



ALPR Committee Meeting

Wednesday, March 4, 2026, at 3:00 PM

City Council Chambers, City Hall (10 3rd Ave SW)

Any person needing special accommodation for the meeting is requested to notify the City Clerk's office at 857-4752.

1. CALL TO ORDER/ROLL CALL
2. PLEDGE OF ALLEGIANCE
3. COMMITTEE WELCOME & OVERVIEW
4. SYSTEM OVERVIEW & DEMONSTRATION
 - 4.1. SYSTEM OVERVIEW & DEMONSTRATION
5. POLICY REVIEW
 - 5.1. AXON LPR POLICY FOR MINOT POLICE DEPARTMENT
6. DATA SUMMARY & SEARCHES PERFORMED COMMITTEE EXPECTATIONS
7. COMMITTEE DISCUSSION
 - 7.1. POTENTIAL CITY COUNCIL RECOMMENDATIONS
8. ADJOURNMENT

Question

WHAT IS AXON FLEET 3?



Answer

- Fleet 3 is an in-vehicle recording system used by law enforcement
- It captures video and license plate reads from patrol vehicles

Question

WHAT ARE COMMON
MISCONCEPTIONS ABOUT
AXON FLEET 3?



Answer

- It is NOT facial recognition
- It is NOT tracking people in real-time
- It is NOT biometric surveillance

Question

HOW DOES THE ALPR
SYSTEM WORK?



Answer

- Fleet 3 scans license plates that pass in front of the camera
- Reads are compared only to hotlists
- If a match occurs, an alert is sent to the officer for verification
- No hotlist = no alert

Question

HOW DO HOTLIST ALERTS
WORK?



Answer

- Alerts come only from hotlist matches
- Officers verify alerts before taking action

Question

WHAT TYPES OF CRIMES
ARE ON THE HOTLIST(S)?



Answer

- ARSON
- BANK ROBBERY
- CHILD ABDUCTOR
- FELONY WARRANT
- GANG OR SUSPECTED TERRORIST
- THREATS TO LAW ENFORCEMENT
- ARMED ROBBERY
- BOLO
- NARCOTICS
- SILVER ALERT
- FELONY THEFT
- AGGRAVATED ASSAULT
- FUGITIVE
- HOMICIDE
- MISSING PERSON
- ROBBERY
- SEX OFFENSE
- AMBER ALERT
- FELONY VEHICLE
- KIDNAPPING
- STALKING
- STOLEN VEHICLE
- THREAT TO KILL
- TERRORIST

Question

WHAT INTEL DATA IS
COLLECTED?



Answer

- License plate image
- Context image of the vehicle
- Plate number, date, time, and location the scan took place
- Inferred vehicle details (make, color, type)

Question

WHAT INTEL DATA IS NOT COLLECTED?



Answer

- No names or personal identity information
- No registration or DMV lookups
- No linkage to outside databases

Question

DOES THE INTEL DATA GET SHARED?



Answer

NO!

- Data stays in Minot's secure environment
- Evidence is shared only when Minot PD initiates it
- Axon cannot access or distribute data independently

Question

WHO CONTROLS THE INTEL
DATA?



Answer

- Minot Police Department controls all the ALPR (Automated License Plate Reader) data
- Axon does not own, or share any of Minot's data

Question

IS THE INTEL DATA LINKED
TO AN IDENTITY/PERSON?



Answer

- Fleet 3 is not tied to personal identity or registration
- No lookups or database comparisons are performed

Question

WHO CAN ACCESS THE
INTEL DATA?



Answer

- Only authorized users can access the system
- Historical searches require a reason, and approval by Chief or Deputy Chief
- All access, searches, and actions are logged and auditable

Question

HOW LONG IS THE INTEL
DATA STORED FOR?



Answer

- Minot PD sets retention periods for reads and hits
- Proposed retention period: 10 days
- Data is automatically deleted when retention expires

Question

HOW IS THE INTEL DATA
SECURED?



Answer

- Data stored in U.S.-based Microsoft Azure data centers
- Encrypted in transit and at rest
- Protected by firewalls, intrusion detection, and audits

Question

IS THERE ANY OVERSIGHT?



Answer

- CJIS Security Addendum compliant
- Independently audited security controls (SOC 2, ISO 27001)
- Regular penetration testing and monitoring
- Multi layered internal department process
- Oversight committee

Question

IS THIS TRACKING PEOPLE
IN REAL TIME?



Answer

- Fleet 3 does NOT track people in real time
- It reads license plates only when they pass the camera
- Alerts are triggered only by hotlist matches

Question

WHAT BOUNDARIES DOES
THE SYSTEM HAVE?



Answer

- Hotlist-based only; no general surveillance
- Does not perform person tracking, gait analysis, or facial recognition
- Does not connect to external databases or share data outside Minot without direction

Automated License Plate Readers (ALPR)

433.1 PURPOSE AND SCOPE

Automated License Plate Reader (ALPR) technology, also known as License Plate Recognition, provides automated detection of license plates. The ALPR is used by the Minot Police Department to convert data associated with vehicle license plates and use it for official law enforcement purposes. The ALPR may also be used to gather information related to active warrants, homeland security, suspect interdiction and stolen property recovery. ALPR technology shall not be used for general surveillance, or intelligence gathering unrelated to specific, documented criminal investigations.

433.2 ADMINISTRATION OF ALPR DATA

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Administration Division Commander. The Administration Division Commander will assign personnel under his/her command to administer the day-to-day operation of the ALPR equipment and data. All ALPR system actions, access and data handling must be logged and included in quarterly privacy audits conducted by the Office of Professional Standards.

433.3 ALPR OPERATION

Use of ALPR is restricted to the purposes outlined below. Department personnel shall not use, or allow others to use, the equipment or database records for any unauthorized purpose.

- a. An ALPR shall only be used for official and legitimate law enforcement business. An ALPR shall not be used for personal or political purposes. The ALPR system shall not be used for the purpose of interfering with individuals engaged in lawful First Amendment activities.
- b. An ALPR may be used in conjunction with any law enforcement operation or official department investigation related to felony level stolen property offenses, narcotics distribution or manufacturing, stolen motor vehicles, missing persons or violent crimes. ALPR data may also be used in any circumstance where there is a justifiable concern for the immediate safety of a person or persons. A minimum of an articulable reasonable suspicion or probable cause is necessary before accessing ALPR data. ALPR data may not be used for pretextual or speculative searches. Each access request must include a case or incident number and justification.
- c. While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas surrounding homicides, shootings and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.
- d. No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.
- e. No ALPR operator may access Criminal Justice Information Sharing (CJIS) data unless otherwise authorized to do so.

Automated License Plate Readers (ALPR)

- f. Upon receipt of an alert and prior to performing a traffic stop, the officer must visually confirm that the scanned plate matches the alert with regard to plate letters, numbers and issuing state. If practicable, the officer should verify an ALPR response through NCIC, CJIS, or local records before taking enforcement action that is based solely upon an ALPR alert.

433.4 ALPR DATA COLLECTION AND RETENTION

All data and images gathered by ALPR are for the official use of the Minot Police Department. Because such data may contain confidential information, it is not open to public review. The ALPR information gathered and retained by this department may be used and shared with prosecutors or others only as permitted by law.

The Administration Division Commander is responsible to ensure proper collection and retention of ALPR data. All ALPR data not linked to an active criminal investigation shall automatically be deleted after 30 days. No extension of this is permitted unless authorized in writing by the Administration Division Commander with documentation of the associated case number.

All ALPR data downloaded to the server should be stored for the period identified in the department records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

433.5 ACCOUNTABILITY AND SAFEGUARDS

All saved data will be closely safeguarded and protected by both procedural and technological means. The Minot Police Department will observe the following safeguards regarding access to and use of stored data:

- a. All non-law enforcement requests for access to stored ALPR data shall be referred to the Records Sergeant and processed in accordance with applicable law.
- b. All ALPR data downloaded to the mobile work station and server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time. All searches must be tied to a specific, documented case number, and personnel must enter a reason for access before querying the system. Unauthorized searches are strictly prohibited.
- c. Persons approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only and must enter a case number and written justification for each access request. Speculative searches are prohibited.
- d. ALPR data may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes, consistent with applicable law.
- e. ALPR system audits shall be conducted every 30 days by the department's Office of Professional Standards. The purpose of the audit will be to determine the number of searches and to determine if the searches were conducted within the policy of the department. A total review of usage will be conducted quarterly by the finance department.

Automated License Plate Readers (ALPR)

- f. Any persons accessing ALPR data outside the scope indicated above shall be subject to disciplinary action.
- g. Supervisor notification is required and shall be made prior to any search request. Hot sheet entries shall be made by a supervisor or require supervisor approval at a minimum.

433.6 COMMUNITY OVERSIGHT (OPTIONAL)

An appointed oversight board or privacy advisory committee shall review ALPR policy and audit reports annually to ensure alignment with community values and legal standards.

ALPR POLICY: QUICK REFERENCE GUIDE

Minot Police Department | Policy 433

I. Operational Workflow

Prior to Enforcement Action:

- **Visual Confirmation:** Manually verify that the physical plate (alphanumerics and state) matches the ALPR alert.
- **Secondary Verification:** Cross-check the alert via **NCIC, CJIS, or local records** whenever practicable.
- **Restriction:** Enforcement action must **not** be based solely on an unverified ALPR alert.

II. Data Access & Accountability

- **Supervisor Notification:** Required *prior* to any system search.
- **Strict Access:** Credentials-based login; speculative or unauthorized searches are prohibited.
- **Documentation:** Every query must be accompanied by a **specific case number** and a **written justification**.
- **Discipline:** Accessing data outside these parameters is grounds for disciplinary action.

III. Retention & Deletion

- ¹⁰~~30~~-**Day Purge:** All data not linked to an active criminal investigation is automatically deleted after ¹⁰~~30~~ days.
- **Extension:** Requires **written authorization** from the Administration Division Commander.
- **Evidence Handling:** Data needed for criminal or civil actions must be downloaded to portable media and booked into evidence.

IV. Oversight Schedule

Interval	Stakeholder	Task
Every 30 Days	Office of Professional Standards	Conduct system audits for policy compliance.
Quarterly	Finance Department	Perform total review of system usage.
Annually	ALPR Committee	Review policy and audit reports for community alignment.

ALPR Operational & Data Checklist

Officer Response & Enforcement

- ☐ **Visual Confirmation:** Have you manually verified that the scanned plate (letters, numbers, and state) matches the alert?
- ☐ **Secondary Verification:** If practicable, have you verified the hit through NCIC, CJIS, or local records?
- ☐ **Action Basis:** Ensure enforcement action is not based *solely* on an unverified ALPR alert.

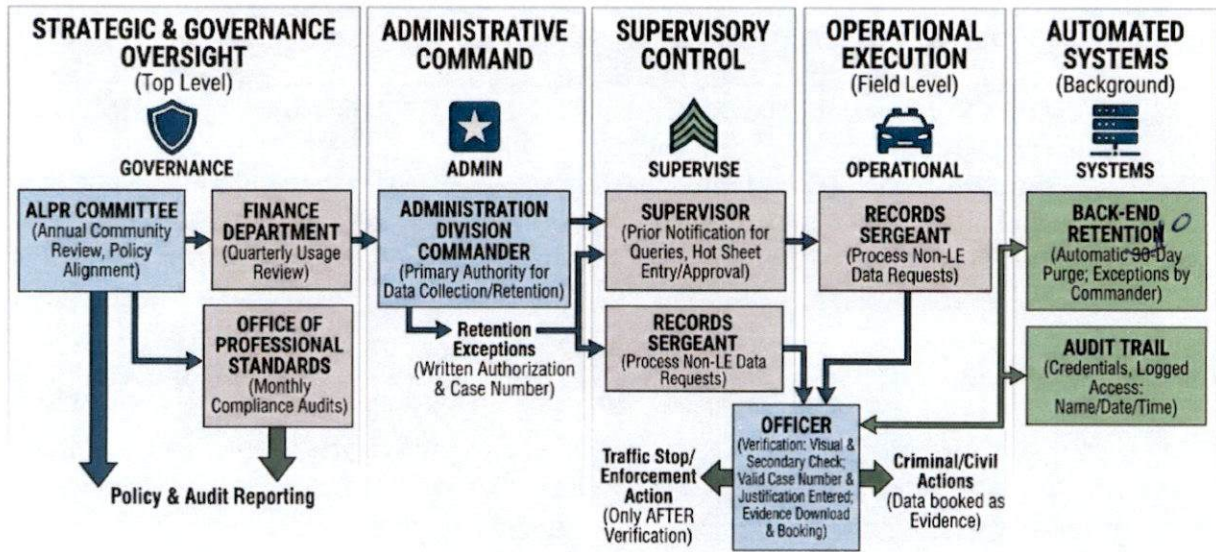
Data Access & Queries

- ☐ **Supervisor Notification:** Has a supervisor been notified prior to the search request?
- ☐ **Authorization:** Is the access for a legitimate law enforcement purpose? (Speculative searches are prohibited).
- ☐ **Documentation:** Have you entered the specific, documented **Case Number**?
- ☐ **Justification:** Have you entered a written reason for the access in the system?
- ☐ **Hot Sheets:** Ensure entries are made or approved by a supervisor.

Retention & Safeguards

- ☒ ¹⁰**30-Day Purge:** Confirm data not linked to an active investigation is deleted after 30 days.
- ☐ **Extension Authorization:** If extending retention, do you have written authorization and a case number from the Administration Division Commander?
- ☐ **Evidence Transition:** If the data is evidence, has it been downloaded to portable media and booked into evidence?
- ☐ **Audit Compliance:** Ensure all access is logged by name, date, and time for the 30-day Office of Professional Standards audit.

MINOT POLICE DEPARTMENT ALPR OPERATIONAL HIERARCHY & REPORTING



Automated License Plate Readers (ALPR)

433.1 PURPOSE AND SCOPE

Automated License Plate Reader (ALPR) technology, also known as License Plate Recognition, provides automated detection of license plates. The ALPR is used by the Minot Police Department to convert data associated with vehicle license plates and use it for official law enforcement purposes. The ALPR may also be used to gather information related to active warrants, homeland security, suspect interdiction and stolen property recovery. ALPR technology shall not be used for general surveillance, or intelligence gathering unrelated to specific, documented criminal investigations.

433.2 ADMINISTRATION OF ALPR DATA

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Administration Division Commander. The Administration Division Commander will assign personnel under his/her command to administer the day-to-day operation of the ALPR equipment and data. All ALPR system actions, access and data handling must be logged and included in quarterly privacy audits conducted by the Office of Professional Standards.

433.3 ALPR OPERATION

Use of ALPR is restricted to the purposes outlined below. Department personnel shall not use, or allow others to use, the equipment or database records for any unauthorized purpose.

- a. An ALPR shall only be used for official and legitimate law enforcement business. An ALPR shall not be used for personal or political purposes. The ALPR system shall not be used for the purpose of interfering with individuals engaged in lawful First Amendment activities.
- b. An ALPR may be used in conjunction with any law enforcement operation or official department investigation related to felony level stolen property offenses, narcotics distribution or manufacturing, stolen motor vehicles, missing persons or violent crimes. ALPR data may also be used in any circumstance where there is a justifiable concern for the immediate safety of a person or persons. A minimum of an articulable reasonable suspicion or probable cause is necessary before accessing ALPR data. ALPR data may not be used for pretextual or speculative searches. Each access request must include a case or incident number and justification.
- c. While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas surrounding homicides, shootings and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.
- d. No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.
- e. No ALPR operator may access Criminal Justice Information Sharing (CJIS) data unless otherwise authorized to do so.

Automated License Plate Readers (ALPR)

- f. Upon receipt of an alert and prior to performing a traffic stop, the officer must visually confirm that the scanned plate matches the alert with regard to plate letters, numbers and issuing state. If practicable, the officer should verify an ALPR response through NCIC, CJIS, or local records before taking enforcement action that is based solely upon an ALPR alert.

433.4 ALPR DATA COLLECTION AND RETENTION

All data and images gathered by ALPR are for the official use of the Minot Police Department. Because such data may contain confidential information, it is not open to public review. The ALPR information gathered and retained by this department may be used and shared with prosecutors or others only as permitted by law.

The Administration Division Commander is responsible to ensure proper collection and retention of ALPR data. All ALPR data not linked to an active criminal investigation shall automatically be deleted after 30 days. No extension of this is permitted unless authorized in writing by the Administration Division Commander with documentation of the associated case number.

All ALPR data downloaded to the server should be stored for the period identified in the department records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

433.5 ACCOUNTABILITY AND SAFEGUARDS

All saved data will be closely safeguarded and protected by both procedural and technological means. The Minot Police Department will observe the following safeguards regarding access to and use of stored data:

- a. All non-law enforcement requests for access to stored ALPR data shall be referred to the Records Sergeant and processed in accordance with applicable law.
- b. All ALPR data downloaded to the mobile work station and server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time. All searches must be tied to a specific, documented case number, and personnel must enter a reason for access before querying the system. Unauthorized searches are strictly prohibited.
- c. Persons approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only and must enter a case number and written justification for each access request. Speculative searches are prohibited.
- d. ALPR data may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes, consistent with applicable law.
- e. ALPR system audits shall be conducted every 30 days by the department's Office of Professional Standards. The purpose of the audit will be to determine the number of searches and to determine if the searches were conducted within the policy of the department. A total review of usage will be conducted quarterly by the finance department.

Automated License Plate Readers (ALPR)

- f. Any persons accessing ALPR data outside the scope indicated above shall be subject to disciplinary action.
- g. Supervisor notification is required and shall be made prior to any search request. Hot sheet entries shall be made by a supervisor or require supervisor approval at a minimum.

433.6 COMMUNITY OVERSIGHT (OPTIONAL)

An appointed oversight board or privacy advisory committee shall review ALPR policy and audit reports annually to ensure alignment with community values and legal standards.