ORDINANCE NO. _____

AN ORDINANCE OF THE CITY OF BEND ESTABLISHING REQUIREMENTS FOR THE APPROVAL, ACQUISITION, USE, MANAGEMENT, OVERSIGHT, AND SUNSETTING OF SURVEILLANCE TECHNOLOGY; PROTECTING PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES; IMPOSING SPECIAL RULES FOR HIGH-RISK SURVEILLANCE TECHNOLOGIES; AND REQUIRING EXCLUSIVE AGENCY CONTROL OF DECRYPTION KEYS FOR CERTAIN DATA.

THE CITY OF BEND ORDAINS AS FOLLOWS:

SECTION 1. TITLE.

This Ordinance shall be known and may be cited as the **Bend Surveillance Technology Accountability, Privacy, and Civil Rights Ordinance**.

SECTION 2. FINDINGS AND PURPOSE.

The City Council finds and declares that:

A. Surveillance technologies can materially affect privacy, anonymity, civil rights, civil liberties, due process, equal protection, freedom of speech, freedom of association, freedom of religion, freedom of the press, and the ability of residents to seek medical care, legal assistance, shelter, mutual aid, or other essential services without undue government monitoring.

B. Technologies that collect or reveal location, movement, association, communications-related metadata, device identifiers, biometric information, or patterns of life are especially sensitive because they can reveal intimate details of a person’s life even where no criminal conduct is present.

C. Surveillance capability frequently expands after procurement through software updates, firmware updates, feature toggles, plug-ins, application programming interfaces, vendor-hosted analytics, cloud migration, data-sharing arrangements, artificial intelligence modules, or integration with other systems.

D. The public has a substantial interest in ensuring that surveillance technology is not acquired, funded, used, expanded, or renewed without transparent democratic approval, enforceable safeguards, periodic review, and meaningful accountability.

E. The City of Bend has a duty to protect law-abiding residents from unnecessary, overbroad, discriminatory, or insecure surveillance, including surveillance that may chill protected activity or expose residents to misuse, data breach, secondary use, commercial exploitation, or mission creep.

F. The City has adopted certain technology-specific and administrative safeguards relating to particular systems and practices. However, those measures do not by themselves establish a comprehensive, citywide, durable framework governing all surveillance technologies, renewals, material changes, vendor controls, and future expansion.

G. Oregon law, including Senate Bill 1516 and other applicable state and federal law, governs certain surveillance technologies and law-enforcement activities. This Ordinance is intended to supplement such

law with local protections to the maximum extent permitted. This Ordinance shall not be construed to authorize conduct prohibited by state or federal law, and any provision of this Ordinance that is more protective of privacy, civil rights, or civil liberties than otherwise applicable law shall govern to the fullest extent permitted.

H. The purposes of this Ordinance are to:

1. require public approval before surveillance technology is acquired, deployed, materially expanded, or renewed;
2. require transparency, minimization, encryption, auditing, and deletion;
3. prohibit uses that are inconsistent with privacy, civil rights, and democratic accountability;
4. impose heightened safeguards for high-risk technologies;
5. ensure that only the Bend Police Department controls decryption of covered stored data, except where disclosure is made through lawful, agency-controlled process; and
6. prevent future scope creep through software-enabled expansion and emerging technologies.

SECTION 3. DEFINITIONS.

For purposes of this Ordinance, the following terms shall have the meanings set forth below:

A. **Authorized User** means a person specifically designated in writing by a City department and permitted under an approved Surveillance Use Policy to access a particular surveillance technology or surveillance data for an authorized purpose.

B. **Biometric Data** means any data or template derived from a person's physiological, biological, or behavioral characteristics that is used or capable of being used to identify, infer the identity of, classify, authenticate, or track a person, including face geometry, voiceprint, iris or retina information, gait, fingerprints, palmprints, or similar characteristics.

C. **Cell-Site Simulator** means a device or system that transmits or receives radio signals for the purpose of identifying, locating, tracking, or obtaining signaling information from cellular telephones or other wireless devices by impersonating, simulating, or interacting with a wireless communications site or network element.

D. **City** means the City of Bend and any department, division, office, board, commission, employee, officer, agent, contractor, consultant, or vendor acting on behalf of the City.

E. **Commercially Acquired Surveillance Data** means location information, camera data, telematics data, license plate data, social-media monitoring output, consumer profile data, brokered data, or any similar dataset obtained from a data broker, private company, or commercial intermediary rather than directly collected by the City.

F. **Data Fusion System** or **Real-Time Crime Center System** means any platform, dashboard, service, or system that aggregates, correlates, analyzes, visualizes, or enables searching across two or more data sources, including cameras, ALPR, CAD, RMS, maps, sensor feeds, signals intelligence, social media, geospatial data, commercial data, or analytics outputs.

G. **Decrypted Data** means data rendered into plaintext, intelligible form, or otherwise made readable beyond encrypted storage or transmission format.

H. **Electronic Device Identifier** means a persistent, semi-persistent, hashed, pseudonymous, or other identifier associated with a phone, vehicle, wearable, telematics system, tag, transponder, beacon, Bluetooth device, Wi-Fi device, RFID tag, or other electronic device or component.

I. **Exclusive Agency Key Control** means a technical and administrative system in which only the Bend Police Department, through agency-controlled cryptographic keys and agency-controlled identity and access systems, may decrypt stored covered data, and in which no vendor, cloud host, subcontractor, or outside entity possesses unilateral decryption capability.

J. **High-Risk Surveillance Technology** means surveillance technology capable of identifying, tracking, inferring information about, or creating historical records about individuals, groups, vehicles, or devices over time or at scale, including ALPR, drones, cell-site simulators, biometric systems, signals intelligence platforms, social-media monitoring systems, commercial location-data systems, and data-fusion systems.

K. **Historical Location Information** means information that reveals or can reasonably be used to reveal the past location, movement, route, travel history, pattern of travel, co-travel, or pattern of life of a person, vehicle, or device.

L. **Material Change** means any change to a surveillance technology, service, contract, configuration, integration, policy, retention setting, data source, software version, firmware, module, plug-in, feature flag, analytics capability, AI capability, sharing capability, user category, hosting arrangement, or access pathway that materially expands collection, retention, sharing, inference, identifiability, monitoring scope, administrative access, or decryption access beyond what the City Council previously approved.

M. **Protected Activity** means conduct protected by the United States Constitution, the Oregon Constitution, or other law, including speech, protest, assembly, petition, journalism, religious exercise, labor organizing, political activity, association, legal advocacy, mutual aid, and access to lawful medical care.

N. **Sensitive Location** means a place where surveillance may reveal especially private or constitutionally sensitive activity, including a house of worship, medical facility, reproductive or gender-affirming care facility, addiction treatment center, domestic-violence shelter, legal-aid office, immigration-services provider, library, newsroom, school, polling place, union hall, political meeting, homeless shelter, sanctioned camp, unsanctioned camp, warming shelter, cooling shelter, safe-parking site, meal site, hygiene site, outreach-service site, or place primarily used by unhoused persons for shelter or essential survival services.

O. **Signal Intelligence System** means any system that captures, detects, stores, analyzes, correlates, or searches for wireless signals, communications-related signaling information, telematics, Bluetooth, Wi-Fi, RFID, beacon emissions, transponder signals, electronic identifiers, or similar data in order to identify, associate, locate, or track persons, devices, or vehicles.

P. **Surveillance Data** means any data, metadata, image, video, audio, signal, identifier, derived data, analytic output, alert, report, model output, or other information collected, generated, inferred, received, retained, or shared through surveillance technology.

Q. **Surveillance Technology** means any software, hardware, service, system, platform, device, sensor, or capability used, designed, or primarily capable of collecting, capturing, recording, retaining, processing, identifying, analyzing, inferring, locating, tracking, monitoring, or sharing information about individuals, groups, vehicles, devices, places, or activities. The term includes technologies that are fixed, mobile, handheld, wearable, aerial, cloud-hosted, vendor-operated, integrated into another platform, or later enabled through an update, plug-in, application programming interface, analytics package, or artificial-intelligence module.

R. **Video Analytics** means software or services that analyze video or image data for identification, classification, object detection, pattern detection, re-identification, behavioral inference, demographic inference, facial recognition, gait recognition, anomaly detection, or similar purposes.

S. Where Oregon law defines a term applicable to a specific technology regulated by this Ordinance, including automated license plate recognition systems, that definition shall govern for that technology to the extent required by law. The incorporation of a state-law definition shall not be construed to narrow any broader protection otherwise provided by this Ordinance unless such narrowing is required by controlling law.

SECTION 4. SCOPE.

A. This Ordinance applies to all City departments, offices, units, employees, officers, agents, contractors, consultants, and vendors acting on behalf of the City.

B. This Ordinance applies whether the surveillance technology or surveillance data is owned, leased, borrowed, donated, piloted, accessed by subscription, hosted in the cloud, vendor-managed, shared through an intergovernmental arrangement, or otherwise operated for City use or benefit.

C. No person or entity shall evade this Ordinance by using a contractor, grant, temporary pilot, free trial, emergency purchase, partner-agency arrangement, data-sharing arrangement, or other indirect means in place of direct City acquisition or operation.

SECTION 5. CITY COUNCIL APPROVAL REQUIRED.

A. Except as expressly provided in subsection H of this Section, no City department shall do any of the following without prior City Council approval by ordinance or resolution after public notice and hearing:

1. seek, accept, or use funding, grants, gifts, loans, in-kind support, or donations for surveillance technology;
2. acquire, borrow, subscribe to, lease, test, pilot, access, or deploy surveillance technology;
3. enter into, renew, extend, or materially modify a contract, memorandum, subscription, or service arrangement involving surveillance technology or surveillance data;
4. enable a new feature, module, integration, analytics capability, AI capability, or data source;
5. join or participate in any regional, statewide, national, or commercial data-sharing or query network;
6. materially expand the use, retention, scope, access, or sharing of an already approved technology;
7. retain surveillance data longer than previously approved; or
8. use an approved surveillance technology for a new purpose.

A. City Council approval shall be technology-specific and shall not be construed to authorize any use, integration, feature, module, workflow, or data source not expressly disclosed and approved.

B. Approval of one surveillance technology does not authorize the acquisition or use of another, even if sold by the same vendor, packaged in the same platform, or integrated with the same service.

C. Approval of hardware does not authorize use of software features not expressly approved.

D. Approval of a platform does not authorize later-available features, modules, integrations, or updates that constitute a Material Change.

E. Any ambiguity shall be resolved in favor of requiring prior City Council approval.

F. No contract term, click-through term, vendor policy, or vendor representation may supersede or narrow the requirements of this Section.

G. **Emergency Use.**

1. In a documented emergency posing an imminent threat of death or serious physical injury, a department may temporarily deploy a surveillance capability without prior City Council approval only for the period strictly necessary to respond to that emergency.
2. Any emergency use under this subsection shall:
    a. be approved in writing by both the Chief of Police and the City Manager;
    b. identify with specificity the facts constituting the emergency;
    c. identify the specific surveillance technology or capability used;
    d. identify the start date and time of use;
    e. be narrowly limited in scope, geography, duration, and purpose;
    f. expire automatically no later than seven (7) days after authorization; and
    g. not be renewed, extended, or reauthorized administratively.
3. A surveillance technology used under this subsection may not be deployed again under emergency authority for the same or substantially similar purpose, facts, operational need, incident type, investigative objective, or programmatic function unless and until City Council approves the technology and use under this Ordinance.
4. Multiple emergency authorizations may not be used to evade the approval, reporting, renewal, sunset, or other requirements of this Ordinance.
5. Any emergency use shall be reported to the City Council within seven (7) days of authorization and publicly disclosed within seven (7) days, unless disclosure of specific facts would create a concrete and articulable threat to an active criminal investigation or to a person's safety. Any temporarily withheld facts shall be disclosed as soon as that risk no longer exists.
6. All data collected, retained, accessed, or shared pursuant to emergency use remains subject to the encryption, minimization, retention, deletion, audit, logging, sharing, and use restrictions of this Ordinance.
7. If City Council does not approve continued use before the emergency authorization expires, use shall cease immediately upon expiration, and any non-evidentiary data collected pursuant to the emergency authorization shall be deleted in accordance with this Ordinance.
8. Nothing in this subsection authorizes the acquisition, pilot, subscription, renewal, expansion, or continued programmatic use of surveillance technology beyond the strictly time-limited emergency authorization described herein.

SECTION 6. REQUIRED PRE-APPROVAL SUBMISSIONS.

Before any approval under Section 5, the sponsoring department shall publicly release, at least thirty (30) days before the hearing, the following:

A. a **Surveillance Impact Report**;

B. a **Surveillance Use Policy**;

C. a **Cybersecurity and Encryption Addendum**;

D. a **Vendor and Data Governance Addendum**;

E. a **Civil Rights and Civil Liberties Impact Addendum**; and

F. for any High-Risk Surveillance Technology, a **Technology-Specific Addendum** addressing the special risks and safeguards applicable to that category.

SECTION 7. SURVEILLANCE IMPACT REPORT.

The Surveillance Impact Report shall include, at a minimum:

A. a description of the technology and all current, latent, optional, configurable, and update-enabled capabilities;

B. the specific purposes for which the department seeks approval;

C. the legal authority for proposed use;

D. the categories of persons, places, vehicles, devices, or activities affected;

E. the categories of data collected, generated, inferred, retained, or shared;

F. whether the technology can reveal Historical Location Information, Biometric Data, Protected Activity, or information about Sensitive Locations;

G. whether the technology can be used for reverse searches, association analysis, geofencing, pattern-of-life analysis, co-traveler analysis, social-graph analysis, or AI-assisted inference;

H. the expected quantity and duration of data collection and retention;

I. all internal and external data-sharing pathways;

J. all vendors, subcontractors, hosting providers, service providers, analytics providers, and integration partners;

K. all costs, including procurement, subscription, storage, maintenance, staffing, training, auditing, redaction, public-records response, and eventual system retirement;

L. a description of cybersecurity risks, privacy risks, civil-rights risks, civil-liberties risks, accuracy risks, bias risks, and mission-creep risks;

M. alternatives considered, including non-technological and less intrusive alternatives;

N. the safeguards proposed to mitigate each material risk; and

O. a statement whether the system can support Exclusive Agency Key Control and, if not, why not.

SECTION 8. SURVEILLANCE USE POLICY.

The Surveillance Use Policy shall include, at a minimum:

A. authorized purposes and prohibited purposes;

B. the categories of Authorized Users;

C. training and certification requirements;

D. supervisor approval requirements;

E. query justification requirements;

F. case-number requirements where applicable;

G. retention and deletion rules;

H. sharing rules and restrictions;

I. audit procedures;

J. breach-response procedures;

K. complaint and redress procedures;

L. disciplinary consequences for misuse;

M. procedures for disabling unapproved features and reporting attempted or automatic feature activation; and

N. procedures for compliance with this Ordinance and applicable law.

SECTION 9. GENERAL PROHIBITIONS.

No City department, employee, officer, agent, contractor, or vendor acting on behalf of the City shall use surveillance technology or surveillance data:

A. to monitor, identify, track, map, catalogue, or analyze Protected Activity absent a warrant supported by probable cause for a specific criminal offense unrelated to the exercise of protected rights, unless controlling law expressly forbids such a warrant requirement for the specific investigative act at issue;

B. for generalized, persistent, or suspicionless tracking of persons, vehicles, devices, or groups;

C. to target, classify, score, or subject any person or group to investigation or enforcement based solely or primarily on race, ethnicity, national origin, religion, disability, sex, sexual orientation, gender identity, immigration status, housing status, political viewpoint, or other protected characteristic;

D. to monitor, identify, track, map, catalogue, or analyze presence at or near a Sensitive Location, except pursuant to a warrant supported by probable cause for a specific violent felony investigation and only to the minimum extent necessary;

E. to identify, map, catalogue, predict, or monitor the movements, associations, or survival activities of unhoused persons absent a warrant supported by probable cause for a specific violent felony investigation and only to the minimum extent necessary;

F. to sell, license, rent, trade, monetize, or commercially exploit surveillance data;

G. to train, fine-tune, benchmark, validate, improve, or otherwise develop a vendor's algorithm, model, analytics engine, product, or service using City surveillance data, including de-identified, pseudonymized, aggregate, sample, derived, or test data;

H. to take enforcement action based solely on automated output, alerting, scoring, inference, or analytic recommendation without independent human review and corroboration;

I. for civil immigration enforcement, except where disclosure or use is specifically required by controlling law; or

J. in any manner not expressly approved by City Council and the applicable Surveillance Use Policy.

SECTION 10. SENSITIVE-LOCATION PROTECTIONS.

A. The City shall not use surveillance technology to identify, track, map, analyze, or document visits to or presence near Sensitive Locations, except as expressly permitted by Section 9(D).

B. Sensitive Locations include, without limitation:

1. protests and marches;
2. union meetings and labor-organizing sites;
3. houses of worship and religious events;
4. abortion, reproductive, and gender-affirming care facilities;
5. addiction-treatment centers;
6. domestic-violence shelters;
7. immigration legal-aid offices and immigration-services providers;
8. libraries, newsrooms, and political meetings; and
9. homeless shelters, sanctioned camps, unsanctioned camps, warming shelters, cooling shelters, safe-parking sites, meal sites, hygiene sites, outreach-service locations, and places primarily used by unhoused persons for shelter or essential survival services.

A. No City department shall use surveillance technology to create a registry, map, dataset, alert system, heat map, or analytic profile concerning unhoused persons, camps, or use of homelessness-related services, except where expressly required by controlling law and specifically approved by City Council after public notice and hearing.

SECTION 11. ENCRYPTION, IDENTITY, AND LOCAL DECRYPTION CONTROL.

A. All surveillance data shall be encrypted in transit and at rest using contemporary, industry-standard cryptographic protections.

B. All covered stored surveillance data collected or maintained by or for the Bend Police Department shall be subject to Exclusive Agency Key Control.

C. No vendor, reseller, cloud host, subcontractor, consultant, or outside agency shall possess unilateral capability to decrypt covered stored data.

D. Access to Decrypted Data shall require authentication through agency-controlled identity systems and multi-factor authentication.

E. Access shall be role-based and limited to the least privilege necessary for the authorized purpose.

F. Shared accounts are prohibited.

G. Privileged administrative access shall be separately logged and audited.

H. Remote maintenance or support shall not expose Decrypted Data except through a documented, time-limited, agency-approved support session that is logged, monitored, and limited to the minimum necessary.

I. No new surveillance technology shall be approved, and no existing surveillance technology shall be renewed or materially expanded, if its architecture cannot support the requirements of this Section, unless City Council makes express written findings, after public hearing, that:

1. no less intrusive or more secure alternative is reasonably available;
2. the public interest compellingly requires the capability; and

3. equally strong compensating controls are imposed by ordinance or approved policy.

A. Nothing in this Section prohibits the City from lawfully disclosing data pursuant to court order, criminal-discovery obligations, public-records law, or other applicable law, provided that any such disclosure is made through agency-controlled process and not through unilateral vendor access to plaintext data.

SECTION 12. VENDOR RESTRICTIONS AND PROCUREMENT SAFEGUARDS.

A. Every contract or agreement involving surveillance technology shall require, at a minimum:

1. City ownership and control of City-generated surveillance data, logs, configurations, and deletion records;
2. prohibition on vendor secondary use;
3. prohibition on vendor AI training, model improvement, or product development using City data;
4. prohibition on undisclosed subcontractors;
5. prohibition on remote feature activation or silent configuration changes;
6. prohibition on silent or unilateral changes to retention settings;
7. breach notification within a contractually specified deadline;
8. deletion certification upon request, contract termination, or expiration of retention periods;
9. City audit rights regarding logs, access records, configurations, and deletion compliance;
10. advance written notice of any change in hosting provider, subcontractor, ownership, merger, acquisition, or material security posture; and
11. compliance with this Ordinance, including compliance upon renewal, extension, amendment, feature activation, and Material Change.

A. Any contract term inconsistent with this Ordinance is void and unenforceable to the fullest extent permitted by law.

B. No contract shall require the City to waive privacy, security, audit, deletion, or public-accountability requirements as a condition of procurement or continued use.

SECTION 13. MATERIAL CHANGES, SOFTWARE UPDATES, AND EMERGING TECHNOLOGIES.

A. No Material Change may be activated, accepted, used, or renewed without prior City Council approval under Section 5.

B. Material Changes include, without limitation:

1. new analytics or AI modules;
2. facial recognition, gait recognition, voice recognition, or other biometric features;
3. reverse-search capability;
4. geofencing or proximity-search capability;
5. pattern-of-life, co-traveler, or associate analysis;
6. broader sharing or new network participation;
7. longer retention periods;

8. collection of new categories of data;
9. new integrations, application programming interfaces, or data sources;
10. migration to vendor-hosted or cloud-hosted storage where not previously approved;
11. new administrative access pathways;
12. any change affecting decryption, plaintext visibility, or key control; and
13. any change enabling location or association analysis based on signals emitted by personal or vehicle-borne electronics.

A. The burden shall be on the sponsoring department to show that a change is not material.

B. Automatic, vendor-pushed, or bundled updates shall not authorize unapproved capabilities.

SECTION 14. LOGGING, AUDITS, AND PUBLIC ACCOUNTABILITY.

A. Every access to surveillance data, Historical Location Information, or Decrypted Data shall generate a log entry recording, to the extent applicable:

1. user identity;
2. date and time;
3. device or terminal used;
4. case number or reference number;
5. specific purpose;
6. legal authority relied upon;
7. categories of data accessed;
8. whether data was exported, copied, disseminated, or shared; and
9. supervisor approval, where required.

A. Supervisory audits shall occur at least monthly for High-Risk Surveillance Technologies and at least quarterly for other approved surveillance technologies.

B. The City shall obtain an annual independent audit of each approved High-Risk Surveillance Technology program.

C. The City shall publish an annual public report describing:

1. approved technologies in use;
2. number of deployments, queries, or uses;
3. number of historical or retrospective searches;
4. categories of purpose;
5. number of sharing events;
6. number of policy violations or misuse incidents;
7. number of breaches or security incidents;
8. retention and deletion compliance;
9. aggregate accuracy and false-match information where applicable;

10. complaints received and their disposition; and
11. any Material Changes proposed, approved, denied, or discovered without approval.

A. Audit reports shall be presented to City Council in a public meeting, except for portions lawfully withheld.

SECTION 15. COMPLAINTS, REDRESS, AND ENFORCEMENT.

A. The City shall maintain a public complaint process through which any person may allege misuse, discriminatory use, overcollection, unlawful sharing, inaccurate data, unlawful retention, unauthorized feature activation, or failure to comply with this Ordinance.

B. The City shall acknowledge complaints within a reasonable time and provide a written disposition unless prohibited by law.

C. Violations of this Ordinance shall be grounds for corrective action, retraining, suspension of access, discipline, contract termination, or other lawful remedy.

D. Any City official or employee who knowingly circumvents logging, encryption controls, audit requirements, or approval requirements commits serious misconduct.

E. Any vendor that knowingly facilitates misuse, unauthorized access, unauthorized sharing, unapproved feature activation, or noncompliance with this Ordinance shall be subject to contract remedies, suspension, termination, and disqualification from future procurement as permitted by law.

SECTION 16. AUTOMATIC SUSPENSION.

A. Use of a surveillance technology program shall be suspended upon a documented finding of any of the following:

1. unauthorized vendor access to Decrypted Data;
2. unlawful sharing outside approved channels;
3. unapproved Material Change activation;
4. significant audit failure;
5. serious breach affecting surveillance data;
6. repeated or systemic misuse; or
7. loss of required encryption, key control, logging, or access controls.

A. A suspended program may resume only after:

1. corrective action has been completed;
2. City Council receives written findings regarding cause, scope, and remediation; and
3. public notice is provided.

ARTICLE I. CAMERA AND VIDEO SURVEILLANCE SYSTEMS

SECTION 17. CAMERA AND VIDEO SYSTEMS.

A. This Article applies to fixed cameras, traffic cameras, public-space cameras, body-worn cameras, in-car cameras, wearable cameras, smart glasses, trailer-mounted camera systems, robot-mounted cameras, and other image or video capture systems used by or for the City.

B. No camera or video system may be used with unapproved Video Analytics.

C. Audio capture shall require separate City Council approval unless already specifically authorized by law and previously approved.

D. The City shall not use camera or video systems for continuous monitoring of Sensitive Locations except as expressly authorized by warrant and approved policy.

E. Retention limits for video data shall be established by approved policy and shall reflect minimization and deletion as soon as no longer necessary for an approved purpose.

ARTICLE II. AUTOMATED LICENSE PLATE RECOGNITION AND VEHICLE-LOCATION SYSTEMS

SECTION 18. APPLICABILITY.

This Article applies to any automated license plate recognition system and any related use of captured license plate data or derived vehicle-location information. This Article shall be construed consistently with Oregon law, including Senate Bill 1516, and shall not be interpreted to authorize any use prohibited by state law.

SECTION 19. AUTHORIZED USES.

ALPR systems may be used only for purposes lawful under Oregon law and this Ordinance, as set forth in an approved Surveillance Use Policy.

SECTION 20. HISTORICAL LOCATION SEARCHES.

A. No Authorized User shall access Historical Location Information derived from ALPR data unless:

1. the user has a warrant supported by probable cause; or
2. the search is expressly authorized by controlling law under a narrow, documented exception.

A. Real-time or near-time alert confirmation shall not authorize a broader retrospective search absent compliance with subsection A.

B. Pattern-of-life analysis, route reconstruction, co-traveler analysis, or retrospective vehicle-movement analysis shall require a warrant unless controlling law expressly provides otherwise.

SECTION 21. HOT LISTS.

A. Every hot-list entry shall be supported by a documented case-specific basis and approved by a supervisor.

B. Each hot-list entry shall include:

1. case number;
2. entering user;
3. approving supervisor;
4. date and time;
5. factual basis;
6. legal basis; and
7. expiration date.

A. Hot-list entries shall expire automatically no later than seven (7) days after entry unless renewed in writing by a supervisor with updated justification.

B. No hot-list entry may be based solely on Protected Activity, association, immigration status, nonpayment of debt, or presence at a Sensitive Location.

SECTION 22. RETENTION.

A. Non-hit, non-flagged ALPR data shall be deleted automatically within seventy-two (72) hours.

B. Evidentiary or alert-related data may be retained only so long as necessary for the associated case or legal requirement.

C. Historical bulk datasets shall not be maintained for speculative future use.

D. Vendors shall certify deletion upon request and upon expiration of retention periods.

SECTION 23. SHARING.

A. ALPR data shall not be shared outside the Bend Police Department except as specifically permitted by controlling law, this Ordinance, and approved policy.

B. No ALPR data may be shared with private companies, data brokers, insurers, repossession services, or for civil immigration enforcement, except where disclosure is specifically required by controlling law.

C. Participation in any external ALPR sharing or search network requires separate City Council approval.

ARTICLE III. SIGNAL INTELLIGENCE AND CELL-SITE SIMULATOR SYSTEMS

SECTION 24. APPLICABILITY.

This Article applies to cell-site simulators, wireless-signals intelligence systems, Bluetooth tracking tools, Wi-Fi identifier-capture systems, RFID systems, telematics-identifier systems, beacon-capture systems, electronic-device correlation tools, and similar technologies capable of identifying, associating, locating, or tracking persons, devices, or vehicles through emitted or associated signals.

SECTION 25. WARRANT REQUIREMENT.

A. No Authorized User shall use a Cell-Site Simulator or Signal Intelligence System to identify, locate, track, or retrospectively analyze a person, device, or vehicle unless authorized by a warrant supported by probable cause, except where controlling law expressly provides a narrower lawful exception.

B. Collection of signaling information from non-target devices shall be minimized to the greatest extent technically possible.

C. Non-target data shall be deleted immediately or as soon as technically feasible and shall not be retained, shared, or used for a secondary purpose.

SECTION 26. PROHIBITED USES.

The City shall not use a Signal Intelligence System or Cell-Site Simulator:

A. for mass collection around protests, houses of worship, clinics, shelters, camps, political meetings, or other Sensitive Locations;

B. for reverse or dragnet searches;

C. to identify co-travelers, associates, or nearby devices absent judicial authorization; or

D. to correlate personal device identifiers with vehicle travel history absent lawful authority and City Council-approved policy.

ARTICLE IV. DRONES AND AERIAL SURVEILLANCE

SECTION 27. APPLICABILITY.

This Article applies to drones, unmanned aircraft systems, tethered drones, aerial camera packages, thermal-imaging devices used from aerial platforms, and other aerial-surveillance systems used by or for the City.

SECTION 28. LIMITS.

A. Aerial-surveillance programs require separate City Council approval.

B. No aerial surveillance shall be used for routine monitoring of public gatherings, protests, or Sensitive Locations absent warrant authority and approved policy.

C. Persistent aerial surveillance is prohibited unless expressly approved by City Council after public hearing with specific written findings of necessity and narrow tailoring.

D. Facial recognition and unapproved Video Analytics are prohibited on aerial platforms.

E. Retention shall be minimized and set forth in approved policy.

ARTICLE V. BIOMETRIC AND VIDEO ANALYTICS TECHNOLOGIES

SECTION 29. PROHIBITION ABSENT EXPRESS ORDINANCE.

A. The City shall not acquire, use, access, or enable facial recognition, gait recognition, voiceprint recognition, emotion recognition, demographic inference, person re-identification, or similar biometric or characteristic-based analytics unless expressly authorized by a future ordinance that specifically names the capability and imposes technology-specific safeguards.

B. Approval of a camera or video system does not constitute approval of biometric, characteristic-based, or re-identification capabilities.

C. Any attempted or automatic activation of such a feature shall be reported immediately and treated as a Material Change.

ARTICLE VI. DATA FUSION AND REAL-TIME CRIME CENTER SYSTEMS

SECTION 30. APPLICABILITY.

This Article applies to Data Fusion Systems and Real-Time Crime Center Systems.

SECTION 31. REQUIREMENTS.

A. Separate approval is required for any Data Fusion System or Real-Time Crime Center System.

B. The City shall maintain a source-by-source inventory of all data inputs.

C. No unapproved data feed may be ingested.

D. No automated suspicion score, risk score, or enforcement recommendation may be used as the sole basis for enforcement action.

E. Every query shall require documented purpose and, where applicable, case number.

F. Visits to or presence at Sensitive Locations shall not be aggregated into profiles, alerts, or pattern-of-life outputs.

ARTICLE VII. SOCIAL MEDIA MONITORING

SECTION 32. SOCIAL MEDIA AND ONLINE SURVEILLANCE.

A. The City shall not acquire or use social-media monitoring, scraping, keyword tracking, event-monitoring, or online-profiling tools without separate City Council approval.

B. Generalized monitoring of journalists, organizers, advocacy groups, labor activity, or political activity is prohibited.

ARTICLE VIII. COMMERCIALLY ACQUIRED SURVEILLANCE DATA

SECTION 33. COMMERCIAL DATA.

A. The City shall not acquire, license, access, or use Commercially Acquired Surveillance Data without separate City Council approval by ordinance after public notice and hearing.

B. The City shall not use commercially acquired location data, commercial ALPR data, app-derived location data, or similar datasets to circumvent the protections of this Ordinance.

ARTICLE IX. DIGITAL FORENSIC EXTRACTION TOOLS

SECTION 34. FORENSIC TOOLS.

A. This Article applies to phone-extraction tools, digital-forensic kiosks, cloud-extraction tools, vehicle-telematics extraction tools, and similar systems.

B. Use of such tools shall be governed by warrant requirements, minimization, logging, retention, and audit rules set forth in approved policy and applicable law.

SECTION 35. RENEWAL, SUNSET, AND PUBLIC INVENTORY.

A. The City shall maintain a public inventory of all approved surveillance technologies. The public inventory shall note any existing administrative or department-level policy that currently governs each listed technology.

B. Approval of a surveillance technology shall expire twenty-four (24) months after approval unless renewed by City Council after public hearing.

C. Renewal shall require updated reports and disclosure of any proposed Material Changes.

SECTION 36. EXISTING CONTRACTS, LEGACY SYSTEMS, AND TRANSITION TO COMPLIANCE.

A. This Ordinance applies immediately upon its effective date to all new acquisitions, pilots, subscriptions, deployments, renewals, extensions, amendments, addenda, statements of work, feature activations, integrations, data-sharing arrangements, and Material Changes involving surveillance technology.

B. For all surveillance technologies, services, platforms, and data arrangements already in use or under contract on the effective date of this Ordinance, the City shall, within ninety (90) days, prepare and publicly release:

1. an inventory of each covered surveillance technology, platform, service, or data arrangement currently in use;
2. the City department using it;
3. the vendor, provider, host, or contractor associated with it;
4. the governing contract, subscription, memorandum, amendment, addendum, or statement of work;

5. the effective date and renewal or expiration date of each such agreement;
6. a preliminary assessment of whether the technology, service, and governing agreement comply with this Ordinance;
7. a remediation plan and timeline for each identified area of noncompliance; and
8. whether each listed technology is governed by an existing City administrative policy, department policy, ordinance, contract term, intergovernmental agreement, or other written rule.

A. No current or future contract, subscription, memorandum, amendment, addendum, statement of work, renewal, extension, optional continuation, feature activation, integration, or Material Change involving surveillance technology may be renewed, extended, amended, expanded, continued beyond its current term, or newly activated unless it complies with this Ordinance.

B. If an existing contract term, technical architecture, or vendor practice prevents full compliance before the next renewal, extension, amendment, or optional continuation date, the City shall use best efforts to renegotiate the agreement into compliance at the earliest lawful opportunity and shall not exercise any discretionary renewal, extension, amendment, expansion, or optional continuation unless and until compliance is achieved.

C. Within one hundred eighty (180) days of the effective date of this Ordinance, each department using surveillance technology shall submit to City Council a compliance report identifying:

1. each surveillance technology, service, or data arrangement in use;
2. each provision of this Ordinance with which it currently complies;
3. each provision with which it does not currently comply;
4. whether each area of noncompliance is legal, contractual, technical, operational, or financial in nature;
5. the specific steps required to achieve compliance;
6. the date by which compliance will be achieved; or
7. if compliance cannot be achieved, whether the technology or service will be discontinued.

A. Any surveillance technology, service, or data arrangement that cannot be brought into substantial compliance with this Ordinance by the earlier of:

1. the next contract renewal, extension, amendment, or optional continuation date; or
2. twelve (12) months after the effective date of this Ordinance,

shall be discontinued unless City Council, after public notice, public hearing, and written findings, grants a temporary and narrowly tailored waiver for identified provisions and sets a final deadline for compliance.

A. No waiver under subsection F may authorize:

1. a use prohibited by Sections 9 or 10 of this Ordinance;
2. an unapproved Material Change;
3. a renewal or extension of a noncompliant contract without express City Council approval in a public meeting;
4. failure to provide required audits, logs, or public reporting; or

5. avoidance of the approval requirements of this Ordinance.

A. Nothing in this Section shall be construed to grandfather any surveillance technology, vendor, platform, or contract indefinitely. Existing use creates no vested right to continued use contrary to this Ordinance.

SECTION 37. RULES OF CONSTRUCTION.

A. This Ordinance shall be liberally construed to protect privacy, civil rights, civil liberties, and democratic accountability.

B. This Ordinance shall be construed to supplement applicable state and federal law to the maximum extent permitted.

C. If a specific provision of this Ordinance is preempted or otherwise invalid as applied to a particular technology, program, or circumstance, that determination shall be construed narrowly, and the remaining provisions of this Ordinance shall continue in full force and effect to the maximum extent permitted.

SECTION 38. SEVERABILITY.

If any section, subsection, sentence, clause, phrase, or application of this Ordinance is for any reason held invalid or unenforceable, such decision shall not affect the validity of the remaining portions or applications of this Ordinance.

SECTION 39. EFFECTIVE DATE.

A. This Ordinance takes effect on the thirtieth (30th) day after adoption.

B. All new acquisitions, pilots, subscriptions, deployments, renewals, extensions, amendments, addenda, feature activations, integrations, data-sharing arrangements, and Material Changes occurring on or after the effective date shall comply with this Ordinance.

C. Existing surveillance-technology programs, contracts, subscriptions, memoranda, amendments, addenda, and related arrangements shall comply in accordance with Section 36 of this Ordinance.

SECTION 40. CODIFICATION.

The provisions of this Ordinance shall be codified in the Bend Code and may be renumbered or reformatted by the City Recorder or codifier consistent with the intent of the City Council.