

OCEAN RANCH AT BEAR BRAND HOMEOWNERS ASSOCIATION

AUTOMATED LICENSE PLATE READER (ALPR) POLICY

1. PURPOSE AND SCOPE

This Policy concerns the Ocean Ranch at Bear Brand Association (“Association”) installing and using an Automated License Plate Reader (ALPR) at the Association’s entry and exit vehicle access gates, which will record high-resolution digital images vehicles and the vehicle license plate information for vehicles entering and exiting community. The ALPR system may also collect vehicle make, color, timestamps, geolocation data. The ALPR system does not capture images of the vehicle interior or occupants of the vehicle. The Association’s purposes for the ALPR system generally include, without limitation, controlling access into the community, deterring unauthorized access into the community, enhancing community security, enforcing the Association’s governing documents, and, in instances where criminal activity, property damage, or similar incidents involving a vehicle occur in the community (collectively, “Incident” or “Incidents”), for purposes of using recorded information to assist the Association and/or police investigating and identifying the perpetrator(s) or person(s) responsible for the Incident for further enforcement action.

Therefore, this Policy establishes the operational guidelines, privacy protections, security measures, and data retention protocols for the ALPR system. The ALPR system shall not be used for the monitoring or tracking of individual resident travel patterns, commercial marketing, or arbitrary personal surveillance.

2. RESPONSIBILITY FOR IMPLEMENTING THIS POLICY’S REQUIREMENTS AND SAFEGUARDS

The Association’s Board of Directors (“Board”) and the Association’s managing agent shall be responsible for implementing the Policy and ensuring compliance with this Policy.

3. AUTHORIZED USERS AND ALPR SYSTEM ACCESS

Access to the ALPR system, including live monitoring, data queries, and historical logs, is strictly restricted to personnel who have a legitimate, authorized business need. Authorized individuals include (“Authorized Personnel”):

- Designated Association Board Members (only when investigating a specific incident).
- The Association's Community Manager or designated management staff (only when investigating a specific incident).
- The Association's contracted third-party vendor or monitoring service managing the ALPR system.
- Authorized technicians from the ALPR vendor (solely for maintenance and technical support).

The Association’s third-party vendor responsible for operating and monitoring the ALPR system shall be responsible for periodic equipment and system checks to ensure the accuracy of the ALPR information, and shall be responsible for correcting any identified data errors.

Prohibited Uses: Accessing any ALPR data for personal reasons, harassment, commercial solicitation, or any other purpose not consistent with the stated purposes in this Policy is prohibited

4. MANDATORY SECURITY AND PRIVACY TRAINING

Prior to gaining access to any ALPR data or software, all Authorized Personnel must complete mandatory training for the purpose of ensuring adherence to California privacy laws, including requiring such Authorized Personnel being informed of the details in this Policy and informed on the following topics:

- Legal requirements under California Civil Code § 1798.90.5 et seq. concerning use of an ALPR system, privacy protections, security measures, and data retention protocols, etc.
- The exact, restricted purpose of the Association's ALPR system, as described above.
- Proper data query procedures, including the requirement to document search justifications, consistent with this Policy.
- Information security protocols, including password protection and data confidentiality.

5. DATA SECURITY, ENCRYPTION, AND SAFEGUARDS

The Association implements the following technical, administrative, and physical safeguards to prevent unauthorized access, modification, destruction, or disclosure of ALPR data:

- **Technical Safeguards:** All ALPR data transmitted over networks or stored in cloud databases must be secured with modern encryption protocols (AES-256 or equivalent). Access requires secure, multi-factor authentication (MFA).
- **Physical Safeguards:** Any physical servers, cameras, and network infrastructure located on-site must be physically locked and monitored via security cameras.
- **Administrative Safeguards:** System credentials shall not be shared among users. Accounts will be immediately deactivated upon an authorized user's separation from, or change in role, with the Association, the Association's management company, or any Association's contracted third-party vendor or monitoring service managing or maintaining the ALPR system.

6. DATA RETENTION AND AUTOMATIC DELETION

In accordance with local and state recommendations for non-law-enforcement entities, the Association enforces a strict data retention threshold to minimize privacy risks:

- **1 Year Purge Rule:** All captured license plate images, optical character recognition (OCR) text data, timestamps, and location coordinates shall be automatically and permanently deleted within **one (1) year** of capture.
- **Exceptions for Incidents:** Data directly relevant to an ongoing criminal investigation, reported property damage, or verified security or similar incident may be extracted and preserved beyond one (1) year. Such data shall be purged promptly after the investigation, legal proceeding, or need for the information concludes.

7. DATA SHARING AND EXTERNAL DISCLOSURE

The ALPR information may be used for only the authorized purposes described in this Policy. ALPR data is proprietary and private to the Association and will not be sold, leased, or shared with third parties for commercial marketing purposes. Sharing with external entities is strictly limited to the following:

- **Law Enforcement Cooperation:** The Association may share specific data plates or access windows with law enforcement agencies upon receipt of a valid subpoena, warrant, court order, or as may otherwise be authorized by the Board for good cause. In emergency situations involving an imminent threat of death, serious physical injury or property damage, data may be provided as reasonably necessary in compliance with applicable law.
- **Prohibited Sharing:** The Association does not link its ALPR database to broader law enforcement 'hot lists' or cross-jurisdictional networks without explicit, documented approval from the Board.

8. AUDITABILITY AND LOGGING

The ALPR system shall maintain an automated, unalterable system audit log of all system activity. Each log entry shall record the following:

- The specific username of the individual accessing the system and , as applicable, the organization or entity with whom the person is affiliated.
- The date and time information is accessed, searched, or retrieved.
- The license plate or search criteria used to execute the query.
- The purpose of accessing the information, such as the documented security incident or business justification for the search.

These audit logs shall be reviewed periodically by the Association's Board and managing agent to ensure compliance with this Policy.

9. PUBLIC NOTICE

This Policy shall be distributed to all Association members upon adoption, and shall be posted in a visible, conspicuous location on the community website or member portal. Conspicuous signage indicating that the community is monitored by license plate reader technology shall be posted at all community vehicular entrances and exits.