

RESOLUTION 26-__

A RESOLUTION OF THE GOVERNING BODY OF THE CITY OF ROSWELL, NEW MEXICO, ESTABLISHING A RESPONSIBLE PUBLIC SAFETY TECHNOLOGY GOVERNANCE FRAMEWORK FOR THE ACQUISITION, USE, MANAGEMENT, RETENTION, SHARING, AND OVERSIGHT OF COVERED PUBLIC SAFETY TECHNOLOGIES

WHEREAS, the City of Roswell recognizes that modern public safety technology can improve officer safety, investigative effectiveness, emergency response, and the protection of residents and property; and

WHEREAS, certain public safety technologies are capable of systematically collecting, identifying, locating, tracking, analyzing, retaining, or sharing information concerning identifiable persons, vehicles, movements, associations, or activities; and

WHEREAS, the Governing Body finds that clear and durable standards can support effective law enforcement while providing appropriate safeguards for privacy, civil liberties, data security, accountability, and public trust; and

WHEREAS, the Governing Body further finds that such standards should remain effective notwithstanding changes in elected officials, City personnel, department leadership, technology vendors, or technical capabilities; and

WHEREAS, the Roswell Police Department currently maintains Policy 612 governing Automated License Plate Reader technology, including provisions addressing official law-enforcement use, training, access, data retention, accountability, and interagency sharing; and

WHEREAS, the Governing Body desires to establish City-level governance principles that complement, rather than replace, lawful department-level operational policies and procedures; and

WHEREAS, the Governing Body intends this framework to apply to covered public safety technologies and material expansions of those technologies, while avoiding unnecessary regulation of ordinary information technology, infrastructure systems, and other technologies that do not materially perform surveillance, tracking, identification, or related public-safety data functions.

NOW, THEREFORE, BE IT RESOLVED BY THE GOVERNING BODY OF THE CITY OF ROSWELL, NEW MEXICO, THAT:

SECTION 1. ADOPTION OF GOVERNANCE FRAMEWORK.

The City of Roswell hereby establishes the following principles for covered public safety technology. These principles shall guide City departments in the acquisition, deployment, use, management, contracting, and material expansion of covered technology, subject to applicable law and any more specific policy adopted by the City or responsible department.

SECTION 2. DEFINITION OF COVERED PUBLIC SAFETY TECHNOLOGY.

“Covered Public Safety Technology” means City-owned, City-leased, City-operated, or City-contracted technology whose primary or material function is to systematically collect, identify, locate, track, analyze, correlate, retain, or share information concerning identifiable persons, vehicles, movements, associations, or activities for public-safety or law-enforcement purposes. Covered technology may include Automated License Plate Readers, networked public-safety camera systems, biometric identification systems,

surveillance-capable unmanned aircraft systems, AI-enabled video or image analytics, vehicle tracking or pattern-analysis systems, and future technologies with substantially similar capabilities.

SECTION 3. AUTHORIZED PURPOSE AND USE.

Covered technology shall be acquired and used only for defined, lawful governmental and public-safety purposes. Use for personal, political, discriminatory, retaliatory, commercial, or other unauthorized purposes is prohibited. Technology-specific policies shall identify authorized uses and, where practicable and appropriate, require searches or queries to be associated with a documented authorized purpose.

SECTION 4. DEPLOYMENT AND LOCATION.

For fixed or geographically deployed covered technology, the responsible department shall establish written criteria governing deployment and location, identify the official authorized to approve deployment, document material placement decisions, and provide for periodic review. Technology-specific policies shall address whether heightened review is appropriate for deployment near locations associated with constitutionally protected or particularly sensitive activity, consistent with legitimate public-safety needs.

SECTION 5. DATA COLLECTION AND TECHNICAL CAPABILITIES.

Technology-specific policies shall identify the categories of information authorized for collection and material analytic capabilities authorized for use. A material new surveillance, identification, tracking, analytic, integration, retention, or sharing capability shall not be deemed authorized solely because it becomes technically available through a vendor, software update, equipment replacement, or system integration.

SECTION 6. ACCESS, SEARCHES, AND AUDITING.

Access to covered systems shall be limited to trained personnel with a legitimate operational need. Access permissions shall be role-based where technically feasible, authenticated, and subject to appropriate approval and periodic review. Covered systems shall maintain audit logs sufficient to identify users and material access or search activity to the extent technically available. Technology-specific policies shall establish search-justification requirements, audit frequency, supervisory responsibility, and procedures for addressing confirmed misuse.

SECTION 7. DATA RETENTION AND DELETION.

Each technology-specific policy shall establish a defined retention period or identify the controlling legally adopted records-retention schedule. Routine data shall be deleted upon expiration of the applicable retention period unless preservation is required for an investigation, evidentiary purpose, litigation, discovery, public-record obligation, legal hold, or other lawful reason. Routine deletion should be automated where technically feasible.

SECTION 8. SHARING AND EXTERNAL ACCESS.

Technology-specific policies shall establish the circumstances under which covered data may be shared with another agency or authorized entity; the approval and documentation required; whether standing or direct database access is permitted; restrictions on downstream re-sharing; applicable retention requirements; auditability; and procedures for suspending or revoking access. Sharing shall be for a lawful and authorized governmental purpose.

SECTION 9. CITY CONTROL; PROHIBITION ON SALE OR COMMERCIAL EXPLOITATION.

Data collected by or on behalf of the City through covered public safety technology shall remain subject to City control as provided by applicable law and contract. Neither the City nor a vendor or contractor acting on behalf of the City shall sell, license, monetize, use for advertising, create an unrelated commercial database from, or otherwise commercially exploit City-collected covered data, except where expressly required by law or specifically authorized by the City for a lawful governmental purpose.

SECTION 10. TRANSPARENCY AND ACCOUNTABILITY.

The City shall maintain an inventory of covered public safety technologies. The responsible department shall provide periodic aggregate information appropriate to the technology, which may include the technology's authorized purpose, deployment or use, retention setting, categories of sharing partners, completion of required audits, material policy changes, and confirmed misuse. Nothing in this Resolution requires disclosure of information protected by law or information whose disclosure would reasonably compromise an investigation, officer or public safety, cybersecurity, confidential sources, or legitimate law-enforcement methods.

SECTION 11. REVIEW OF NEW TECHNOLOGY AND MATERIAL CHANGES.

Before acquisition of a new covered public safety technology, or before a material expansion of an existing covered technology, the responsible department shall complete a review process established by the City Manager in consultation with the City Attorney and appropriate Information Technology and departmental personnel. The review should address operational purpose, data collection, access, retention, sharing, security, privacy safeguards, fiscal and contractual considerations, and whether governing-body review is required.

SECTION 12. MATERIAL CHANGE.

For purposes of this Resolution, a material change includes a significant change in purpose, functionality, authorized use, type or scope of data collected, analytic capability, retention, external sharing, integration with another system, or geographic scale. Routine maintenance, security patches, equipment replacement, or technical changes that do not materially expand collection, use, analysis, retention, or sharing do not constitute a material change.

SECTION 13. EMERGENCY OR EXIGENT USE.

Nothing in this Resolution is intended to prevent lawful temporary use of covered technology when reasonably necessary to respond to an emergency, imminent threat to life or safety, significant cybersecurity incident, or other exigent circumstance recognized by law. Such use shall be documented and subsequently reviewed in accordance with procedures established by the City.

SECTION 14. DEPARTMENT-LEVEL POLICIES.

Departments using covered technology shall maintain technology-specific operational policies and procedures consistent with this Resolution. Nothing herein is intended to require public disclosure of confidential investigative methods, security information, or other information protected from disclosure by law.

SECTION 15. AUTOMATED LICENSE PLATE READERS.

Automated License Plate Reader technology shall be the initial technology reviewed under this framework. The City Manager, City Attorney, Chief of Police, and appropriate Information Technology personnel are requested to review RPD Policy 612 and recommend any amendments or supplemental City policy necessary to address camera-placement criteria, authorized data and analytics, access authorization, documented search justification, audit frequency, routine retention and deletion, interagency or standing

access, downstream sharing, City control of data, prohibition on commercial exploitation, and appropriate aggregate reporting.

SECTION 16. IMPLEMENTATION.

The City Manager, in consultation with the City Attorney, Chief of Police (or designee), Information Technology personnel, and other affected department heads, is directed to develop reasonable administrative procedures, technology-review forms, procurement and contract standards, and technology-specific policies necessary to implement this Resolution.

SECTION 17. CONSTRUCTION.

This Resolution establishes City governance principles and is not intended to interfere with lawful law-enforcement discretion, alter evidentiary obligations, require disclosure prohibited by law, or supersede controlling federal or New Mexico law. In the event of a conflict, controlling law shall govern.

SECTION 18. EFFECTIVE DATE.

This Resolution shall become effective upon adoption.

PASSED, ADOPTED, SIGNED, AND APPROVED this ____ day of _____, 2026.

CITY SEAL

ATTEST:

Amalia Martinez, City Clerk

Timothy Z. Jennings, Mayor

WORKING DRAFT — FOR REVIEW BY THE CITY ATTORNEY, CITY MANAGER, POLICE CHIEF, AND GOVERNING BODY