Bend Surveillance Procurement and Contracting Framework

Section 1. Title and Purpose

1.1 Title

This document shall be known as the **Bend Surveillance Procurement and Contracting Framework**.

1.2 Purpose

This Framework is intended to translate City surveillance-governance principles into practical procurement standards, contract requirements, review triggers, renewal conditions, and implementation procedures.

The purpose of this Framework is to help ensure that surveillance-related technologies, services, platforms, datasets, and vendor relationships used by or on behalf of the City of Bend are governed not only by policy goals, but also by enforceable procurement language and contract controls.

This Framework is intended to:

- protect privacy, civil rights, civil liberties, democratic participation, and public trust;
- reduce legal, operational, procurement, cybersecurity, and vendor-dependence risk;
- prevent mission creep through software updates, analytics modules, feature activation, data-source expansion, and contract renewal;
- ensure that data ownership, retention, deletion, key control, vendor access, and audit rights are governed by City requirements rather than vendor defaults;
- provide a repeatable process for procurement, renewal, continuation, review, and transition; and
- complement any applicable City ordinance, City policy, departmental use policy, or state or federal law.

Section 2. Executive Summary

Modern surveillance systems are rarely static. They are often cloud-hosted, remotely updated, modular, subscription-based, and capable of expanding through analytics, AI functions, integrations, vendor support arrangements, and data-sharing pathways after the initial procurement is complete.

For that reason, surveillance governance does not live only in ordinances or department policies. It also lives in vendor contracts, renewal language, hosting arrangements, feature-activation rules, subcontractor terms, retention settings, audit rights, and the practical conditions under which a vendor may access or alter the system.

This Framework is intended to help the City of Bend govern those issues consistently.

It provides:

- core procurement principles,
- mandatory baseline contract terms,
- stronger terms for high-risk technologies,
- technology-specific addenda,
- review triggers for renewals, extensions, and material changes,
- vendor compliance-certification requirements,
- City compliance-review procedures,
- a legacy contract transition framework, and
- implementation tools.

This Framework is intended to complement broader surveillance ordinance language and department policy by ensuring that the City's public-policy goals are reflected in the actual contracts and procurement processes that govern surveillance systems in practice.

Section 3. Core Procurement Principles

3.1 Necessity and Proportionality

The City should procure surveillance technology only where there is a clearly defined, lawful, and documented public purpose, and where the anticipated use is proportionate to that purpose. Procurement should not proceed where a less intrusive reasonable alternative is available and sufficient.

3.2 Public Accountability

Surveillance-related procurement should reflect City policy, Council direction, and public accountability. The acquisition, renewal, expansion, or material modification of surveillance technology should not be governed solely by vendor offerings, default system settings, or informal operational practice.

3.3 Data Minimization

Contracts and procurement documents should require the minimum collection, retention, processing, sharing, and exposure of data necessary to carry out the approved purpose. Where non-evidentiary or non-actionable data can be avoided, shortened, or promptly deleted, the City should require that result.

3.4 City Control Over Data and System Expansion

The City should maintain meaningful control over surveillance data, system settings, approved purposes, enabled capabilities, retention periods, sharing arrangements, and future expansion. No vendor should be permitted to determine or materially alter these matters unilaterally.

3.5 No Silent Feature Expansion

No surveillance-related capability should be materially expanded through software updates, feature flags, analytics modules, integrations, configuration changes, or hosted-service enhancements without prior City review and any approval required by City policy or law.

3.6 Security by Contract

Privacy, cybersecurity, auditability, deletion, vendor-access limits, and system-accountability requirements should be embedded directly into contracts and related procurement documents. Core safeguards should not depend solely on vendor marketing statements, default settings, or informal assurances.

3.7 No Vendor Secondary Use

City surveillance data should not be used by vendors or their subcontractors for unrelated internal business purposes, product development, analytics improvement, benchmarking, artificial-intelligence training, commercialization, or any other purpose beyond the approved contracted service.

3.8 Renewal Conditioned on Compliance

No covered surveillance contract, subscription, amendment, extension, optional continuation, feature activation, or material expansion should proceed unless the vendor and the City program are in compliance with applicable City requirements, contract terms, and approved use limitations.

3.9 Technology-Neutral Governance

The City's surveillance procurement framework should be interpreted broadly enough to govern current and emerging technologies, including tools that are fixed, mobile, wearable, aerial, cloud-hosted, software-defined, or later expanded through analytics or artificial-intelligence modules.

3.10 Protection of Civil Rights and Civil Liberties

Surveillance procurement should reflect the City's interest in protecting privacy, civil rights, civil liberties, democratic participation, and public trust. Contracts should not enable or normalize unnecessary monitoring of law-abiding residents, protected activity, or sensitive locations.

Section 4. Scope and Applicability

This Framework applies to surveillance-related procurements, agreements, services, and operational arrangements, including purchases, subscriptions, software licenses, SaaS agreements, hosting agreements, cloud-service agreements, support agreements, pilot agreements, trial agreements, statements of work, renewals, extensions, amendments, addenda, optional continuations, feature activations, integrations, data-sharing arrangements, and other procurement instruments involving covered surveillance functions.

This Framework applies whether a covered surveillance-related system or service is City-owned, vendor-owned, leased, borrowed, donated, accessed by subscription, cloud-hosted, vendor-operated, integrated into another platform, or made available through a third party on behalf of the City.

No vendor, department, contractor, or operational arrangement should be treated as outside this Framework merely because the technology is described as a service rather than a system, a pilot rather than a deployment, an upgrade rather than an expansion, or a dataset rather than a surveillance technology. If the substance of the procurement falls within this Framework, the Framework applies.

Section 5. Technology Classification Structure

Each covered procurement should be classified as either a baseline surveillance procurement or a high-risk surveillance procurement.

A procurement should be treated as high-risk where it materially involves one or more of the following:

- Historical Location Information;
- biometric or characteristic-based identification or inference;
- signal intelligence or device-identifier capture;
- mass public-space monitoring;
- pattern-of-life, reverse-search, or inferential analytics;
- cross-system or cross-dataset correlation;
- hosted law-enforcement or investigative workflows involving sensitive City data; or
- commercial surveillance data.

A covered procurement may be subject to more than one technology-specific addendum. Where more than one addendum applies, all applicable addenda should be reviewed and incorporated, and the more protective requirement should govern unless controlling law requires otherwise.

Section 6. Mandatory Baseline Contract Terms

Every covered surveillance-related contract, agreement, subscription, statement of work, amendment, addendum, renewal, extension, feature activation, or related procurement instrument should include, at a minimum, terms substantially similar to the following.

6.1 Definitions

The contract should define all key terms necessary to ensure clarity and enforceability, including, as applicable: Surveillance Technology, Surveillance Data, City Data, Approved Purpose, Material Change, Vendor Personnel, Subcontractor, Security Incident, Breach, Decrypted Data, Derived Data, Audit Log, Deletion Certification, and Exclusive Agency Key Control.

6.2 Compliance with City Law, Policy, and Approved Use

The vendor shall comply with all applicable City ordinances, approved City policies, procurement requirements, and use limitations governing the technology or service. The contract shall specify that vendor obligations apply not only at contract execution, but also upon renewal, extension, amendment, feature activation, and Material Change.

6.3 City Ownership and Control of City Data

The contract shall state that all City-generated or City-collected surveillance data, associated logs, configurations created for City operations, retention records, deletion records, exports, and related operational records are the property of the City. Vendor ownership of proprietary software, platforms, or systems shall not diminish or override City ownership and control of City data.

6.4 Purpose Limitation

The vendor may collect, host, process, access, transmit, store, or otherwise handle City data only to the extent necessary to provide the specific approved service described in the contract. Any use outside that scope is prohibited unless expressly authorized in writing by the City and permitted by applicable law and policy.

6.5 Prohibition on Vendor Secondary Use

The contract shall prohibit the vendor and all subcontractors from using City data, or any derivative, de-identified, aggregated, pseudonymized, sample, or test version of City data, for

product development, service improvement unrelated to the contracted service, benchmarking, analytics improvement, internal business intelligence, model or algorithm training, artificial-intelligence development, commercialization, marketing, resale, or unrelated research.

6.6 No Sale, Disclosure, or Unauthorized Sharing

The vendor shall not sell, license, disclose, transfer, rent, trade, monetize, or otherwise make City data available to any third party except as expressly required to perform the contracted service and expressly authorized by the City in writing.

6.7 Subcontractor Disclosure and Control

The contract shall require advance written disclosure of all subcontractors with access to City data or material system functions, City approval for material subcontractors, written flow-down of all applicable contract restrictions to subcontractors, and advance written notice before any material change in subcontractor relationships.

6.8 Hosting, Storage, and Processing Transparency

The vendor shall disclose where City data is hosted, stored, processed, replicated, and backed up, including all relevant service providers and jurisdictions, and shall provide advance written notice of any material change in hosting provider, hosting architecture, storage region, backup arrangement, or processing environment affecting City data.

6.9 Encryption and Security Controls

The contract shall require contemporary industry-standard encryption for City data in transit and at rest, along with authentication, access controls, logging, account management, incident response, and administrative-security practices appropriate to the sensitivity of the system. Vendor-managed encryption alone shall not be deemed sufficient where the vendor or its personnel can independently decrypt covered City data.

6.10 Exclusive Agency Key Control

For any covered surveillance technology designated by the City as requiring heightened data-control protections, and for any high-risk surveillance technology that stores covered sensitive City data, the contract shall require Exclusive Agency Key Control, or functionally equivalent City-controlled safeguards sufficient to prevent routine vendor access to plaintext City data and unilateral vendor decryption capability.

The contract shall further require that:

- only the City, or where applicable the Bend Police Department through agency-controlled identity and access systems and agency-controlled cryptographic key management, may authorize routine access to decrypted stored data;
- vendor personnel, subcontractors, and support staff shall have no routine ability to view covered data in plaintext;
- the vendor shall disclose in writing whether any function of the service requires access to decrypted data, when such access occurs, what personnel or subprocessors may obtain such access, and what technical and contractual controls limit that access;
- any exceptional vendor access to decrypted data must require prior written City authorization, be narrowly limited, logged, monitored, and auditable; and
- the City shall retain the right to audit key-management practices and to rotate, suspend, revoke, and replace keys or equivalent controls without vendor interference, subject only to technical limitations disclosed in writing before contract execution.

6.11 Access Control and Named Users

The vendor shall support role-based access, least-privilege configuration, named user accounts, and administrative segregation where applicable.

6.12 Vendor Personnel Access Restrictions

Vendor personnel access to City data shall be limited to the minimum necessary to provide contracted support or maintenance. Such access shall be time-limited, documented, logged, and subject to City authorization where required by City policy or contract.

6.13 Retention, Deletion, and Deletion Certification

The contract shall specify applicable retention periods, automatic deletion requirements where applicable, deletion upon contract termination or expiration, deletion from backups, replicas, caches, and derived indexes to the extent technically feasible, and written deletion certification upon request and at contract end.

6.14 Audit Logs and Record Preservation

The vendor shall maintain and preserve audit logs and related compliance records sufficient to document system access, administrative actions, exports, sharing events, deletion activity, support sessions, key-access events, requests for exceptional access, and material configuration changes affecting City operations.

6.15 City Audit and Verification Rights

The contract shall grant the City reasonable rights to inspect, review, or obtain documentation sufficient to verify compliance with contract terms relating to data handling, retention, deletion,

access, logging, subcontractors, key-management practices, requests for exceptional access, and material feature changes.

6.16 Security Incident and Breach Notification

The contract shall require prompt notice to the City of any actual or suspected breach, unauthorized access, unauthorized disclosure, improper vendor access, material configuration failure, integrity failure, accidental activation of unapproved capabilities, or loss or compromise of encryption-key or equivalent access-control protections affecting City data or City operations.

6.17 Change Management and Material Changes

The vendor shall provide advance written notice and obtain any required City approval before implementing a Material Change, including but not limited to new analytics features, AI or model-based features, integrations with other platforms or data sources, changes to retention behavior, changes to administrative-access pathways, new sharing features, new search capabilities, hosting or architectural changes affecting control, access, visibility, or plaintext exposure, or any change affecting key management, decryption pathways, or vendor visibility into covered data.

6.18 Public Records, Preservation, and Export Cooperation

The vendor shall reasonably assist the City in responding to public-records requests, litigation holds, preservation obligations, discovery obligations, and lawful export needs. The contract shall require the vendor to provide City data in a usable and reasonably accessible format upon request or at termination.

6.19 Termination and Transition Assistance

Upon contract termination, expiration, or nonrenewal, the vendor shall provide reasonable transition assistance, including data export, preservation of necessary logs during transition, orderly migration support where applicable, and timely deletion after transfer is complete.

6.20 Remedies for Noncompliance

The contract shall provide the City with enforceable remedies for vendor noncompliance, including notice and cure requirements, suspension of access or use, withholding of payment, termination for cause, preservation of records, and disqualification from future procurement where lawfully permitted.

6.21 Renewal, Extension, Amendment, and Feature Activation Conditions

The contract shall state that renewal, extension, amendment, optional continuation, feature activation, integration, or other material operational continuation is conditioned on continued

compliance with City requirements, approved use limitations, and all applicable contract safeguards.

Section 7. Enhanced Terms for High-Risk Surveillance Technologies

Enhanced terms shall apply to any covered technology that is capable of:

- generating, storing, or enabling access to Historical Location Information;
- identifying, tracking, or correlating persons, vehicles, devices, or groups over time or at scale;
- capturing or analyzing biometric or characteristic-based information;
- collecting or analyzing wireless signals, electronic-device identifiers, or communications-related signaling data;
- aggregating multiple surveillance or investigative data sources into a single searchable or analytic platform;
- enabling reverse searches, geofencing, pattern-of-life analysis, co-traveler analysis, associate analysis, or similar retrospective or inferential searches;
- performing AI-assisted, predictive, inferential, anomaly-detection, or automated risk-scoring functions; or
- supporting cloud-hosted or vendor-hosted investigative workflows involving sensitive City data.

Where a covered technology qualifies as high-risk, the contract shall be written and interpreted in favor of stricter retention, stricter access control, narrower vendor rights, more detailed auditability, greater City control over feature activation and system changes, and stronger conditions for renewal and continued use.

Contracts for High-Risk Surveillance Technologies should include:

- heightened review before procurement or renewal;
- heightened retention controls, especially for non-evidentiary and non-actionable data;
- heightened vendor-access restrictions;
- heightened logging requirements;
- heightened audit rights;
- restrictions on latent, optional, or future capabilities;
- restrictions on investigative and search expansion;
- heightened notice of changes;
- public reporting support; and
- heightened renewal conditions.

Section 8. Technology-Specific Addenda

Addendum A. ALPR and Vehicle-Location Systems

This addendum applies to ALPR and related vehicle-location systems, hosted ALPR platforms, ALPR analytics/search tools/sharing networks, and any module or integration that expands ALPR into broader tracking or pattern-of-life functionality.

Core contract requirements include:

- narrow purpose limitation;
- disclosure of all captured data categories;
- a hard retention period for non-hit, non-flagged, non-evidentiary data;
- no speculative historical bulk retention;
- support for historical search controls;
- documented hot-list and alert controls;
- sharing restrictions and control over participation in external networks;
- no commercial enrichment or outside data fusion without approval;
- no secondary use, AI training, or product development using City ALPR data;
- Exclusive Agency Key Control where designated;
- vendor access restrictions;
- search and query logging;
- administrative and configuration logging;
- export and download controls;
- deletion certification;
- reporting support; and
- renewal, continuation, transition, and more-protective-rule clauses.

Addendum B. Automated Traffic Enforcement Systems

This addendum applies to red-light and speed-enforcement systems, vendor back-office platforms, image-review workflows, mailing/citation workflows, and related analytics or dashboards.

Core contract requirements include:

- purpose limitation;
- full disclosure of data categories and system functions;
- clear City ownership of City data notwithstanding vendor ownership of proprietary BOS software;
- no vendor secondary use;
- separate retention rules for violation and non-violation data;
- review workflow transparency;
- disclosure of registered-owner lookup pathways;
- vendor access restrictions;
- remote access and support controls;
- encryption and key-control requirements where designated;

- no silent feature expansion;
- configuration and workflow logging;
- audit logs and oversight records;
- public-records and evidentiary cooperation;
- no fee escalation triggered solely by City privacy safeguards;
- transition and exit support;
- renewal and continuation conditions; and
- a more-protective-rule clause.

Addendum C. Fixed Security Camera Systems

This addendum applies to fixed security camera systems, cloud-hosted video management systems, related storage/retrieval/export tools, and modules that expand a camera system into broader analytics or tracking.

Core contract requirements include:

- purpose limitation;
- specific disclosure of data categories and system functions;
- camera placement and scope controls;
- no audio by default;
- no analytics by default;
- retention and deletion requirements;
- sensitive-location protections;
- live monitoring and playback controls;
- vendor access restrictions;
- remote access and administrative support controls;
- encryption and key-control requirements where designated;
- no silent feature expansion;
- configuration and workflow logging;
- audit logs and oversight records;
- export, sharing, and external access controls;
- public-records and legal-compliance support;
- deletion certification;
- renewal and continuation conditions;
- transition and exit support; and
- a more-protective-rule clause.

Addendum D. Drones / UAS

This addendum applies to drones/UAS, related command and control software, cloud-hosted UAS data platforms, drone analytics, and any module or integration that materially expands a UAS program.

Core contract requirements include:

- purpose limitation consistent with City policy and law;
- specific disclosure of data categories and system functions;
- mission-type disclosure and limits;
- privacy-by-design and exclusion controls;
- thermal/infrared/vision-enhancement controls;
- no analytics by default;
- no weaponization or interference features;
- third-party storage and cloud-hosting disclosure;
- vendor access restrictions;
- remote access and support controls;
- encryption and key-control requirements where designated;
- no silent feature expansion;
- flight, mission, and review logging;
- evidence integrity and chain-of-custody support;
- retention and deletion requirements;
- intergovernmental sharing and disclosure controls;
- public notification and reporting support;
- renewal and continuation conditions;
- transition and exit support; and
- a more-protective-rule clause.

Addendum E. Signal Intelligence and Cell-Site Simulator Systems

This addendum applies to cell-site simulators, IMSI-catcher or Stingray-type systems, wireless identifier capture systems, Bluetooth/Wi-Fi/RFID tracking systems, signal-analysis platforms, and related modules or integrations.

Core contract requirements include:

- purpose limitation;
- disclosure of all data categories and system functions;
- warrant-support architecture;
- target/non-target distinction;
- non-target minimization and deletion;
- no reverse or dragnet searches by default;
- no device-to-person or device-to-vehicle cataloging by default;
- no commercial enrichment or external data fusion;
- no secondary use, AI training, or product development;
- Exclusive Agency Key Control where designated;
- vendor access restrictions;
- remote access and support controls;
- search, collection, and mission logging;
- administrative and configuration logging;

- retention and deletion requirements;
- export and sharing controls;
- public-records, legal-compliance, and oversight support;
- renewal and continuation conditions;
- transition and exit support; and
- a more-protective-rule clause.

Addendum F. Data-Fusion and Real-Time Crime Center Platforms

This addendum applies to platforms that aggregate multiple surveillance or investigative data sources into a single interface, including RTCC dashboards, search/correlation platforms, event-monitoring systems, and analytics engines.

Core contract requirements include:

- purpose limitation;
- source-by-source disclosure and source-specific approval control;
- no hidden ingestion;
- disclosure of all categories of data and outputs;
- no analytics by default;
- no automated enforcement basis;
- sensitive-location and protected-activity restrictions;
- no cross-dataset profiling by default;
- no commercial enrichment or outside data fusion by default;
- no secondary use, AI training, or product development;
- access control and role separation;
- vendor access restrictions;
- remote access and support controls;
- encryption and key-control requirements where designated;
- query and search logging;
- administrative and configuration logging;
- data retention and derived-output controls;
- public-records, legal-compliance, and oversight support;
- reporting support;
- renewal and continuation conditions;
- transition and exit support; and
- a more-protective-rule clause.

Addendum G. Biometric and Video Analytics Systems

This addendum applies to facial recognition, person re-identification, gait recognition, voiceprint systems, demographic inference, emotion recognition, anomaly detection directed at individuals or groups, cross-camera tracking, and related advanced analytics.

Core contract requirements include:

- prohibition absent express authorization;
- disclosure of all covered functions;
- disabled-by-default treatment;
- no silent feature expansion;
- narrow purpose limitation;
- no characteristic-based profiling by default;
- accuracy, error, and performance disclosure;
- no sole reliance for enforcement;
- no watchlist or matching by default;
- no cross-system or cross-camera tracking by default;
- no secondary use, AI training, or model improvement;
- no commercial enrichment or external matching;
- vendor access restrictions;
- remote access and support controls;
- encryption and key-control requirements where designated;
- query, match, and alert logging;
- administrative and configuration logging;
- retention and deletion requirements;
- public-records, legal-compliance, and oversight support;
- renewal and continuation conditions;
- transition and exit support; and
- a more-protective-rule clause.

Addendum H. Commercially Acquired Surveillance Data

This addendum applies to brokered location data, app-derived location data, commercial ALPR data, private camera-network data, telematics feeds, consumer movement datasets, data-broker identity/location/association products, and similar services.

Core contract requirements include:

- purpose limitation;
- source and provenance disclosure;
- no circumvention of City safeguards;
- disclosure of all categories of raw data and derived outputs;
- no hidden enrichment or matching;
- no reverse, dragnet, or pattern-of-life functions by default;
- no commercial enrichment of City data;
- no secondary use, AI training, or product development;
- no reliability claims without disclosure;
- no sole reliance for enforcement;
- sensitive-location and protected-activity restrictions;
- access control and role separation;

- vendor access restrictions;
- remote access and support controls;
- encryption and key-control requirements where designated;
- query, output, and export logging;
- administrative and configuration logging;
- retention and deletion requirements;
- public-records, legal-compliance, and oversight support;
- renewal and continuation conditions;
- transition and exit support; and
- a more-protective-rule clause.

Section 9. Procurement Review Process

Before procurement activity proceeds, the responsible City department should determine whether the proposed technology, service, platform, dataset, or related agreement falls within the scope of the Framework. If covered, the department should classify the procurement, identify applicable addenda, assemble required documentation, route the matter for legal, procurement, and technical review, determine whether Council approval is required, obtain vendor disclosures, and maintain a written record of review.

The written record should show how the technology was classified, which addenda were applied, whether Council approval was required, what major issues were identified, how those issues were resolved, and whether any features were expressly rejected, disabled, or deferred.

Section 10. Review Triggers for Renewals, Extensions, and Material Changes

The City should treat the following events as requiring renewed review under this Framework:

- renewals, extensions, or other continuations;
- amendments or addenda affecting function, access, retention, hosting, integration, or legal rights;
- activation of optional, premium, pilot, beta, or future-available features;
- AI or analytics changes;
- addition of new data sources, connectors, APIs, or feeds;
- materially broader search or query capability;
- new sharing or network participation;
- hosting or subcontractor changes;
- retention or deletion changes;
- key-control or access-pathway changes;
- relevant policy or legal changes; and
- incidents such as unauthorized access, unapproved feature activation, significant audit failure, or serious breach.

The City should evaluate the substance of the change, not merely the vendor's label for it, and should document the trigger review, required approvals, imposed conditions, and final decision.

Section 11. Vendor Compliance Certification

The City should require vendors to submit written compliance certifications at defined points in the procurement and contract lifecycle, including before go-live, renewal, extension, amendment, feature activation, Material Change, new integration, material hosting or subcontractor change, or at any additional time reasonably requested by the City.

Each certification should address:

- compliance with applicable contract safeguards;
- whether any Material Change has occurred;
- whether any new feature, analytics module, AI function, integration, or search capability has been activated or made available;
- whether any hosting, subcontractor, retention, deletion, key-management, decryption, plaintext-access, or privileged-access condition has changed;
- whether any breach, unauthorized access, logging failure, deletion failure, or significant security incident has occurred;
- whether outstanding audit findings or compliance issues remain; and
- whether the vendor remains able and willing to comply with all applicable City requirements.

Where key-control safeguards are required, the certification should also address who controls the keys or equivalent access controls, whether any outside party has unilateral capability to decrypt covered stored data, whether any exceptional access event has occurred, and whether the City remains able to rotate, suspend, revoke, or replace keys or equivalent safeguards.

Section 12. City Compliance Review and Renewal Checklist

Before the City renews, extends, amends, materially expands, activates a feature in, or otherwise continues a covered surveillance-related contract, the City should conduct and document a compliance review sufficient to determine whether continuation is permissible and prudent.

The review should consider:

- whether the technology is still correctly classified;
- whether the same addenda still apply;
- whether new features, integrations, datasets, or analytic capabilities have become available;
- whether any latent or future-available capability has been activated or exposed;
- whether hosting, storage, subcontractor, ownership, or processing arrangements have changed;
- whether retention and deletion settings are functioning as required;

- whether audit logs are complete and preserved;
- whether any breach, unauthorized access, logging failure, or deletion failure has occurred;
- whether key-control protections remain in place where required;
- whether any exceptional plaintext access has occurred;
- whether complaints, audit findings, policy violations, or other compliance issues have arisen;
- whether continued use remains necessary and proportionate; and
- whether less intrusive reasonable alternatives are now available.

The review should end with one of five outcomes: approved, approved with conditions, deferred pending remediation, denied, or escalated for Council approval.

Section 13. Legacy Contract Transition Framework

The City should apply a transition framework to surveillance-related technologies, services, platforms, datasets, and agreements already in use or already under contract when the City begins applying this Framework.

The transition framework should:

- identify legacy contracts and systems;
- determine where current safeguards already exist;
- identify areas of noncompliance or incomplete protection;
- prioritize remediation, renegotiation, or discontinuation where necessary; and
- prevent indefinite grandfathering of outdated contract terms, vendor practices, or unsupported capabilities.

For each legacy system, the City should maintain an inventory entry identifying the system, vendor, department, current term, renewal dates, classification, applicable addenda, known high-risk capabilities, and whether the system is governed by an existing administrative policy, department policy, ordinance, contract term, intergovernmental agreement, or other written rule.

Where a legacy contract or program is partially compliant or materially noncompliant, the City should prepare a transition plan identifying the compliance gap, the nature of the issue, the corrective action required, the responsible party, the remediation timeline, and whether interim restrictions or Council escalation are needed.

No legacy contract should be renewed or materially expanded simply because it has been renewed in the past.

Section 14. Implementation Tools

To support consistent application of this Framework, the City should maintain and use practical implementation tools sufficient to guide procurement staff, legal counsel, technical reviewers, department personnel, and decisionmakers through covered surveillance-related procurements and continuation events.

Recommended tools include:

- a procurement intake checklist;
- a technology classification worksheet;
- a vendor questionnaire;
- a contract review checklist;
- a renewal and continuation review form;
- a feature and Material Change review form;
- a legacy transition worksheet;
- a logging and audit verification checklist;
- an inventory and source-of-authority record;
- a public reporting support template; and
- a decision log and audit trail.

The existence of an implementation tool, checklist, worksheet, or form shall not be construed to narrow, waive, or replace the substantive requirements of the Framework.