Axon License Plate Reader Contract

Health and Safety Committee

March 11, 2026

Resolution 26-0246

Contract details

- $150,000
- One year

Request

- Vote to delay to a date certain of March 18th in Health and Safety Committee

Contract Deliverables

- 50 Axon Outpost Cameras - Fixed ALPR camera, deployable on poles, trailers or buildings with solar power.
- Access to Axon Vehicle Intelligence Software Suite

Axon ALPR Protections

- Access limited to Denver Safety personnel
- No national database
- Denver owns and controls its own data
- Highest level data security
- 21-day retention policy
- Access is logged and auditable

Data Security & Privacy

FedRAMP High Cloud Security
All ALPR data is stored on infrastructure with FedRAMP High authorization — the highest level of federal cloud security, requiring compliance with 392 individual security controls.

Encryption at Every Level
AES-256 encrypted on-device storage with FIPS-validated modules. TLS 1.2+ encryption for all data in transit. Data is wiped from cameras after secure upload — a stolen camera contains no retrievable plate data.

Independently Verified Certifications
SOC 2 Type II, ISO 27001/27017/27018/27701, CJIS Security Policy compliant, and zero-trust architecture aligned with CISA and NIST guidelines. All verified by independent third-party auditors.

Evidence.com
Storage system that has been used in Denver for the past decade to store sensitive digital evidence including body-worn camera footage.

Denver Retains Full Control

Denver Owns Its Data

Denver retains complete ownership of all ALPR data. Axon does not pool data into a sharing network and does not sell or resell agency data to any third party.

Invite-Only Sharing & Tamper-Proof Auditing

Data sharing with other agencies is strictly invite-only and fully revocable. Every search, login, and export is recorded in an immutable audit log that cannot be altered or deleted.

Legal Requests & Community Transparency

All warrants, subpoenas, and public records requests are routed to Denver — not the vendor. Axon's public transparency portal gives residents visibility into how the system is used.

ALPR Policy Safeguards

Training Requirement
- Mandatory training required before system use or data access

Public View
- Deployment limited to public roads or vehicles visible from public spaces

Prohibited Uses
- Constitutional rights violations or First Amendment monitoring
- Discriminatory use, harassment, or intimidation
- Parking, traffic, or driver's license enforcement; personal use

Alert Verification Before Action
- ALPR alert alone does not authorize a vehicle stop

ALPR Policy Safeguards

Data Retention & Legal Protections

- Data auto-purged after policy-defined retention periods

Audit Trail & Oversight

- Every access logged: officer, case number, date, time, purpose
- Monthly audits
- Officers under investigation: access immediately suspended

Restricted Data Sharing

- Sharing only in response to law enforcement official investigation
- No sharing for conduct legal under Colorado law
- No sharing to aid prosecution related to reproductive care

Technology Services Update

Vendor Risk Assessment Updates
Enhancements have been made to the Vendor Risk Assessment process, including links and resources to help vendors understand applicable local and federal regulations, as well as best practices.

Contract Governance Improvements
New Breach and Remedy language has been drafted for Technology Services Contracts to strengthen governance and improve enforcement of vendor non-compliance.

Data Equity and Civil Liberties
Technology Services is collaborating with the Mayor's Office of Social Equity and Innovation to develop methods for evaluating vendor data equity and ensuring vendors protect civil liberties through operational and technological safeguards.

Axon LPR Vendor Risk Assessment Outcome

Vendor assessed through Automated Questionnaire & Vendor Trust Center
Completed: 1/30/2026
Status: Approved

Questions

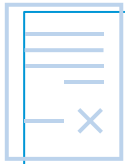
APPENDIX

DPD Technology Acquisition

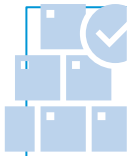
- Cyber Bureau evaluates technology – Works with other agencies, DPD teams, to establish efficacy and impact to operations. Aligned with strategic goals.
- TS Intake Process – Vendor Risk Assessment (VRA), TAR (Technical Architecture Review), etc…
- Competitive Process / Purchasing Rules
- Contracting
- Policy
- Implementation and Sustainment

Vendor Risk Assessments

Identification of risk and potential mitigation



Need for additional requirements such as a data sharing agreement or contract vs. purchase order



Vendor Approval or Denial

Vendor Risk Assessments: AI & Privacy

- CCD Data Lifecycle Overview
- Data Collection
- Data Use
- Data Sharing
- Data Retention
- Data Storage & Security
- Data Archival
- Data Disposal

1. SCOPE & USE

2. RISK & IMPACT

3. GOVERNANCE & OVERSIGHT

DPD Policy Controls

- DPD OMS 119.00 – Operations Technology
- Publicly accessible
- Defines technology objective, appropriate use, data governance, auditing
- Policy created based upon legal review by CAO and review of policies from other law enforcement organizations, agencies, including IACP for best practices.