CHAPTER 35 SURVEILLANCE TECHNOLOGY AND EQUIPMENT

35.01 PURPOSE

The purpose of this policy is to establish guidelines governing the acquisition, operation, access, use, retention, preservation, dissemination, security, and oversight of surveillance technology utilized by the Department, specifically Automatic License Plate Reader (ALPR/LPR) systems and Unmanned Aircraft Systems (UAS), commonly referred to as drones.

The Department recognizes that surveillance technology can enhance public and officer safety, assist in criminal investigations, locate wanted, missing, or endangered persons, improve situational awareness, document incidents, and enhance the efficient deployment of law enforcement resources.

The Department further recognizes that the use of surveillance technology carries significant responsibilities concerning constitutional protections, individual privacy, information security, and public trust. Surveillance technology shall therefore be utilized only for authorized purposes and in accordance with applicable federal law, North Carolina law, and Department policy.

35.02 POLICY

It is the policy of the Department that surveillance technology shall be used only for legitimate law enforcement, public safety, emergency response, training, or other authorized governmental purposes.

Surveillance technology shall not be used for personal purposes or in an arbitrary, discriminatory, harassing, retaliatory, or otherwise unlawful manner.

Access to surveillance systems and information obtained through those systems shall be limited to authorized personnel having a legitimate and documented purpose for such access.

The use of surveillance technology shall be conducted in a manner consistent with the United States Constitution, North Carolina Constitution, North Carolina General Statutes, applicable federal regulations, judicial decisions, and Department policy.

35.03 DEFINITIONS

A. Automatic License Plate Reader (ALPR/LPR)

A system consisting of one or more mobile or fixed automated high-speed cameras used in combination with computer algorithms to convert images of license plates into computer-readable data, as defined by North Carolina law.

B. Captured Plate Data

Information obtained through an ALPR system, including the license plate number and associated information captured by the system, such as the date, time, location, vehicle image, or other information generated by the system.

C. Alert/Hit

A notification generated when a license plate detected by an ALPR system potentially matches a license plate contained within an authorized database or alert list.

D. Alert/Hot List

A database or list containing license plates associated with vehicles or persons having a legitimate law enforcement nexus.

E. Historical Search

A search or query of previously captured ALPR data.

F. Law Enforcement Purpose

For purposes of ALPR use, a law enforcement purpose shall have the meaning established by N.C.G.S. §20-183.30 and includes:

1. Actions related to criminal investigations, arrests, prosecutions, post-conviction confinement, or supervision;

2. Apprehending an individual with an outstanding felony warrant;

3. Locating a missing or endangered person; or

4. Locating a lost or stolen vehicle.

G. Unmanned Aircraft System (UAS)

An unmanned aircraft and associated elements, including communication links and components necessary for the pilot in command to safely and efficiently operate the aircraft in the national airspace system.

H. Pilot in Command (PIC)

The person designated as having final responsibility and authority for the safe operation of a UAS during a particular flight.

I. Surveillance

The observation, monitoring, collection, or recording of information concerning a person, dwelling, curtilage, private property, vehicle, location, activity, or event through technological means.

35.04 GENERAL RESPONSIBILITIES

A. Surveillance equipment shall only be operated or accessed by Department personnel who have received appropriate authorization and training.

B. Employees shall use surveillance technology only in furtherance of their official duties.

C. Employees shall not attempt to circumvent security, audit, retention, or access-control features of any surveillance system.

D. Employees shall not allow another person to use their individual username, password, authentication credentials, or system account.

E. Employees shall have no expectation of personal privacy concerning their use of Department surveillance systems. Searches, queries, downloads, access, and other system activities may be recorded and audited.

F. Employees shall immediately report suspected unauthorized access, misuse, loss, disclosure, or compromise of surveillance information to a supervisor.

G. All initial, recurrent, proficiency and specialized training associated with ALPR and UAS operations shall be documented and maintained in accordance with the Department's training records system and applicable NCLEA requirements.

35.05 AUTOMATIC LICENSE PLATE READER SYSTEMS

A. Authorized Use

ALPR systems and captured plate data shall be obtained, accessed, preserved, and disclosed only for a law enforcement purpose authorized by N.C.G.S. Chapter 20, Article 3D.

Authorized purposes include:

1. Actions related to criminal investigations, arrests, prosecutions, post-conviction confinement, or supervision;

2. Apprehending an individual with an outstanding felony warrant;

3. Locating a missing or endangered person; and

4. Locating a lost or stolen vehicle.

B. Captured plate data **shall not** be used for the enforcement of traffic violations.

C. Authorized Databases

ALPR systems may compare captured plate data against databases approved by the Chief of Police or designee and permitted by law.

The Department shall identify and maintain a record of databases authorized for comparison.

When updates to authorized databases are available, the ALPR system shall be updated at least every 24 hours or as soon as practicable after updated information becomes available.

C. Department-Created Alerts

Employees shall create or request an ALPR alert only when the alert serves an authorized law enforcement purpose.

Department-created alerts should include, when applicable:

1. License plate number;
2. Reason for the alert;
3. Associated case, incident, warrant, or investigative reference number;
4. Identity of the employee entering or requesting the alert;
5. Date of entry;
6. Applicable expiration date; and
7. Relevant officer-safety or investigative information.

Employees responsible for Department-created alerts shall ensure the information remains accurate and shall remove or cause the removal of an alert when the underlying law enforcement purpose no longer exists.

D. Response to ALPR Alerts

An ALPR alert shall be treated as an investigative lead and shall not automatically constitute independent legal justification for enforcement action.

Before initiating enforcement action based substantially upon an ALPR alert, an officer shall, when reasonably practicable:

1. Visually verify that the observed license plate matches the plate identified by the ALPR system;
2. Compare available vehicle information with the vehicle observed;
3. Confirm through an appropriate law enforcement database or communications center that the information generating the alert remains current and valid; and
4. Consider the totality of the circumstances before taking enforcement action.

Any detention, search, arrest, or other enforcement action shall be supported by the legal justification required under the circumstances.

E. Historical Searches

Historical ALPR searches shall only be conducted for an authorized law enforcement purpose. Whenever the system provides the capability, the employee conducting the search shall enter:

1. A case or incident number; and
2. A brief description or other indication of the law enforcement purpose for the search.

Employees shall not conduct historical ALPR searches based upon curiosity or for personal, political, commercial, retaliatory, or other unauthorized purposes.

F. Broad or Sensitive Searches

ALPR searches designed to identify multiple vehicles, establish patterns of movement or association, identify vehicles present at a particular sensitive location or event, or otherwise conduct broad historical analysis should receive supervisory authorization before being conducted, unless exigent circumstances make prior approval impracticable.

Particular consideration shall be given to searches involving locations or activities associated with constitutionally protected activity, including religious institutions, political events, demonstrations, medical facilities, or similar sensitive locations.

Nothing in this section authorizes an ALPR search that is otherwise prohibited by North Carolina law.

G. Prohibited ALPR Uses

Employees shall not use ALPR systems or information:

1. For personal purposes;
2. For general traffic enforcement;
3. To locate or track another person without an authorized law enforcement purpose;
4. To obtain information regarding family members, friends, acquaintances, coworkers, public officials, celebrities, or other persons based upon curiosity or personal interest;
5. To monitor lawful First Amendment-protected activity absent an independent lawful law enforcement purpose;
6. For commercial purposes;
7. In a discriminatory, harassing, or retaliatory manner; or
8. For any purpose prohibited by law or Department policy.

35.06 ALPR DATA RETENTION AND PRESERVATION

A. Captured plate data shall not routinely be preserved for more than 90 days after the date the data is captured.

B. Captured plate data may be preserved beyond 90 days only as authorized by N.C.G.S. §20-183.32, including pursuant to:

1. A lawful preservation request;
2. A search warrant issued pursuant to North Carolina law; or
3. A federal search warrant issued in compliance with federal law.

C. A preservation request shall comply with the requirements of N.C.G.S. §20-183.32, including applicable requirements concerning a written and sworn statement, identification of the relevant data, facts supporting the request, and associated investigation.

D. Personnel seeking preservation of ALPR information shall coordinate with the appropriate investigative supervisor or other designated employee to ensure the request satisfies statutory requirements.

E. Preserved data shall not be retained beyond the period authorized by law unless continued preservation is lawfully authorized.

F. Data incorporated into an investigative or evidentiary record shall thereafter be maintained in accordance with applicable law and Department evidence and records-retention requirements.

35.07 ALPR TRAINING AND PROFICIENCY

A. ALPR users shall receive appropriate training before being granted system access.

B. Training should include:

1. Authorized uses;
2. Statutory restrictions;
3. Alert verification;
4. Historical searches;
5. Data retention and preservation;
6. Information sharing;
7. Privacy and constitutional considerations;

8. Security requirements; and

9. Department policy.

C. All initial, recurrent, proficiency, and specialized training associated with ALPR access shall be documented and maintained in the Department's official training records system in accordance with the Department's Training Policy and applicable NCLEA requirements.

35.08 ALPR DISCLOSURE AND INFORMATION SHARING

A. Captured plate data is confidential and shall be handled in accordance with North Carolina law.

B. Captured plate data shall not be treated as a public record when North Carolina law provides otherwise.

C. Captured plate data may only be disclosed to persons or agencies authorized by N.C.G.S. §20-183.32 and for a legitimate law enforcement purpose.

D. Disclosure to another qualifying law enforcement agency shall be pursuant to the written request required by North Carolina law. Electronic written requests may be accepted when legally permissible.

E. The Department may decline disclosure when it determines that disclosure would compromise an ongoing investigation.

F. Captured plate data shall not be sold for any purpose.

G. The Department shall maintain appropriate documentation of ALPR disclosures.

35.09 ACCESS TO EXTERNAL ALPR SYSTEMS

A. Employees may access ALPR information maintained by another law enforcement agency or authorized ALPR network only when:

1. The employee has an authorized law enforcement purpose;

2. Access complies with the rules governing the external system;

3. Access is permitted by North Carolina and federal law; and

4. The employee complies with the documentation requirements of this policy.

B. Employees accessing an outside ALPR system remain subject to this policy.

35.10 ALPR SECURITY, MAINTENANCE, AND AUDITING

A. Security

1. Access to ALPR systems shall be limited to authorized personnel according to job responsibilities and operational need.
2. Where available, multifactor authentication and other reasonable security controls should be utilized.

B. Maintenance and Calibration

The Department shall maintain applicable maintenance and calibration schedules and records for Department-operated ALPR systems as required by North Carolina law.

C. Auditing

1. The Department shall conduct an audit of ALPR use at least annually. Additional audits may be conducted at the direction of the Chief of Police.
2. Audits shall examine:
    a. User access;
    b. Historical searches;
    c. Search justifications;
    d. Alert-list entries;
    e. Data preservation;
    f. Data sharing and disclosure;
    g. Retention compliance;
    h. External-system access;
    i. Security practices; and
    j. Suspected or identified unauthorized use.
3. The results of each formal audit shall be reported to the Chief of Police and maintained in accordance with Department records requirements and policies.

35.11 ALPR VENDOR AND THIRD-PARTY REQUIREMENTS

A. Contracts involving ALPR systems or storage should address, when applicable:

1. Department ownership or control of Department-generated information;
2. Data retention and deletion;
3. Vendor access to Department information;
4. Restrictions on secondary or commercial use;
5. Information sharing;
6. Cybersecurity protections;
7. Security-breach notification;
8. Audit capabilities;
9. Termination of vendor access; and
10. Return or destruction of Department information upon termination of the contractual relationship.

B. Vendor functionality shall not expand the authorized uses of ALPR information beyond those permitted by North Carolina law and Department policy.

35.12 UNMANNED AIRCRAFT SYSTEM (UAS) PROGRAM

A. General

Department UAS operations shall comply with the United States Constitution, North Carolina law, applicable Federal Aviation Administration requirements, and Department policy. Only personnel authorized by the Department and possessing the required training, certification, or qualification shall operate a Department UAS.

B. Authorized Uses

Subject to applicable legal requirements, a Department UAS may be deployed for:

1. Search and rescue operations;
2. Missing-person searches;
3. Tactical operations;
4. Barricaded-person incidents;
5. Hostage situations;
6. Crime scene documentation;
7. Serious traffic collision documentation or reconstruction;
8. Pursuit or apprehension of an escapee or suspect when authorized by law;
9. Situations involving an imminent threat to life;
10. Situations involving a threat of serious property damage;
11. Situations involving the imminent destruction of evidence;
12. Hazardous-material incidents;
13. Disaster or emergency response;
14. Situations in which UAS deployment may reduce substantial risk to officers, emergency responders, or the public;
15. Photography of gatherings to which the general public is invited when permitted by law;
16. Training and proficiency exercises;
17. Department facility or public property documentation; and
18. Other lawful law enforcement operations approved by the Chief of Police or his/her designee.

35.13 UAS SURVEILLANCE AND LEGAL AUTHORITY

A. Department personnel shall comply with N.C.G.S. §15A-300.1 when using a UAS for surveillance.

B. Except as otherwise authorized by law, Department personnel shall not use a UAS to conduct surveillance of:

1. A person or an occupied dwelling and its curtilage without the person's consent; or

2. Private real property without the consent of the owner, easement holder, or lessee.

C. The use of a UAS by law enforcement is authorized by law in the following circumstances:

1. Pursuant to a search warrant authorizing UAS use;

2. A qualifying high-risk terrorist threat; *North Carolina law allows law-enforcement UAS use to counter a high risk of terrorist attack by a specific individual or organization when the required determination has been made by the U.S. Secretary of Homeland Security or the North Carolina Secretary of Public Safety based upon credible intelligence.*

3. To conduct surveillance of an area within an officer's plain view when the officer is in a location where the officer has a legal right to be;

4. When reasonable suspicion exists that swift action is necessary to:

a. Prevent imminent danger to life;

b. Prevent serious damage to property;

c. Forestall the imminent escape of a suspect;

d. Prevent the destruction of evidence;

e. Conduct pursuit of an escapee or suspect; or

f. Facilitate the search for a missing person;

5. To photograph gatherings to which the general public is invited on public or private property; or

6. Under other circumstances expressly authorized by federal or North Carolina law.

D. When uncertainty exists regarding whether a proposed UAS operation constitutes surveillance requiring a search warrant or other legal

authorization, personnel should consult a supervisor and, when appropriate, a prosecutor or legal advisor before deployment.

E. Personnel shall recognize that unauthorized UAS surveillance may result in civil liability and may affect the admissibility of evidence.

F. Relationship to Search and Seizure Policy

1. Nothing in this policy supersedes the Department's Search and Seizure Policy.

2. UAS surveillance constituting a search or seizure shall comply with the Department's Search and Seizure Policy, applicable constitutional requirements, N.C.G.S. §15A-300.1, and other applicable law.

3. When a search warrant authorizes UAS surveillance, personnel shall operate within the scope and limitations of the warrant.

35.14 UAS SUPERVISORY AUTHORIZATION

A. Except for training, equipment testing, or other routine administrative flights specifically authorized by the UAS Program Coordinator, operational UAS deployments shall receive supervisory authorization when circumstances permit.

B. The supervisor authorizing the deployment should consider:

1. The purpose of the deployment;

2. Whether the proposed operation is authorized by law;

3. Whether a search warrant or consent is required;

4. Whether an exigent circumstance exists;

5. Whether less intrusive or safer alternatives are reasonably available;

6. Potential risk to officers, the public, and property; and

7. Applicable FAA or airspace restrictions.

C. Emergency deployment may occur without prior supervisory authorization when delay would create an unreasonable risk to life, safety, evidence, or apprehension of a suspect and the deployment is otherwise legally permissible.

D. A supervisor shall be notified as soon as reasonably practicable following an emergency deployment.

E. Prolonged, recurring, or targeted UAS surveillance should receive command-level authorization in addition to any search warrant or other legal authority required by law.

35.15 UAS PILOT IN COMMAND

A. The designated Pilot in Command (PIC) has final responsibility for the safe operation of the aircraft and shall:

1. Determine whether the flight may be conducted safely and legally;
2. Identify the FAA operating authority applicable to the flight;
3. Verify applicable airspace requirements and authorizations;
4. Conduct or ensure completion of appropriate pre-flight inspections;
5. Consider weather, visibility, obstacles, persons, vehicles, and other hazards;
6. Ensure compliance with the applicable FAA operating authority;
7. Maintain operational control of the aircraft;
8. Terminate a flight when continued operation would create an unreasonable safety risk or violate applicable law or regulation; and
9. Document the flight as required by this policy.

B. No supervisor shall require a PIC to conduct a flight that the PIC reasonably determines cannot be safely or legally conducted.

35.16 FAA OPERATING REQUIREMENTS AND COMPLIANCE

A. Department UAS operations shall be conducted under the appropriate FAA authority applicable to the operation, including 14 CFR Part 107 or authorized Public Aircraft Operations/Certificate of Waiver or Authorization when applicable.

B. When the Department possesses more than one form of operating authority, personnel shall identify the authority under which the particular operation is being conducted.

C. Personnel serving as Remote Pilot in Command under Part 107 shall possess the certification required by the FAA and maintain required aeronautical knowledge currency.

D. Department aircraft shall be properly registered and marked and shall comply with applicable Remote Identification requirements.

E. The PIC shall determine the classification and status of airspace in which the operation will occur and obtain required airspace authorization before flight.

F. Operations shall comply with applicable Temporary Flight Restrictions and other FAA airspace restrictions.

G. Night operations shall comply with applicable FAA pilot qualification, aircraft lighting, airspace, and operational requirements.

H. Operations over persons, open-air assemblies, or moving vehicles shall only be conducted when permitted by the FAA authority governing the flight and in accordance with applicable limitations.

I. Beyond Visual Line of Sight operations shall not be conducted unless specifically authorized under applicable FAA authority and approved by the Chief of Police or designee.

35.17 UAS RECORDING AND EVIDENCE

A. UAS recording equipment should be activated when recording serves an operational, investigative, evidentiary, training, documentation, or public safety purpose.

B. Any UAS photograph, video, recording, or other digital information determined to possess evidentiary or investigative value shall be submitted to the Department evidence management system and handled in accordance with Department Property and Evidence Policy.

C. Evidentiary UAS material shall be maintained in a manner that preserves its integrity and chain of custody.

D. UAS imagery shall not be stored on personal devices or unauthorized systems.

E. Non-evidentiary recordings shall be retained and disposed of in accordance with applicable North Carolina records-retention requirements and Department policy.

F. Employees shall not make personal copies of UAS recordings.

35.18 UAS LAUNCH AND RECOVERY AND SPECIAL OPERATING RESTRICTIONS

A. Department UAS launch and recovery shall comply with N.C.G.S. §15A-300.2, applicable FAA requirements, and local ordinances.

B. Required consent or legal authorization shall be obtained before launching or recovering a UAS from State or private property.

C. Operations from property owned or controlled by a unit of local government shall comply with applicable local requirements.

D. The PIC shall select launch and recovery locations that reasonably minimize risk to persons, property, and other aircraft.

E. UAS operations in proximity to local confinement facilities or State or federal correctional facilities shall comply with N.C.G.S. §15A-300.3.

F. UAS operations in proximity to a forest fire shall comply with N.C.G.S. §15A-300.4, applicable FAA restrictions, and any Temporary Flight Restriction.

G. Nothing in this policy authorizes a flight that would interfere with manned firefighting aircraft or emergency operations.

35.19 UAS PRIVACY AND PROHIBITED USES

A. Department UAS shall not be used:

1. For personal purposes;

2. For harassment, intimidation, or retaliation;

3. To conduct surveillance based solely upon a person's race, ethnicity, national origin, religion, sex, political affiliation, or other status protected by law;

4. To monitor lawful demonstrations, protests, religious activities, political activities, or other First Amendment-protected activities absent an independent legitimate law enforcement or public safety purpose;

5. To conduct surveillance of a person, dwelling, curtilage, or private property contrary to North Carolina law;

6. To intentionally observe areas in which a person has a reasonable expectation of privacy without appropriate legal authority;

7. For unauthorized personal photography or recording;

8. For commercial purposes;

9. In violation of FAA regulations or operating authority; or

10. For any purpose prohibited by federal or North Carolina law.

B. UAS imagery shall not be subjected to facial recognition, biometric identification, persistent automated tracking, or similar automated identification technology unless specifically authorized by Department policy, approved by the Chief of Police, and permitted by applicable law.

C. The availability of a technological capability through a UAS manufacturer or vendor does not, by itself, constitute Department authorization to use that capability.

D. Department personnel shall recognize that unauthorized UAS surveillance may result in civil liability and may affect the admissibility of evidence obtained during the operation. When the legal authority for a proposed surveillance operation is uncertain and circumstances permit, personnel shall consult a supervisor and, when appropriate, the District Attorney or Town Attorney before deployment.

35.20 UAS FLIGHT DOCUMENTATION

Each operational UAS deployment shall be documented. Documentation should include, as applicable:

1. Date and time of deployment;

2. Location;

3. Pilot in Command;

4. Visual Observer, if applicable;

5. Requesting officer or unit;

6. Supervisory authorization;

7. Purpose of deployment;

8. Associated case or incident number;

9. Legal authority for surveillance, when applicable;

10. Search warrant information, when applicable;

11. FAA operating authority, when appropriate;

12. Flight duration;

13. Whether photographs or recordings were obtained;

14. Whether evidence was collected;

15. Any unusual occurrence, accident, loss of control, or equipment malfunction;

16. Any additional information required by FAA regulations or Department procedures.

35.21 QUARTERLY READINESS INSPECTIONS

The UAS Program Coordinator shall ensure that each Department UAS and associated mission-essential equipment receives a documented readiness inspection at least quarterly.

The inspection shall include, as applicable:

1. Aircraft condition;

2. Batteries;

3. Propellers;

4. Controllers;

5. Communications equipment;

6. Firmware and software status;

7. Remote Identification functionality;

8. Safety equipment; and

9. Other mission-essential components.

Identified deficiencies and corrective actions shall be documented.

Equipment presenting a safety concern shall be removed from operational service until the deficiency has been corrected and the equipment has been determined suitable for return to service.

35.22 UAS ACCIDENTS, INCIDENTS, AND MALFUNCTIONS

A. Any UAS accident, collision, loss of aircraft, flyaway, significant equipment malfunction, injury, or property damage shall be immediately reported to a supervisor and the UAS Program Coordinator.

B. The aircraft and associated equipment shall be removed from operational service when necessary, until inspected and determined safe for continued operation.

C. Reasonable steps shall be taken to protect Department data, memory devices, system credentials, and evidence contained on a lost, damaged or inaccessible aircraft.

D. The UAS Program Coordinator shall ensure that any notification or reporting required by the FAA or other governmental authority is completed.

35.23 UAS TRAINING AND PROFICIENCY

A. UAS pilots shall maintain all certifications and qualifications required by the Department and applicable federal law.

B. The Department should establish minimum recurring proficiency requirements for UAS pilots. Training should include:

1. Aircraft operation;

2. Emergency procedures;

3. FAA regulations;

4. North Carolina UAS law;

5. Constitutional search-and-seizure requirements;

6. Department policy;

7. Privacy and civil liberties;

8. Evidence collection and preservation;

9. Night operations when applicable;

10. Airspace requirements;

11. Crew resource management; and

12. Scenario-based operational training.

C. Training and proficiency flights shall be documented and records shall be maintained by the UAS Program Coordinator.

D. All initial, recurrent, proficiency, and specialized training associated with UAS operation shall be documented and maintained in the Department's official training records system in accordance with the Department's Training Policy and applicable NCLEA requirements.

35.24 SURVEILLANCE TECHNOLOGY DATA SECURITY

A. Surveillance information shall be maintained only on Department-approved systems.

B. Access shall be restricted according to job responsibilities and operational need.

C. Where technologically available, systems shall maintain audit logs documenting user access and activity.

D. Employees shall not:

1. Share system credentials;

2. Store surveillance data on personal devices;

3. Transmit surveillance information through unauthorized communication systems;

4. Download information without an authorized purpose; or

5. Attempt to defeat system security or audit functions.

E. Access privileges shall be promptly modified or terminated when an employee changes assignments, separates from employment, or no longer requires access.

F. Software, firmware, and security updates should be maintained in accordance with Department information-technology procedures and operational requirements.

35.25 SUPERVISORY RESPONSIBILITY AND ACCOUNTABILITY

A. Supervisors shall take reasonable steps to ensure surveillance technology is used in accordance with all applicable state and federal law and Department policy. Supervisory responsibilities include:

1. Reviewing requests for surveillance deployments when required;
2. Ensuring appropriate legal authority exists;
3. Reviewing suspected misuse;
4. Ensuring required documentation is completed;
5. Addressing identified training deficiencies; and
6. Referring potential policy violations for appropriate administrative investigation.

35.26 ACCOUNTABILITY AND MISUSE

A. Employees shall immediately report known or suspected unauthorized access, use, preservation, or disclosure of surveillance information. Suspected misuse shall be investigated in accordance with Department policy.

B. Employees who violate this policy may be subject to disciplinary action up to and including termination and may also be subject to applicable civil or criminal penalties. Nothing in this section limits any criminal penalty established by North Carolina law for the unlawful obtaining, accessing, preserving, or disclosure of ALPR information.

35.27 COMPLAINTS

A. Complaints alleging misuse of Department surveillance technology shall be accepted and investigated in accordance with Department complaint and internal-investigation procedures.

B. Complaints involving possible unauthorized access to or disclosure of ALPR information shall be promptly reviewed for potential violations of North Carolina law.

35.28 PROGRAM ADMINISTRATION

A. The Chief of Police shall designate a Surveillance Technology Program Coordinator, or separate ALPR and UAS Program Coordinators.

B. Program responsibilities shall include, as applicable:

1. Maintaining lists of authorized users;
2. Managing access permissions;
3. Coordinating initial and recurring training;
4. Maintaining ALPR maintenance and calibration records;
5. Conducting or coordinating ALPR audits;
6. Reviewing ALPR information-sharing practices;
7. Maintaining UAS aircraft and equipment records;
8. Maintaining UAS flight and training records;
9. Monitoring pilot certifications and proficiency;
10. Monitoring compliance with applicable FAA requirements;
11. Coordinating equipment maintenance;
12. Reviewing reported accidents, malfunctions, and misuse;
13. Evaluating vendor security and data practices;
14. Reviewing system effectiveness; and
15. Recommending policy revisions to the Chief of Police.

35.29 ACQUISITION OR EXPANSION OF SURVEILLANCE TECHNOLOGY

A. Before acquiring a new surveillance technology or substantially expanding the capabilities or use of an existing technology, the Department should evaluate:

1. The legitimate operational need for the technology;
2. Legal authority governing its use;
3. Constitutional implications;
4. Privacy and civil-liberty concerns;
5. Information collected by the technology;

6. Data ownership;

7. Data retention;

8. Access controls;

9. Vendor access to Department information;

10. Data sharing with third parties;

11. Cybersecurity protections;

12. Audit capabilities;

13. Training requirements;

14. Costs and continuing contractual obligations; and

15. Appropriate supervisory oversight.

B. New features involving facial recognition, biometric identification, artificial intelligence, automated tracking, predictive analytics, association analysis, or other materially expanded surveillance capabilities shall not be considered authorized merely because the feature becomes available through an existing vendor or system. Such capabilities shall undergo legal, operational, privacy and command review before deployment.

35.30 ANNUAL PROGRAM AND POLICY REVIEW

The Surveillance Technology Program Coordinator shall review this policy at least annually and/or whenever there is a significant change in applicable law, technology, FAA regulation, vendor capability, or Department operations. Recommended revisions shall be submitted through the chain of command to the Chief of Police for approval and implementation.

35.31 REFERENCES

A. North Carolina Law

1. N.C.G.S. Chapter 20, Article 3D — Automatic License Plate Reader Systems (§§20-183.30 through 20-183.33)
2. N.C.G.S. Chapter 15A, Article 16B — Use of Unmanned Aircraft Systems (§§15A-300.1 through 15A-300.4)

B. Federal Aviation Administration Regulations

1. 14 CFR Part 107 — Small Unmanned Aircraft Systems
2. Applicable FAA Certificates of Waiver or Authorization
3. Applicable FAA airspace authorizations and operational requirements

C. NCLEA Standards

1.11 — Bias-Free Policing
1.13 — Complaints
2.04 — Training Records
6.03 — Search Warrants / Warrantless Searches / Search and Seizure
6.04 — Preliminary Investigations
6.05 — Follow-Up Investigations
6.18 — Special Use Equipment and Vehicles
11.01, 11.03, and 11.04 — Applicable Property and Evidence Requirements

D. Department Policies

Chapter 9 - Training Policy
Chapter 13 - Complaint/Internal Investigation Policy
Chapter 17 – Criminal Investigations
Chapter 19 - Property and Evidence Policy
Chapter 24 - Search and Seizure Policy
Chapter 28 - Records Retention/Records Management Policy