

INLAND EMPIRE HEALTH PLAN		
Department: Facilities, Safety & Security		
Subject: Automated License Plate Recognition (ALPR) Usage and Privacy Policy	Policy #:	FAC_SS_001
Written by: Kameron Persaud, Safety & Security Manager	Original Effective Date:	July 1, 2026
Approved by: IEHP Legal Counsel	Revision Date:	N/A

APPLIES TO:

- A. This policy applies to any vehicle entering IEHP property. This includes employees, contractors, vendors, visitors, and members of the public whose vehicle license plates are captured by the Automated License Plate Recognition (ALPR) system. This policy also applies to IEHP Safety & Security personnel authorized to access ALPR data.

POLICY:

- A. IEHP utilizes ALPR technology to support campus safety, security, and potential future parking management needs. IEHP is committed to ensuring that all ALPR data is collected, accessed, stored, used, and disposed of in compliance with applicable laws, including California Civil Code §§ 1798.90.51 and 1798.90.55. IEHP protects the privacy of individuals whose vehicle information is captured by the ALPR system and limits access to ALPR data to trained, Authorized Personnel only.
- B. ALPR data will be used solely for safety, security, and incident-related operational purposes. It will not be used for employee performance evaluation, attendance tracking, productivity monitoring, or any purpose unrelated to campus safety or incident investigation.
- C. IEHP does not provide proactive or automated access to ALPR data to external parties. ALPR data may be disclosed only when necessary to report or investigate criminal activity or when legally compelled.

PURPOSE:

- A. The purpose of this policy is to establish clear guidelines for the use, access, security, retention, and disposal of ALPR data collected on IEHP property. The policy ensures protection of individual privacy while enabling IEHP to use ALPR technology to deter and detect security risks, enhance campus safety, and support future operational needs.

DEFINITIONS:

- A. Automated License Plate Recognition (ALPR): A system that uses cameras and software to capture and convert images of vehicle license plates into computer-readable data.

- B. ALPR Data: Information collected or generated by the ALPR system, including license plate images, converted text, timestamps, and associated metadata.
- C. Authorized Personnel: IEHP Safety & Security team members who have been granted permission to access ALPR data after completing required training.
- D. Access Log: A record that tracks which Authorized Personnel access ALPR data, when access occurs, and the purpose for accessing it.
- E. Security Control: Measures implemented to protect ALPR data against unauthorized access, disclosure, alteration, or destruction.

PROCEDURES:

A. Purpose of the ALPR System

IEHP uses ALPR cameras positioned at parking lot entrances to enhance campus safety and security. The system is used to deter and detect criminal activity, support incident investigations, ensure the safety of team members and visitors, and may support future parking management operations.

B. Authorized Access and Oversight

Access to ALPR data is restricted to Authorized Personnel, as defined in this policy. Authorized Personnel must complete mandatory training prior to receiving access. Access is approved by IEHP Safety & Security leadership only and any access approval must be justified by a business need as contemplated by this policy. Oversight responsibilities of the Safety & Security Manager include monitoring system usage, conducting routine audits of access logs, and ensuring compliance with all applicable laws and policies.

1. Training will cover this policy, applicable legal requirements, privacy protections, proper system usage, and data security responsibilities.
2. Retraining will be required if this policy materially changes, if the individual's role changes, or if audit findings indicate corrective action is necessary.

C. Monitoring and Auditing

IEHP will conduct regular audits of the ALPR system, including periodic reviews of access logs, assessments of data usage, and checks for compliance with policy and legal requirements. All findings will be documented, and corrective actions will be implemented if misuse or non-compliance is identified.

1. Any instance in which ALPR data or images are shared with law enforcement must be documented in the access logs. The documentation shall include the date and time of the disclosure, the Authorized Personnel involved, the law enforcement agency, the purpose of the request or incident involved, and a description of the information provided. This record will supplement the access log and will be subject to audit.

D. Data Sharing and Access Controls

IEHP does not provide proactive or automated access to ALPR data to law enforcement agencies. IEHP may, however, share ALPR data or images with law enforcement when such sharing is connected to reporting or investigating criminal activity. Examples include motor vehicle accidents, suspected theft, vandalism, threats to safety, or other incidents where law enforcement requests evidence as part of an active or potential investigation. All such sharing must be limited to the minimum necessary information and must relate directly to a specific incident or investigation. IEHP will not perform license plate searches at the request of law enforcement unless related to a specific incident or legal process. Any other release of ALPR data requires a valid warrant, subpoena, or court order and must be reviewed by IEHP's Legal department.

E. Data Accuracy

IEHP will implement reasonable measures to ensure the accuracy of ALPR data, including regular system maintenance, verification of system performance, and training of Authorized Personnel on proper data handling. System errors, misreads, or inaccuracies will be addressed and corrected when identified.

F. Security Procedures

ALPR data will be protected through security controls, including encryption, restricted access, secure storage, and regular system security assessments. IEHP will maintain reasonable safeguards to prevent unauthorized access, use, or disclosure of ALPR data. IEHP's ALPR vendor may access the ALPR system solely for maintenance or troubleshooting purposes. Such access is limited to what is necessary, occurs only under strict contractual confidentiality and security requirements, and requires prior approval from IEHP Safety & Security leadership.

G. Data Retention and Destruction

ALPR data will be retained for no longer than 60 days, unless the data is related to an open investigation or as required by law. After 60 days, said data will be permanently destroyed using secure deletion methods that prevent retrieval. IEHP will review the retention schedule periodically to ensure it remains consistent with operational needs and legal requirements.