
- Review of ALPR alerts and resulting enforcement actions
- Insuring data releases are lawful and properly documented

Willful misuse of unauthorized access to ALPR data may result in disciplinary action and may constitute a gross misdemeanor under state law.

434.10 MAINTENANCE

ALPR equipment shall be maintained in accordance with manufacturer specifications. Any system malfunction, security concern, or suspected data compromise must be reported immediately.

434.11 TRANSPARENCY

The department will publicly provide information describing:

- The purpose and authorized uses of ALPR systems
- Data retention periods
- Audit and Accountability measures
- General privacy protections applied to ALPR data

Warden Police Department

Warden PD Policy Manual

AUTOMATED LICENSE PLATE READERS (ALPR)
