

Regulation on Automatic License Plate Recognition Systems

I. Purpose. This regulation sets Systemwide minimum standards for Automatic License Plate Recognition (ALPR) systems used by constituent institutions of the University of North Carolina System ("UNC System"). These standards govern how ALPR technology and data are secured, retained, and audited. This regulation ensures that campus safety teams adopting new technology maintain the highest standards of privacy, data accountability, mandatory training, and oversight, while fully complying with applicable laws, including Article 3D of Chapter 20 of the North Carolina General Statutes.

II. Scope and Institutional Responsibility.

A. This regulation applies to each constituent institution that owns, leases, subscribes to, operates, or obtains access to an ALPR system through its campus law-enforcement agency or on that agency's behalf. This regulation does not apply to technology controlling access to parking facilities.

B. Before an ALPR system becomes operational, each covered institution shall adopt written institutional directives implementing this regulation and complying with applicable law. Institutions may implement more restrictive safety protections or measures surrounding ALPR systems within their policies, provided such measures comply with applicable law and enhance campus community safety.

C. The chief of police shall designate an ALPR administrator responsible for administration, access controls, records management, auditing, retention, training, and vendor coordination.

D. Institutional directives may be scaled to local staffing, technology, geography, and operational needs but shall not provide less protection or oversight than this regulation.

III. Authorized and Prohibited Uses.

A. ALPR systems and ALPR data may be used only for documented law enforcement purposes and only by authorized users acting within the scope of their official duties. Authorized uses include criminal investigations, locating missing or endangered persons, locating lost or stolen vehicles or license plates, apprehending persons with outstanding felony warrants, and responding to validated ALPR alerts.

B. ALPR systems and ALPR data shall not be used to enforce traffic violations; monitor persons or vehicles based solely on protected characteristics or lawful expressive activity; conduct broad, speculative, or indiscriminate searches; track attendance at political, labor, religious, or social events absent a documented law-enforcement purpose; or otherwise circumvent legal restrictions, retention limits, access controls, or audit requirements.

C. System placement and deployment decisions shall be reasonably related to public safety, or law enforcement needs and shall consider privacy, civil-liberties, community-impact, and data-security risks.

IV. Access, Security, and Disclosure.

A. Access to ALPR systems and data shall be limited to trained authorized users and protected through institution-approved security controls, including multifactor authentication.

B. ALPR systems shall maintain audit logs sufficient to identify users, searches, alerts, disclosures, and other system activity. These audit logs shall be made available upon request to the UNC System vice president for safety & emergency operations or designee.

C. Authorized personnel must encrypt and secure all ALPR data during storage and transit to meet the highest applicable standards of both university information security and criminal-justice information policies. ALPR data shall be strictly protected.

D. An institution shall remain responsible for compliance when systems or data are hosted, maintained, or operated by third parties, including data that is hosted or stored by a third-party using cloud-based infrastructure outside of the direct control of the institution.

V. Contracts and Service Arrangement Minimums. Contracts and service arrangements for ALPR systems must meet the following minimum requirements:

1. Each must ensure that vendors agree to support the institution's compliance with the terms of this regulation;
2. Each must provide that ALPR data remains under the institution's control and may be processed only to provide contracted services;
3. Each must prohibit model training, sale, advertising use, independent analytics, or other secondary use of ALPR data;
4. Each must require role-based access, logging, encryption, incident notification, secure deletion, and cooperation with audits and legal holds;
5. Each must limit subcontractor access and require equivalent protections;
6. Each must prohibit the vendor from disclosing ALPR data except as directed by the institution or required by law, with advance notice to the institution when legally permitted; and
7. Each must require return or secure destruction of ALPR data when the agreement ends.

VI. Retention, Preservation, and Destruction.

A. Routine ALPR data must be automatically and irretrievably deleted no later than 30 days after capture, notwithstanding the longer 90-day period allowed by statute. No exception to this deletion schedule is permitted unless an active, written qualifying preservation request, search warrant, court order, or other authority permitted by law in compliance with G.S. 20-183.32 is logged into the agency audit system prior to the expiration of the 30-day deletion window.

B. A preservation request must be written and sworn and must contain the information required by G.S. 20-183.32, including the relevant camera location, plate, dates and time frames, case and parties, and specific and articulable facts establishing relevance and materiality to a qualifying investigation or other statutorily authorized matter.

C. Data preserved through a preservation request must be destroyed no later than one year after the initial request unless the period is reset by a renewed written qualifying request or the data is retained under another lawful authority.

D. Hot-list entries must be removed when no longer relevant. Audit and administrative records must be retained in accordance with applicable records-retention schedules and legal requirements. As used here, a "hot list" means database populated with items of specific concern to the investigative interests of law enforcement within the constituent institution. This may include, but is not limited to, stolen or wanted vehicles and license plates, missing persons, human trafficking, and vehicles registered to individuals with active domestic violence protective orders or others banned from university property.

E. Institutions must configure and periodically verify automated deletion processes.

VII. Disclosure and Interagency Access.

A. ALPR data is confidential, not a public record, and may be disclosed only as authorized by law. Requests for access or disclosure from other federal, state, and local law-enforcement agencies in North Carolina shall be documented, reviewed, and may be approved by the ALPR administrator or designee. Requests for access or disclosure from law-enforcement agencies located outside North Carolina, including federal agencies operating in different states, shall be documented and reviewed by the ALPR administrator or designee but must be time-limited and approved by a campus official who reports directly to the chancellor. Any interagency sharing arrangement must be governed by a legally binding, formal agreement explicitly restricting authorized purposes, enforcing advanced security protocols, defining minimal retention periods, requiring mandatory, independent third-party auditing, and specifying immediate, automatic termination of access for non-compliance. An institution must deny a request unless disclosure is explicitly and unambiguously mandated by statutory law.

B. Continuous, automated, bulk, or federated data access by external North Carolina-based agencies is strictly prohibited unless authorized by a written agreement approved by the agency head and institutional legal counsel, addressing limitations of purpose, users, data, duration, further disclosure, retention, security, and auditing and shall permit suspension or termination of access. Each disclosure or access event must also satisfy the written request and legitimate purpose requirements of applicable law. Similar access afforded to external agencies based outside of North Carolina must comply with the foregoing requirements,

and, in addition, that access must be time-limited and approved by a campus official who reports directly to the chancellor.

C. Data received from another ALPR system shall receive protections at least equivalent to data generated by the institution and shall be used subject to the providing agency's restrictions.

VIII. Training, Oversight, and Accountability.

A. No person may access or operate an ALPR system before completing institution approved training. Refresher training and documented policy review shall occur at least semi-annually; after material legal, regulatory, policy, or system changes; and immediately following any recorded system misuse. Institutions shall maintain detailed, auditable training records for authorized users, which must be reviewed at least semi-annually by a designated command staff member.

B. Training shall address, at a minimum: authorized and prohibited purposes; privacy, civil-rights, and civil-liberties protections; data quality, plate misreads, hit confirmation, and avoidance of confirmation bias; access, security, sharing, retention, preservation, and destruction requirements; documentation and audit-log requirements; reporting suspected misuse, security incidents, and equipment problems; and the automatic revocation of system access as a consequence of violations.

IX. Supervisory Oversight, Auditing, and Accountability.

A. Supervisors shall, at least quarterly (or monthly, if high volume of data is identified), review all user access, searches, hot-list entries, alerts, disclosures, preservation actions, and retained data for compliance and reasonable use. Every review must be formally documented, signed by the supervisor, and logged in an immutable or timestamped audit trail. Each covered campus law enforcement agency shall conduct and document an audit at least semi-annually and submit the results to the campus chief of police. The audit shall evaluate strict compliance with this regulation, the institutional directive, and all applicable state and federal data privacy laws.

B. Audit findings presenting any legal, privacy, civil rights, security, or operational risk must be reported within 24 hours to the chief compliance officer, general counsel, chief information security officer, and chief of police or their designee. Access must be immediately suspended upon detection to protect data and prevent misuse.

C. All suspected misuse, security incidents, or violations must immediately be investigated. Mandatory corrective action shall be enforced, comprising immediate access revocation, mandatory retraining, formal disciplinary action to include termination, immediate contract corrections, if warranted, and immediate referral to legal authorities. In addition to any civil or criminal penalties imposed by law, any employee found to have misused this technology maintained by the institution shall be subject to appropriate workplace disciplinary processes.

X. Institutional Implementation and Transparency.

A. Institutions shall mandate rigid adherence to all requirements of G.S. 20-183.31, this regulation, and the following specific operational controls include: access controls (multi-factor authentication, role-based access, and the principle of least privilege), retention and preservation

(non-rewritable storage, automated deletion, and legal hold freezes), disclosure processes (multi-tier authorization, mandatory redaction, and cryptographic logging), training requirements (mandatory pre-access certification and semi-annual refresher training), auditing procedures (continuous automated logging, weekly log reviews, and scheduled and unscheduled audits), and incident reporting (immediate containment, zero-exception reporting within 24 hours, and root-cause disclosure).

B. Subject to absolute operational security or campus safety guidance, institutions may provide a generalized public overview of the ALPR program. This overview is strictly limited to legal authority and a basic explanation of the institution's process. Specific retention periods, privacy vulnerabilities, camera locations, and technical configurations shall not be disclosed except as required by law. Any information that could tangibly compromise law enforcement tactics or technical system integrity must be withheld from public materials in accordance with applicable law.

XI. Other Matters.

A. **Effective Date.** The requirements of this regulation shall be effective on December 1, 2026. Institutions operating an ALPR system on that date shall bring their institutional directives, contracts, configurations, and practices into compliance no later than January 1, 2027.

B. **Relation to State and Federal Law.** This regulation supplements and does not supplant or modify statutory, regulatory, constitutional, court-ordered, or other legal requirements. If a conflict arises, controlling law governs, and the institution shall consult legal counsel and apply the remainder of this regulation to the fullest extent possible.

C. **Authority.** This regulation is promulgated by the president pursuant to Section 100.2 of the UNC Policy Manual, *Adoption of the UNC Policy Manual, Promulgation of Policies, and Use of Reporting Requirements*, and applicable law.