Automated License Plate Recognition Systems and Information

(Interim Policy)

Responsible Official:	Vice Chancellor, Chief Information Officer
Responsible Office:	Office of Information Technology
Issuance Date:	05/26/2026
Effective Date:	05/26/2026
Summary:	This Policy governs the use of Automated License Plate Recognition (ALPR) Systems on any property owned, leased, or controlled by the University of California, Merced.
Scope:	This Policy applies to the use, maintenance, sharing, and dissemination of ALPR Information by the UC Merced Police Department (UCM PD) and the UC Merced Department of Transportation Services (TAPS).

Contact:	Nick Dugan, Vice Chancellor and Chief Information Officer
Email:	ndugan@ucmerced.edu
Phone:	(209) 228-4089

I. SUMMARY

Enacted to support the campus parking, safety, and law enforcement functions, this Policy governs the use, maintenance, sharing, and dissemination of Automated License Plate Recognition (ALPR) Information by the UC Merced Police Department (UCM PD) and UC Merced Transportation and Parking Services (TAPS).

This Policy serves as the usage and privacy policy required by CA Civil Code §§ 1798.90.51 and 1798.90.53 to ensure that the collection, use, maintenance, sharing, and dissemination of ALPR Information is consistent with federal, state, and local law and local practices.

II. DEFINITIONS

***ALPR*:** Automated License Plate Recognition (ALPR) System and Information collectively.

***ALPR Information*:** Information or data collected using an ALPR System.

***ALPR System*:** A searchable computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms to read and convert images of registration plates and the characters they contain into computer-readable data.

***Authorized Users*:** The only individuals permitted to install, operate, or search within the UCM PD or TAPS ALPR System.

***Campus ALPR Authority*:** The UC Merced campus official who authorizes the operation of ALPR Systems and the use of ALPR Information.

Major Change(s): Are changes that could have an effect on the privacy of individuals or security or governance of ALPR Systems or Information, including but not limited to changes related to ownership, technology, incidents, modification of scope, uses of AI, laws and regulations, risk assessments, vulnerabilities, or material updates or shifts in technology.

***PD ALPR System(s)*:** The ALPR System(s) procured, used, or accessed by UCM PD to assist with law enforcement and campus safety functions.

***TAPS ALPR System*:** The ALPR System procured, used or accessed by TAPS to monitor campus parking.

III. POLICY TEXT

UC Merced utilizes ALPR technology to capture and store digital license plate data and images to support campus parking, safety, and law enforcement functions, while recognizing the established privacy rights of the public and our UC community. All data and images collected by the ALPR are for official University use for the authorized purposes below.

A. AUTHORIZED USES AND PURPOSES

1. UCM PD may utilize PD ALPR System(s):

   To identify a vehicle on campus property when UCM PD identifies a lawful public safety or law enforcement need, including the detection of a vehicle (or person associated with that vehicle) wanted pursuant to a criminal investigation, in violation of a court order, in violation of an official campus stay-away order, or which poses a threat to one or more members of the campus community.

2. TAPS may utilize the TAPS ALPR System(s):

   To manage parking, count occupancy, identify violation locations, and enforce parking rules.

3. Authorized Users shall not use or allow others to use the equipment or database records for any other purpose (Civil Code § 1798.90.51; Civil Code § 1798.90.53). In no case shall the ALPR System be used for any purpose other than parking operations, legitimate law enforcement, or public safety purposes.

4. All other uses of ALPR Information must comply with applicable law and University policy, and are permitted only upon prior written approval by the Campus ALPR Authority.

B. TRAINING

1. All Authorized Users must complete training on ALPR Systems and Information prior to active use and certify they have read and understand all applicable University policies and procedures. Training must include:

    a. Systems operations to ensure the safeguarding of ALPR Information.

    b. Specific uses for which ALPR Systems and/or ALPR Information have been authorized.

    c. ALPR Information Requirements set forth below, and the procedures to implement them.

    d. UC Cyber Security training

C. PRIVACY AND SECURITY OF UCM PD AND TAPS ALPR SYSTEMS

1. Any installation of an ALPR System or new use of ALPR Information must undergo a privacy and security review by the Campus Privacy Officer and Chief Information Security Officer, respectively, for Protection Level 4, as defined by BFS-IS-3: Electronic Information Security, prior to implementation and upon any Major Changes to the system, vendor, or processes for access. The Campus ALPR Authority must ensure that Authorized Users, defined below, use administrative, operational, technical, and physical safeguards to protect ALPR Information from unauthorized access, use, destruction, modification, or disclosure, including the following minimum safeguards:

    a. Administrative:

        i. Username and password-protected access to the ALPR System in compliance with UC Merced password policies.

        ii. Monitoring and auditing usage of the database and ALPR Information.

        iii. Appropriate training and access controls.

b. Physical:

   i. Secure storage of computers with access to ALPR Systems and Information.

   ii. Physical access is limited to ALPR technicians, Campus ALPR Authority, TAPS Director, and the Chief of UCM PD or their designee(s).

c. Technical: All information will be encrypted in transit and at rest and protected from unauthorized access, use, or disclosure in accordance with UC Policy BFB-IS-3.

d. Data Protection:

   i. ALPR Information is classified at Protection Level 3 and Protection Level 4 (depending on the specific combinations of data at issue).

   ii. UC Merced departments with Authorized Users who utilize ALPR Information are responsible for ensuring systems and processes are in place for its proper collection, storage, and disposal in compliance with applicable UC data retention and disposal standards.

D. SHARING OF ALPR INFORMATION

1. Sharing, disclosing, publishing, providing access to, selling, or exchanging of ALPR Information from the UCM PD ALPR or TAPS ALPR Systems outside of UCM PD, TAPS, or designated IT staff assigned to UCM PD and TAPS is prohibited unless required by law or in accordance with applicable law and after consultation between the Campus ALPR Authority, campus legal counsel, and the campus privacy officer, in support of law enforcement investigations, academic research, or other legal purpose.

2. The ALPR data may be shared only with public agencies and only as otherwise permitted by law (Civil Code § 1798.90.55).

   For purposes of this section, a public agency is limited to California state or local agencies, including law enforcement agencies, and does not include out-of-state or federal law

enforcement agencies (Civil Code § 1798.90.5). UCM PD may share the date, time, and location of any confirmed matches of ALPR data with other public agencies related to an ongoing and active investigation. To provide such information, public agencies are required to provide:

a. A formal request on department letterhead or form provided by UCM PD;

b. Contact information;

c. Associated case number;

d. Crime being investigated;

e. Requested license plate number; and

f. Make, model, and color of vehicle.

3. No UCM PD ALPR or TAPS ALPR database access will be provided to any external law enforcement or immigration enforcement agency, including joint task forces that involve non-UCM entities, public agencies or other government organizations, unless required by law, court order, or search warrant, or where there is explicit consent of the data subject(s).

4. Public access: ALPR Information shall be made public or deemed exempt from public disclosure pursuant to state or federal law. Information related to the maintenance and governance of ALPR Systems and access to ALPR Information shall be available for public disclosure, in accordance with applicable law.

5. All other disclosures to external entities are expressly prohibited except where required by law.

E. ALPR INFORMATION REQUIREMENTS.

1. Except as described below, ALPR Information will be retained for sixty (60) days and then deleted, unless a court order or legal authority requires otherwise. Data retention limits shall be enforced through automated settings in the ALPR System, configured by the Campus ALPR Authority or their designee in accordance with the retention periods established in this Policy and the UC Records Retention Schedule. The Records Management Coordinator shall be consulted in establishing retention settings and shall periodically verify that system settings conform to the approved schedule.

2. UCM PD and TAPS ALPR Systems information may be aggregated and kept for legitimate business needs, including, but not limited to, security assessments, traffic reporting, parking activity, and maintenance needs.

3. Accuracy of Data. UCM PD and TAPS ALPR data collection is automated such that license plate images and details of collection are included in the system without human review. Although infrequent, license plate translation may be incomplete or inaccurate. Any alert provided by an ALPR System is to be considered informational and advisory in nature and requires further verification before action. The UCM PD and TAPS Managers, or their designees, will manually review the license plate or plate image to validate the license plate before initiating an investigation into an incident.

IV. RESPONSIBILITIES

A. FOR IMPLEMENTATION AND ENFORCEMENT

1. The Vice Chancellor, Chief Information Officer is the Campus ALPR Authority and is responsible for implementing this Policy in accordance with California Civil Code § 1798.90.51. The VC-CIO may delegate the role of Campus ALPR Authority, except that duties may not be delegated to TAPS or the UC Merced Police Department, but the role may not be further redelegated.

B. AUTHORIZED USERS

1. Authorized Users must operate ALPR Systems or access or use ALPR Information only for the purpose(s) specified and as appropriate within the authorized personnel's job function. Any other operation, access, or use is unauthorized and may result in civil or criminal penalties, disciplinary action under university policies or, as applicable, collective bargaining agreements.

2. The following are the Authorized Users of the UCM PD ALPR and TAPS ALPR Systems for the following activities:

3. System Security and Maintenance: In addition to periodic audits of the system, designated UCM PD, TAPS, Office of Information Technology, and vendor staff for the system will monitor the ALPR System for performance, governance, reliability, and functionality;

    a. UCM PD ALPR Search: Dispatchers, Patrol Operations, personnel directly responsible for UCM PD safety operations;

    b. TAPS Search: Personnel directly engaged in or responsible for the oversight of parking enforcement; and

    c. Monitoring, auditing, and oversight: As described below.

4. All Authorized Users must complete all applicable background checks prior to access to any ALPR System or Information.

C. AUDITING AND OVERSIGHT

1. UCM PD shall be responsible for storing and monitoring all logins and queries of the UCM PD ALPR System, as required by CA Civil Code § 1798.90.52. At a minimum, the following information must be maintained for every query of the ALPR System: username, the date and time of access, the purpose for the access, and the license plate number or other data element(s) used to query the ALPR System.

2. TAPS shall be responsible for storing and monitoring all logins and queries of the TAPS ALPR System, as required by CA Civil Code § 1798.90.52. At a minimum, the following information must be maintained for every query of the ALPR System: username, the date and time of access, the purpose for the access, and the license plate number or other data element(s) used to query the ALPR System.

3. UC Merced departments with Authorized Users must conduct periodic monitoring to review access rules, logs, configuration, and to confirm active individual accounts. The Campus ALPR Authority or their designee will periodically monitor querying activity via electronic logs to ensure searches are tied to legitimate transactions and other aforementioned business needs. In accordance with the University of California Records Retention Schedule, audit logs will be retained for 8 years and then destroyed. Records pertaining to pending, foreseeable, or ongoing litigation, an investigation, an ongoing audit, or a request for records cannot be destroyed until these actions have been completed or resolved. Records pertaining to pending, foreseeable, or ongoing litigation, an investigation, an ongoing audit, or a request for records will be maintained in accordance with the University's Records Management Program guidelines and instructions from legal counsel.

D. CONTRACTING

1. Procurement is responsible for ensuring that contracts comply with this Policy and with the University's data sharing policies and procedures.

E. PUBLICATION AND POSTING

1. In accordance with CA Civil Code § 1798.90.53, the ALPR Policy must be publicly published. The Vice Chancellor, Chief Information Officer will ensure that this Policy undergoes the campus administrative policy development process so the Policy is formally issued and posted on the UCM Administrative Policy website. The Chief of UCM PD will ensure that this Policy is posted conspicuously on the UCM PD website. The Director of

Transportation and Parking Services will ensure that this Policy is posted conspicuously on the TAPS website.

2. Chief of UCM PD is responsible for ensuring that a public notice is posted at the entrance(s) of any facility with fixed ALPR cameras associated with UCM PD.

3. Director of Transportation and Parking Services is responsible for ensuring that a public notice is posted at the entrance(s) of any facility with fixed ALPR cameras associated with TAPS ALPR System(s).

V. REFERENCES AND RESOURCES

State Laws and Regulations

- CA Civil Code §§ 1798.90.5 – 1798.90.55

UC Policy

- UC Protection Level Classification Guide
- UC Institutional Information Disposal Standard
- UC Records Retention Schedule

VI. REVISION HISTORY

Date	Action/Summary of Changes
5/26/2026	Interim Policy issued