# Surveillance Technology Oversight Ordinance

*Proposed ordinance for Council consideration*

Note on placement: The following text is proposed for Chapter 2, Administration, as Article VII, sections 2-415 through 2-433. The City Clerk should confirm the placement and numbering before formal introduction. This note is not part of the proposed ordinance.

Be it ordained by the City Council of the City of Biddeford, as follows:

Chapter 2, Administration, of the Revised Code of Ordinances, City of Biddeford, Maine, is hereby amended by adding Article VII, Surveillance Technology Oversight, to read as follows:

## ARTICLE VII

## SURVEILLANCE TECHNOLOGY OVERSIGHT

### Sec. 2-415. Title; purpose; authority.

**(a)** This article shall be known as the Biddeford Surveillance Technology Oversight Ordinance.

**(b)** The purpose of this article is to ensure public deliberation before City surveillance technology is funded, acquired, or used; protect privacy, civil rights, and civil liberties; prevent discriminatory and viewpoint-based surveillance; and make compliance with law and Council-approved safeguards verifiable through records, independent review, and public reporting.

**(c)** This article is adopted under the Constitution of Maine, Article VIII, Part Second; 30-A M.R.S. § 3001; and the City Charter. It regulates the City's own activities and persons acting on its behalf. It does not confer authority on the City to engage in surveillance otherwise prohibited by law. A more protective local restriction applies where it is within municipal authority and does not conflict with controlling law.

**(d)** Council approval under this article is necessary but is not a warrant, authorization to violate confidentiality, appropriation, procurement award, or permission to disregard any independently applicable law. A department shall comply with all applicable requirements, including any stricter requirement governing a particular technology or data type.

### Sec. 2-416. Definitions; applicability.

The following words and terms, when used in this article, shall have the meanings set forth in this section:

**(a) City agency** means a City department, division, bureau, office, board, commission, or committee, and an officer, employee, volunteer, agent, contractor, or subcontractor acting on its behalf. Contractor obligations apply to services performed for the City, not to unrelated private conduct. The City Manager shall coordinate administration subject to the Mayor's Charter authority. References to an office include its lawfully appointed acting officer; a vacancy does not extend a deadline.

**(b) School Department** means the School Committee, Superintendent, and personnel acting under their educational authority. Notwithstanding subsection (a), acquisition and use controlled by these school officials under state law and Charter Article V are outside this article's Council-approval and administrative requirements. Equivalent protections may be addressed through a corresponding policy independently adopted by the School Committee or a lawful interdepartmental agreement. City agencies remain subject to this article when operating in schools, accessing school systems, or receiving or sharing school data. School participation does not authorize a City agency to evade this article. Applicable state surveillance and education privacy laws continue to apply to school officials independently of this article.

**(c) External entity** means a person or governmental or private organization outside the City agency or agencies expressly authorized for the technology. It includes another municipality, a county, regional, tribal, state, or federal agency, a task force, a fusion center, a vendor, and an information-sharing network.

**(d) Surveillance technology** means electronic hardware, software, a service, or a system capable of collecting, capturing, recording, retaining, processing, intercepting, analyzing, monitoring, or sharing audio, visual, digital, location, thermal, biometric, behavioral, or similar information or communications associated with, or capable of being associated with, a specific individual or group. It includes systems and vehicles equipped with such technology and access to technology or data operated by another entity.

**(1)** Examples include cell site simulators; automated license plate recognition systems; electronic toll readers; fixed, mobile, networked, and cloud-connected cameras; body-worn and vehicle cameras; facial, voice, iris, and gait recognition; mobile DNA capture; gunshot detection; x-ray imaging; surveillance-capable lighting; computer intrusion tools; social media monitoring; through-wall imaging; radio and wireless scanners; RFID readers; drones and ground vehicles carrying surveillance equipment; commercial location and mobility analytics, including products described as aggregated or de-identified; student or employee activity monitoring; and systems integrating surveillance data, tracking targets, generating investigative reports, or predicting criminal activity. Listing a technology does not authorize it.

**(2)** The term excludes the following only while they lack the described surveillance capabilities or are used solely in the limited manner stated: routine office hardware not used for surveillance; parking ticket devices without automated identification or tracking; manually operated, non-wearable handheld cameras and recorders not designed for surreptitious use and limited to manual capture and download; devices unable to record or transmit audio or video or be remotely accessed; City databases that contain no surveillance data; and manually operated internal communication systems not used for surreptitious monitoring. An exclusion does not extend to added surveillance software, integrations, analytical functions, or subsequent surveillance uses.

**(e) Surveillance data** means information collected, obtained, processed, or derived through surveillance technology, including query results and metadata. **Compliance records** means query and access logs, approval records, configuration histories, audit records, and records documenting retention, disclosure, deletion, complaints, and corrective action. Compliance records are subject to this article's safeguards and disclosure requirements; their retention shall be scheduled separately from underlying surveillance data. Copying scan content or personal data into a compliance record does not avoid a statutory retention limit or confidentiality requirement.

**(f) New surveillance technology** means technology not previously approved under this article, including a materially different capability or use. **Material change** includes expanded collection, coverage, quantity beyond an approved limit, analytical capability, purpose, user agency, recipient, retention, or privacy risk. A replacement or security update is not new if the City Manager documents that it remains within every approved limit and changes no surveillance capability or authorized use. A new vendor agreement still requires the review applicable under Section 2-418.

**(g) Query** means a search, lookup, request, retrieval, or review of surveillance data, including a search performed for another person, an automated alert or matching process, and access to live surveillance feeds. An approved policy may specify how to log continuous feeds or repeated automated processing as identified sessions or jobs, provided individual access and significant actions remain auditable.

**(h) Algorithmic identification or assessment** means a software output purporting to identify a person or vehicle, narrow possible identities, locate or classify an event, or predict or score a person's conduct or risk. It includes facial recognition leads, plate matches, gunshot detection outputs, and predictive scores.

**(i) Discriminatory** means disparate treatment because of an actual or perceived trait, characteristic, or status protected against discrimination by applicable federal, state, or City law, or association with a person having such a trait, characteristic, or status; or disparate impact on such persons. **Disparate impact** means a disproportionate adverse effect compared with similarly situated persons who do not have that trait, characteristic, or status.

**(j) Viewpoint-based** means targeting a person, community, group, or association because of activity protected by the First Amendment to the United States Constitution or Article I, Sections 3, 4, or 15 of the Constitution of Maine.

**(k) Lead agency** means the City agency designated in the approval order to maintain the technology, coordinate participating agencies, keep compliance records, and ensure compliance with this article and the approved policy. Before Council action, the City Manager shall designate a provisional lead agency for each proposed, existing, or emergency program; that designation assigns responsibility and does not authorize use. Every participating agency remains responsible for its own conduct.

### Sec. 2-417. Compliance with state law; verification.

**(a)** Automated license plate recognition. Operation and receipt or use of data shall be lawful under 29-A M.R.S. § 2117-A. Before approval, the lead agency shall identify the applicable statutory exception, permissible purposes, confidentiality requirements, and retention rules. For law enforcement scan data governed by subsection 5 of that statute, the agency shall:

**(1)** Configure deletion no later than 21 days after collection, or the shorter approved period, unless the particular data qualifies for the statutory exception for intelligence and investigative record information defined in 16 M.R.S. § 803(7).

**(2)** Document each decision to retain data under that exception, identifying each record, decision date, responsible official, investigation or intelligence reference, factual basis, and review date. A single document may cover multiple specifically identified records only if it establishes that the stated factual basis applies to every included record. A blanket designation of all scans as investigative information is prohibited. These documentation and review requirements are local safeguards.

**(3)** Obtain an annual vendor attestation and independently check system settings and deletion records, including copies held by processors and approved recipients. No contract, backup setting, or vendor default may extend a statutory retention limit. A claimed preservation obligation shall be evaluated by the City Solicitor against the specific statute; a generic legal hold is not an automatic exception to the 21-day limit.

**(4)** Report aggregate retention determinations, failures, corrective action, and verification results under Section 2-426. No publication under this article overrides the confidentiality of information collected or retained by law enforcement under § 2117-A(4).

**(b)** Facial surveillance. No City agency may obtain, retain, possess, access, use, or request a facial surveillance system or resulting information except as permitted by 25 M.R.S. § 6001 and authorized under this article. The policy shall identify the precise lawful pathway, required request and disclosure records, and restrictions on use of results. Council approval cannot create an additional statutory exception. Any contemplated system capability, including a disabled capability, shall be disclosed before procurement and may be acquired or retained only if lawful. A vendor's assurance that a prohibited capability is switched off is not sufficient to establish legality.

**(c)** Corroboration. As a local condition of City investigative activity, an algorithmic identification or assessment alone shall not support an investigative detention, search, arrest, or application for a warrant. The agency shall document corroborating evidence, the steps taken to verify the output, and the legal basis for the proposed action. Where probable cause is required, independent evidence developed without reliance on that identification or assessment shall itself establish probable cause. Repeating the output in a report or identification procedure does not create independent corroboration. This paragraph governs City conduct and does not purport to establish a court's evidentiary rule.

**(d)** Other requirements. Each proposal and annual report shall address applicable requirements for drones under 25 M.R.S. § 4501; tracking devices under 16 M.R.S. §§ 638-640; electronic communications under 16 M.R.S. §§ 641-646; location information under 16 M.R.S. §§ 647-650-B; employer surveillance under 26 M.R.S. § 620-A; criminal history and intelligence information under 16 M.R.S. chapters 7 and 9; and immigration-related activities under 5 M.R.S. chapter 337-E. This list is not exhaustive. A police drone acquisition requires the governing-body approval prescribed by state law even if a local exception would otherwise apply. Federal aviation, communications, privacy, and constitutional requirements remain applicable.

**(e)** Suspected crimes shall be referred promptly to the appropriate prosecutorial authority by the City Solicitor, using independent counsel where a conflict requires it. The public compliance report shall identify the fact and general status of a referral when lawful; it shall not disclose protected investigative or personnel information. This article creates no criminal offense and does not limit an existing state or federal offense.

### Sec. 2-418. Prior approval of City Council.

**(a)** Except for the limited transition in Section 2-420 and temporary emergency use in subsection (g), no City agency shall do any of the following without prior express Council approval following a public hearing:

**(1)** Seek, apply for, solicit, or accept funds or in-kind support for surveillance technology, including grants and donations.

**(2)** Acquire, borrow, lease, accept, install, or activate surveillance technology, including a free trial, pilot, demonstration, or evaluation using actual surveillance data, regardless of price or funding source.

**(3)** Use surveillance technology or data for a purpose, in a manner, or with a material change not previously approved, including an expanded sharing arrangement.

**(4)** Solicit proposals or enter into, materially amend, renew, or extend an agreement to acquire, share, or use surveillance technology or data, unless that specific action falls within an express, unexpired Council authorization.

**(5)** Accept access to surveillance technology or data operated by an external entity, whether access is direct, indirect, paid, or free.

**(b)** Publicly available product research and nonbinding requests for general information may precede approval if they involve no actual surveillance, transfer of nonpublic City data, commitment of funds, grant application, solicitation of acquisition proposals, or promise of future purchase. A demonstration may use synthetic data only. These activities create no right to subsequent approval.

**(c)** The lead agency shall submit the Section 2-419 documents through the City Manager to the City Clerk for public posting and referral under Section 2-429. The City Solicitor shall identify legal constraints, and the responsible financial and technical officers shall evaluate costs and security. An incomplete submission shall be identified promptly in writing and does not start a period reserved for a complete submission.

**(d)** The public hearing shall occur only after the complete Surveillance Impact Report and proposed Surveillance Use Policy have been continuously available on the City's designated website for at least 21 calendar days. Printed copies shall be available through the City Clerk. The hearing notice shall identify the technology, requested actions, location of the documents, and means of submitting oral, written, and electronic comments. Charter and Council Rules notice requirements also apply. A material revision expanding surveillance or reducing a safeguard requires a new 21-day posting period. The Council shall consider the public comments before deciding.

**(e)** Approval shall be by a written Council order identifying the lead and participating agencies, technology and version, approved documents, specific actions and uses, deployment and spending limits, recipients, conditions, and any expiration date. Mere inclusion in a budget, consent to a grant, or approval of a different technology does not constitute approval under this article. Approval to seek funding or solicit proposals may be limited to that stage; it does not authorize acquisition or use unless the order expressly does so. Final terms and material changes shall return for approval.

**(f)** The order shall follow applicable Charter and Council Rules procedures. Separate appropriation, bidding, contract, duration, and execution requirements remain in force, including Charter Article III, Section 8 and Council Rule 4(d), when applicable. Administrative implementation rests with the offices authorized by the Charter and Code. The Council may suspend or revoke authorization or require corrective conditions; an order cannot waive this article.

**(g)** Temporary emergency use. The Police Chief, Fire Chief, or other department head may authorize temporary access, borrowing, or use without prior approval only on specific documented facts establishing an imminent danger of death or serious bodily injury, where delay to obtain approval would materially increase that danger and an already authorized method is inadequate. The action shall be otherwise lawful and the least intrusive reasonably available means. The official shall notify the City Manager, Mayor, City Solicitor, and City Clerk as soon as practicable and within 24 hours, and file a public report within seven calendar days, subject to Section 2-427. The report shall describe the danger, technology, users, data collected and shared, legal authority, duration, costs, and disposition of data.

**(1)** Use shall end when the danger ends or 72 hours after it began, whichever occurs first. Continued use requires ordinary approval; successive emergency declarations for substantially the same facts may not restart the period. A declared state of emergency alone creates no exemption.

**(2)** This subsection does not authorize a prohibited technology or purpose, waive a warrant or statutory acquisition requirement, authorize a permanent purchase or long-term contract, or override spending authority. Sections 2-417, 2-422, 2-423, 2-425, 2-427, and 2-430 continue to apply. An emergency does not excuse logging; where immediate entry is impossible, the contemporaneous facts and actions shall be recorded as soon as practicable and within 24 hours.

**(3)** For technology lacking an approved policy, the authorizing official shall record the precise purpose, legal basis, users, minimum collection, recipients, safeguards, logging method, and lawful data disposition as emergency conditions. These conditions substitute only for the missing policy's operational specifications during the authorized emergency; they cannot relax any substantive restriction. Any impossibility of obtaining a vendor certification before immediate use shall be documented, reasonable controls verified before access, and verification completed as soon as practicable and within 24 hours or use shall cease.

### Sec. 2-419. Surveillance impact report; surveillance use policy.

**(a)** No acquisition or use may proceed under an approval unless the Council expressly approves both the Surveillance Impact Report and Surveillance Use Policy. Statements of proposed limits and safeguards in the approved documents are binding conditions. If the documents conflict, the more protective lawful limit governs until the Council resolves the conflict. A confidential supplement may be supplied only as Section 2-427 permits; it cannot substitute for a meaningful public description of the proposed program.

**(b)** The Surveillance Impact Report shall include:

**(1)** The technology, vendor, operation, all capabilities including disabled functions, integrations, proposed users, and data sources.

**(2)** The specific public purpose, evidence of need and expected effectiveness, performance and error measures, less intrusive alternatives, and reasons alternatives would be inadequate.

**(3)** Proposed deployment locations, quantity and coverage; selection criteria where deployment is not uniform; and foreseeable impacts on affected communities.

**(4)** Acquisition, implementation, subscription, maintenance, storage, training, staffing, auditing, replacement, and termination costs over the proposed term; funding sources and conditions; and any financial incentive linked to use, enforcement, data, fines, or recoveries.

**(5)** Potential civil rights, privacy, and civil liberties harms, including disparate impacts and impacts on protected activity, and specific affirmative measures to prevent them.

**(6)** Applicable legal authority and restrictions; the records-retention schedule and data categories proposed; and how the program will satisfy Sections 2-417, 2-423, 2-424, 2-425, and 2-427.

**(7)** Documented misuse, errors, breaches, and unauthorized access involving the technology or vendor during the preceding three years, sources reasonably reviewed, limits of the available evidence, and preventive measures proposed for Biddeford. A lack of available information is not proof of a lack of risk.

**(c)** The Surveillance Use Policy shall state:

**(1)** The purposes, permitted and prohibited capabilities and uses, legal standards for each use, deployment limits, and rules for analyzing and reviewing data.

**(2)** Data collected and generated, expected incidental collection, measures to minimize collection, and lawful methods and deadlines for segregating and disposing of unnecessary data.

**(3)** Encryption, individual credentials, access permissions, training, supervision, suspension of access, cybersecurity controls, and breach response.

**(4)** A record-type-specific retention and disposal plan approved for legal sufficiency by the City Solicitor and records officer. Each period shall be the shortest lawful period necessary for the authorized purpose, consistent with applicable minimum retention requirements, maximum retention limits, and specifically applicable preservation duties. The plan shall separate active operational access from restricted preservation and shall address backups, derived data, compliance records, deletion verification, and periodic review of exceptions. No City policy may shorten an applicable mandatory minimum or extend an applicable statutory maximum.

**(5)** Every authorized recipient or precisely defined class of recipients, with separate identification of any federal or out-of-state governmental arrangement; the necessity and permitted purpose of disclosure; data and access limits; legal standards; recipient obligations; onward disclosure restrictions; and the process for approving later changes under Section 2-418. A class authorization may not conceal unlimited network-wide access.

**(6)** Handling of compulsory demands, emergency disclosures, and requests by data subjects, including review, logging, notice, and available remedies.

**(7)** Logging and quarterly audits under Section 2-422; review by persons independent of the operating program; performance and equity measures; and enforceable corrective actions.

**(8)** A public complaint and question process, accessible contact information, the response deadlines in Section 2-430, and procedures for notices of misuse.

**(9)** Training required before access and at least annually thereafter; configuration verification; deactivation and exit arrangements; the lead agency; and each participating agency's responsibilities.

### Sec. 2-420. Existing surveillance technology; transition.

**(a)** Within 60 calendar days after this article takes effect, the City Manager shall publish an inventory of every City agency's surveillance technology, access arrangement, pilot, and pending acquisition, including vendor, functions, acquisition date, responsible agency, funding, annual cost, data and retention settings, agreements, renewal and termination dates, authorized users, and external access and sharing. Each agency head shall certify the agency's submission, including a report of no technology when applicable. Disclosure is subject to Section 2-427; any withheld item shall be described as fully as law permits.

**(b)** An agency seeking to continue a use, data-intake practice, or sharing arrangement actually in operation before the effective date shall submit complete Section 2-419 documents within 120 calendar days after the effective date. Failure to submit by that deadline requires cessation at that time. If approval has not been granted within 180 calendar days after a timely complete submission, and in all events by day 300 after the effective date, the agency shall cease use and sharing until approval is obtained. Filing a replacement submission does not restart a deadline. A pending purchase, unused license, or signed agreement is not an existing use.

**(c)** Temporary continuation under subsection (b) shall be limited to the preexisting scope and shall not constitute permanent authorization or approval by the City Council. State and federal law, Section 2-423(f)'s prohibited purposes, Section 2-425, and Section 2-430's nonretaliation and preservation duties apply immediately. Existing agencies shall implement Sections 2-422 and 2-427 within 60 days, using secure supplemental logs if needed, and Sections 2-423(a)-(e) within 60 days through a publicly posted interim operating and sharing policy. The City Manager shall approve the interim policy after legal review; it shall specify users, purposes, justification categories, logging, retention, audits, and lawful preexisting sharing arrangements within this article's limits. For temporary continuation only, these specifications fulfill references to an approved policy in Sections 2-422 and 2-423. No new recipient or expanded access may be added without Section 2-418 approval. An agency unable to comply by the applicable deadline shall stop the affected use. New uses shall comply in full before they begin.

**(d)** Existing contracts shall be reviewed within 60 days. The City shall seek amendments needed for compliance and shall exercise lawful termination or nonrenewal rights where compliance cannot be achieved. A preexisting contractual obligation may affect payment or termination duties but does not itself authorize surveillance use beyond this section's deadlines or contrary to law. New contracts, renewals, and material amendments are governed by Section 2-424.

**(e)** Existing and discontinued programs shall report their activity under Section 2-426, including activity during the transition. The City Clerk shall maintain a public schedule of submission and cessation deadlines. An office vacancy or lack of a committee recommendation does not extend a deadline.

### Sec. 2-421. Standards for approval; duration.

**(a)** The Council shall approve a request only upon written findings, supported by the submitted record and public input, that the demonstrated benefits outweigh the full costs; that less intrusive alternatives have been considered; that civil rights and civil liberties will be safeguarded; and that authorized uses and deployments will neither be discriminatory or viewpoint-based nor have a disparate impact on a community or group. The City Council shall deny the request or require further revision if the required findings cannot be made.

**(b)** Identification of a risk is not consent to its occurrence. Approval shall specify affirmative safeguards, measurable performance and equity criteria, and corrective conditions. It may be time-limited or limited to a pilot meeting all requirements of this article.

**(c)** The approved report, policy, findings, orders, and subsequent revisions shall remain publicly available throughout use and thereafter under applicable retention requirements, subject to Section 2-427. Approval remains subject to annual review, suspension, and revocation; it grants no vested right to continued use or future funding.

### Sec. 2-422. Conditions of operation.

**(a)** Each query shall be linked to a case, incident, missing-person matter, or another uniquely identified authorized task. Every human-directed query shall record a meaningful written reason and an approved justification category at the time of access. Categories may include authorized noninvestigative activities, such as safety response, maintenance, auditing, or a records request, and shall be specific enough to permit meaningful review. Generic entries such as investigation or official use, standing alone, are insufficient. Free text supplements and does not replace the category. A specific task description may populate the written reason if the user confirms its accuracy for the particular query.

**(b)** The approved policy shall define logging for automated processing and continuous feeds, identifying the authorized job or session, purpose, configuration, responsible operator, start and end times, data sources, alerts, and subsequent human access. Routine operation may not be relabeled automated to conceal individual queries.

**(c)** Each lead agency shall conduct and document an audit at least quarterly. The review shall test case or task linkage, authorization, justification, repeat searches, anomalous hours or volumes, inactive accounts, external and proxy queries, sharing settings, retention exceptions, and deletion. The annual independent review under Section 2-429 shall evaluate these results and a sample of underlying compliance records. Reports shall identify limitations and corrective actions, including a finding that no violation was detected when that is the result.

**(d)** Access shall use individual credentials and least-privilege permissions. Shared credentials are prohibited. Automated service accounts shall be uniquely identified, restricted to an approved job, assigned to a responsible custodian, and logged. No user may perform a query for a person or purpose that could not lawfully receive the information under the approved policy. An external request does not supply an independent basis for City access. External and proxy queries remain subject to Section 2-423.

**(e)** Before activation and at least quarterly, the lead agency shall obtain a written vendor certification of actual retention, deletion, access, sharing, and secondary-use settings and independently verify them through available technical records and tests. A vendor certification alone is insufficient. For a City-built system with no vendor, an independent qualified City technical officer shall certify the settings. Only an authorized City official may approve a change to a surveillance setting, within the approved policy; the change shall be logged. Contracts shall prohibit unilateral vendor changes to these settings. Any discrepancy shall be reported to the City Manager and Council within seven calendar days of discovery.

A setting that expands surveillance or access beyond approval shall be disabled promptly. If a required control cannot be verified or maintained, the affected operation shall be suspended.

**(f)** Upon a substantiated finding of unauthorized collection, access, use, or disclosure, the agency shall notify each affected person whose identity and contact information are reasonably ascertainable, without collecting unnecessary additional personal information, as soon as practicable and within 30 calendar days. The notice shall describe the event, affected information, corrective steps, and complaint and review routes. Earlier notices required by law remain required.

**(1)** The City Solicitor may delay notice only on a written, particularized determination that notice is prohibited by law or would create a specific risk to an active investigation or a person's safety. The justification shall be reviewed every 30 days; notice shall issue within 30 days after the ground ends. Confidentiality required by law may continue while legally necessary. The public report shall disclose lawful aggregate information about delayed notices.

**(2)** Failure to identify an affected person does not excuse corrective action, records preservation, or reporting. Notice of a suspected data-security breach shall also comply with independently applicable law.

### Sec. 2-423. Sharing of data; access by outside entities.

**(a)** Voluntary disclosure, receipt, shared-system access, and proxy queries require express authorization in the Council-approved policy, except for temporary existing arrangements under Section 2-420 and the limited temporary emergency authorization under Section 2-418(g) or subsection (h). Legally compelled disclosures are governed by subsection (g). Default access shall be off. The policy shall identify why sharing is necessary and the minimum data needed. A vendor's standard network membership or an external agency's request is not authorization.

**(b)** A federal or out-of-state governmental sharing arrangement requires express Council approval identifying the particular agency and arrangement. This requirement does not create an exemption for Maine recipients, who remain subject to subsection (a). Compelled disclosures under subsection (g) and emergency disclosures under subsection (h) are limited exceptions to advance Council approval, not general authorizations for continuing access.

**(c)** Approved sharing shall require the collection, maintenance, and dissemination of criminal intelligence information about individuals to conform to the principles of 28 C.F.R. Part 23, including a documented reasonable suspicion of involvement in criminal activity and relevance of the information to that activity. As a local requirement, these safeguards apply to City criminal intelligence sharing whether or not federal funding independently makes Part 23 applicable. They shall not be interpreted to authorize bulk retention or to classify all administrative, emergency, or evidentiary records as criminal intelligence. Other data remain subject to their particular legal rules and approved limits.

**(d)** Before voluntary access or disclosure, the recipient shall agree in writing to the approved purposes, confidentiality, access and retention limits, audit cooperation, notice of legal demands and breaches to the extent lawful, and no onward disclosure to unauthorized recipients. The City shall suspend access upon a material breach, seek return or lawful deletion, and report corrective action. A processor may act only as Section 2-424 permits. Public disclosure required by law and legally protected access by a data subject are governed by Section 2-427, not an agreement to restrict those rights.

**(e)** Each disclosure and external access shall be logged with the date, recipient entity and authorized individual, data or query, requesting entity, purpose, and legal basis. Public reporting shall protect personal identifiers and confidential content. The City shall require records of external queries against City data and shall disable access that cannot be audited.

**(f)** City resources, surveillance data, and proxy queries shall not be used voluntarily for civil immigration enforcement; to identify or track a person because of protected expression, association, religion, or petition; or to investigate or support enforcement against conduct that is lawful under Maine law. This last restriction concerns targeting the lawful conduct itself; it does not bar investigating a distinct violation of Maine law merely because the investigation incidentally involves lawful activity, or an approved missing-person, rescue, or nonpunitive administrative service that does not target lawful conduct for enforcement. No Council order may authorize these prohibited purposes. All applicable duties under 5 M.R.S. chapter 337-E remain in force. This subsection does not prohibit communication of citizenship or immigration-status information to the extent a restriction on that communication is precluded by controlling federal law, including 8 U.S.C. §§ 1373 and 1644. This limited savings provision does not authorize disclosure of location, addresses, query histories, or other surveillance data beyond what controlling law requires or protects from restriction.

**(g)** Compulsory process. Upon a demand asserted to be legally compulsory, the City Solicitor shall determine its validity, scope, confidentiality, and available grounds for objection or a protective order. The City shall comply only to the legally required extent and shall use available lawful means to prevent disclosure prohibited by law. A subpoena, administrative request, or warrant is not automatically authority for unrestricted system access. The demand, determination, information disclosed, and any notice restriction shall be logged. Ordinary Council approval is not required for a disclosure legally compelled after that review; legal process does not authorize new voluntary collection or a continuing sharing arrangement.

**(h)** Emergency disclosure. The responsible department head may authorize otherwise lawful disclosure of the minimum information necessary to address an imminent danger of death or serious bodily injury where delay would materially increase the danger. The Section 2-418(g) documentation, notification, seven-day report, and duration requirements apply. If obtaining the written recipient agreement required by subsection (d) first is impracticable without materially increasing the danger, the official shall document why, communicate available purpose and onward-disclosure restrictions, and seek written confirmation promptly. This exception does not authorize continuing access without an agreement. It waives only prior Council approval and the impracticable timing of that local agreement for the particular disclosure; it does not waive statutory confidentiality, other controlling requirements, or the prohibitions in subsection (f).

### Sec. 2-424. Procurement; contracts.

**(a)** Every new, renewed, or materially amended agreement for surveillance technology or data shall:

**(1)** Require compliance with this article and the approved policy by the contractor and its subcontractors; identify all processors and approved storage locations; and permit only City-authorized purposes and access.

**(2)** Apply Maine law to the extent legally permissible and require disputes to be heard in a state court in Maine or, where federal jurisdiction applies, a federal court in Maine. It shall not require an out-of-state forum or displace mandatory public-law obligations through private dispute terms.

**(3)** Preserve the City's ability to disclose the agreement, technology, capabilities, policies, and activities as required by law and this article. It shall create no contractual secrecy exception and shall recognize statutory confidentiality. Vendor consent shall not be a condition of compliance with a lawful disclosure duty.

**(4)** Recognize City custody or control of its surveillance data and compliance records; provide timely, complete, machine-readable access without additional export charges; preserve usable copies on termination; and permit verification of settings, access, retention, deletion, and security.

**(5)** Permit vendor processing and necessary storage only to perform the specifically authorized City service. It shall prohibit independent retention, sale, licensing, advertising, profiling, product development, or model training using City data or derivatives, including aggregated or de-identified derivatives. Processing shall not confer an independent right to exploit data. Subprocessors shall have equivalent obligations.

**(6)** Specify prompt breach and legal-demand notice to the extent lawful, investigation and audit cooperation, remediation, and suspension of access. It shall include the certification and verification requirements of Section 2-422(e).

**(7)** Provide return or transfer of required records followed by verified lawful deletion of remaining vendor and subprocessor copies on termination or the applicable retention deadline, whichever comes first where legally required. A specifically applicable preservation duty shall be documented and copies restricted; no general backup exception may override a statutory limit.

**(8)** Permit termination for convenience on no more than 30 days' notice without early termination penalty, and immediate suspension or termination for material illegality or breach. Payment for authorized services already delivered is not an early termination penalty. Any claimed unavoidable payment shall be disclosed in the impact report before approval.

**(b)** No City agency may agree to terms inconsistent with this article. The City shall not rely on a conflicting provision to avoid its public duties and shall assert invalidity or unenforceability where supported by law. Existing agreements shall be addressed through Section 2-420(d), negotiation, and lawful termination; this article does not itself adjudicate a third party's vested contract rights or authorize breach of controlling law.

### Sec. 2-425. Prohibited technologies and uses.

**(a)** No City agency may acquire, possess, borrow, access, or use:

**(1)** Facial surveillance or automated license plate recognition except through the applicable statutory permissions and the approval or limited temporary authorization applicable under Section 2-418 or 2-420. No local temporary authorization replaces a statutory acquisition, possession, or use requirement.

**(2)** A predictive policing system that lists, scores, or ranks individuals based on a prediction of future criminal conduct. Place-based analytics remain subject to ordinary review and may not be used as a proxy for a prohibited person-based program.

**(3)** A tool for computer intrusion or interception of communication contents in an investigation without a warrant from a court of competent jurisdiction and all other authority required by law. A warrant alone does not authorize conduct outside its scope or otherwise prohibited by law. Routine defensive administration of City systems, without investigative surveillance of persons, is not computer intrusion for this paragraph.

**(4)** Surveillance data from a commercial data broker where direct acquisition of the same data would require a warrant, court order, or subpoena. This is a local prohibition on the commercial acquisition route and is not an exception to Section 2-431's broader prohibition on paid private surveillance data.

**(b)** No City agency shall use surveillance technology or data in a discriminatory or viewpoint-based manner or contrary to constitutional rights. A security or investigative purpose does not by itself justify targeting protected activity. Neither a vendor label nor an external agency's participation changes these prohibitions.

### Sec. 2-426. Annual agency reports; review.

**(a)** Each lead agency shall publish an Annual Surveillance Report for each technology, including existing, suspended, or discontinued programs, by March 15 for the preceding calendar year. Publication shall be accompanied by simultaneous filing with the City Clerk, Council, and oversight body; the Clerk shall record the referral date. The first report following approval shall be due on the earlier of that March 15 or the first anniversary of approval; an anniversary report shall cover the period since approval, and the next March 15 report shall clearly identify any overlapping period. No period of operation may be omitted. A report of no use is required when an authorization exists but the technology was not used.

**(b)** The report shall include actual uses and deployments; query and access totals by justification, unit, and City or external initiation; automated processing and alert counts separately from human queries; data received and shared, recipient organizations, types, legal standards, and purposes; census-tract deployment information where applicable; retention exception counts and deletion verification; complaints and responses; all quarterly audit findings and corrective actions; misuse notices and lawful reasons for delay; subject-access requests and outcomes; violations and referrals; error and false-identification counts alongside arrests, charges, and clearances to which the technology contributed; civil rights and disparate-impact analysis; and full annual costs and proposed funding. The agency shall explain measures and limitations and shall not present a correlation as proof that the technology caused an outcome. Missing information and failures to maintain required records shall be expressly disclosed.

**(c)** Personal identities shall not be included in public reporting merely because individuals received or supplied information. Aggregation and redaction shall follow Section 2-427. The agency shall not collect new protected-trait or identity data solely for this report where less intrusive existing information or voluntary, appropriately protected community input can support the assessment.

**(d)** Within 30 days after publication, the lead agency shall hold at least one well-publicized, accessible community meeting to discuss the report, answer questions, and receive comments. A combined meeting is permitted if every program can be meaningfully addressed. Written and electronic input shall also be accepted and forwarded for oversight review.

**(e)** For a program approved under Section 2-418, within 90 days after each report is due, the Council shall determine in public, using the Section 2-421 standard, whether to continue authorization, impose corrective conditions, suspend use, or discontinue it. A continuation decision shall follow the subsection (d) community meeting and consideration of its comments, and receipt of the oversight recommendation or expiration of the Section 2-429(b) review period. Protective suspension or reduction need not await those steps. Increased surveillance authority requires Section 2-418 review; a reduction or suspension does not. The Council may not treat the absence of a report as evidence of compliance. If a required report is more than 30 days overdue, or the Council has not completed review within the 90-day period, authorization is suspended until the missing report and review are completed. Programs operating solely under Section 2-420 remain subject to annual reporting and the initial approval and cessation deadlines in Section 2-420; an annual report or review does not extend those deadlines. Section 2-418(g) remains the only emergency exception.

### Sec. 2-427. Public records; audits; publication; individual access.

**(a)** Within 30 days after the end of each calendar quarter, the lead agency shall publish a machine-readable log of queries and access, including date and time, responsible agency and unit, approved justification category, case or task reference where lawful, external requesting or recipient entity, and whether the entry concerns human or automated activity. Subject identities, plates, device identifiers, query terms that identify persons, and result content shall not be proactively published.

**(b)** All publication and access duties are subject to controlling confidentiality law, including 29-A M.R.S. § 2117-A(4), 16 M.R.S. chapters 7 and 9, applicable personnel, juvenile, education, and health confidentiality, and the Maine Freedom of Access Act. The records custodian, with legal review where needed, shall separate nonconfidential information and disclose it. When even the existence, timing, or number of particular entries is protected, the public release shall use a lawful aggregate description instead. Otherwise, each withholding shall identify its specific legal basis and the number of entries or fields withheld. A generalized claim of operational sensitivity or vendor confidentiality is insufficient.

**(c)** Nothing in this article restricts access available under 1 M.R.S. §§ 401-414 or other law, changes statutory response or appeal periods, or creates a new exemption. Public-records requests shall be processed under the applicable law, even if the records are also included in an annual or quarterly publication.

**(d)** A person may request existing query records concerning an identifier associated with that person during the period requested. The agency may require proportionate proof of identity and connection to that identifier for nonpublic subject-access treatment; such proof is not a condition of an ordinary request for public records. It shall disclose information that can lawfully be disclosed to the requester without violating another person's rights or a confidentiality requirement. Identity proof alone does not overcome statutory confidentiality.

**(1)** The agency shall acknowledge the request within five working days and respond or state the lawful reason further time is needed within 30 calendar days after receipt of sufficient identifying information. For a request governed by the Freedom of Access Act, its procedures and time limits control. Any denial or redaction shall identify the specific authority and available review route, with as much explanation as law permits. No disclosure is promised where law prohibits it.

**(2)** The agency shall permit administrative review by a records officer or City Solicitor not implicated in the complaint, without making that review a prerequisite to a statutory remedy. A ground based on a temporary investigation shall be reconsidered at least every 30 days while the request remains pending. A statutory confidentiality requirement may continue as long as the law requires.

**(e)** Oversight membership does not create access to confidential information. The City Solicitor shall identify the lawful basis and safeguards before any nonpublic disclosure to a reviewer. Where lawful access cannot be provided, a qualified independent person who may lawfully inspect the material shall report nonconfidential findings and limitations. Executive session may be used only under an applicable provision of 1 M.R.S. § 405; votes and final actions shall occur in public as required by law.

## Sec. 2-428. Annual report of City Council.

By April 15 each year, the City Clerk, for the Council, shall publish in print and online a report of the preceding calendar year's requests, approvals, denials, required modifications, pending matters, emergency uses, and missed deadlines. It shall include or link to all Section 2-426 reports and identify reports not submitted. Printed copies may contain specific online references. The Clerk shall update the public register after Council annual-review decisions and after the Section 2-429 equity assessment so the April report is not mistaken for a completed review of later decisions.

## Sec. 2-429. Oversight; community equity assessment.

**(a)** Unless and until an ordinance assigns these functions to an existing or newly created advisory body, the full City Council shall perform the oversight duties in this section. Preliminary oversight discussion and final approval shall be distinct agenda items, with a written record of findings and public input. The duties prescribed by this section shall apply without further designation by the City Council. A change in oversight structure requires an ordinance consistent with Charter Article X, Section 8 and does not alter prior authorizations or pending deadlines.

**(b)** The oversight body shall review each proposal and annual report, solicit community input, recommend approval, denial, limits, or corrective action, and monitor compliance. It shall provide a written recommendation within 45 days after referral of a complete proposal or annual report. When the Council itself performs oversight, its written preliminary findings fulfill this recommendation requirement. The Council may proceed after that period if no recommendation is available, documenting the missing review; the 21-day public-posting requirement and all other deadlines remain applicable.

**(c)** By September 15 each year, beginning in the first calendar year after this article takes effect, the oversight body shall publish and submit a Community Equity Impact Assessment and Policy Guidance. It shall identify communities experiencing or perceiving disproportionate surveillance and resulting harms; evaluate agency findings and residents' experience; recommend changes to laws, approvals, and policies; identify resources, implementation responsibilities, and accountability needed for each change; and advise how future proposals should be reviewed. The assessment shall be developed through public meetings, written and electronic comments, and outreach to communities historically subject to disproportionate surveillance. It is separate from the operating agency's self-assessment.

**(d)** An officer, employee, or contractor responsible for operating a reviewed program may provide information but shall not vote on its advisory review or serve as its independent auditor. Other conflicts shall be disclosed and handled under applicable law and City rules. This section does not alter Charter voting rights of Council members. The City Manager shall provide administrative support; departments under review shall not control the conclusions of the oversight body.

**(e)** The Council shall arrange an annual independent compliance review by a qualified City officer outside the operating program or an outside reviewer, within appropriated resources. The reviewer shall examine a documented sample of approvals, queries, sharing, retention exceptions, settings, and corrective actions, consistent with Section 2-427(e), and report findings in time for the annual Council review. Lack of resources shall be reported to the Council with an estimate of the work and appropriation needed; it shall not be reported as a finding of compliance or excuse a statutory duty.

### Sec. 2-430. Enforcement; remedies; protected disclosures.

**(a)** A person whose legally protected interests are adversely affected by a violation may seek declaratory or prospective injunctive relief to enforce this article in a court of competent jurisdiction, to the extent authorized by municipal home rule and applicable law. This subsection expressly provides a local compliance remedy to that extent. It does not dispense with standing, jurisdiction, procedural requirements, applicable immunities, or rules governing review of municipal action. Existing statutory, constitutional, and other lawful remedies remain available. No tort damages remedy or court rule of evidence is created by this article.

**(b)** In an action authorized by subsection (a), a prevailing plaintiff is entitled to reasonable costs and attorneys' fees against the City to the extent the City may lawfully provide that remedy. This provision does not expand a court's jurisdiction or override controlling limitations on such an award. The City shall not seek fees solely because a good-faith claim was unsuccessful. The remedies in this subsection and subsection (a) are severable from each other and from the rest of this article.

**(c)** Any person may submit a complaint to the City Clerk, City Manager, or City Solicitor without first proving personal injury. The City Clerk shall provide a secure submission route, explain that confidentiality is protected only as provided by law, and forward the complaint for impartial review. Receipt shall be acknowledged within five working days. A written disposition or explanation of further investigation shall issue within 30 calendar days, with updates every 30 days while pending. A complaint involving an assigned reviewer shall be referred to an unconflicted official or additional counsel engaged by the Council under Code Section 2-74. Records shall be preserved and public findings shall be redacted as law requires. An administrative complaint is not a prerequisite to an otherwise available court or statutory remedy.

**(d)** The City Solicitor is responsible for pursuing appropriate ordinance enforcement under Code Section 2-67, including injunctive relief and recovery of civil penalties. A person acting for a City agency who knowingly violates this article commits a civil violation for which a penalty of $100 to $2,500 may be adjudged. Each distinct unlawful acquisition, deployment, query, or disclosure is a violation; the same act shall not be counted repeatedly solely because it violates multiple provisions. Penalties accrue to the City under 30-A M.R.S. § 3001(4). This is the specific penalty for this article in place of the general penalty in Code Section 1-12. Nothing authorizes private collection of that penalty or displaces an applicable immunity.

**(e)** Upon credible evidence of ongoing unlawful use or a material failure of an approved safeguard, the responsible department head or City Manager shall promptly suspend the affected access or operation pending review, preserving required records. The Council may direct suspension, corrective conditions, or revocation. Employee discipline may include termination, subject to the Charter, Code, due process, personnel rules, and collective bargaining agreements. Contract remedies remain available against vendors.

**(f)** No City agency or person acting for it shall retaliate against an employee or applicant for making, preparing to make, being perceived as making, or assisting a lawful, good-faith disclosure of a suspected violation to a City official, oversight body, prosecutor, or other appropriate authority. Prohibited retaliation includes adverse personnel action and threats affecting employment, compensation, access needed for assigned duties, or lawful process. This protection supplements the Maine Whistleblowers' Protection Act, 26 M.R.S. §§ 831-840, and other applicable protections. It does not authorize unlawful public disclosure of confidential information.

**(g)** Data obtained in violation. Upon discovery of surveillance data collected or derived in violation of this article, the agency shall immediately stop operational use and voluntary dissemination, restrict access, preserve compliance evidence, and notify the City Solicitor and records officer. It shall identify affected copies and recipients and seek equivalent restrictions. The City shall not voluntarily offer the data against a member of the public, except as evidence of a violation of this article.

**(1)** The City Solicitor and records officer shall document obligations under 5 M.R.S. § 95-B, applicable State Archivist schedules, specific technology statutes, court process, pending records requests, litigation preservation, and criminal discovery, including potentially exculpatory material. Relevant material shall be supplied to prosecuting or defense counsel or a court as legally required through lawful procedures. A copy furnished to a defendant does not by itself terminate all preservation duties.

**(2)** Records whose preservation is legally required shall be segregated and accessible only for the identified legal purpose. The duty and continuing need shall be reviewed at least quarterly. Other unlawfully collected data shall be destroyed promptly once lawful disposition is established, including authorized processor copies. Section 2-417(a)'s specific ALPR requirements control the treatment of ALPR data; this subsection does not establish a blanket exception to them.

**(3)** Disposal, preservation, recipient notifications, and any legally compelled disclosure shall be documented without unnecessarily duplicating sensitive data. Compliance records sufficient to investigate misconduct shall be retained under their applicable schedule. The public annual report shall state lawful aggregate results. Courts and prosecutors outside the City's control retain their own lawful authority over evidence and proceedings.

### Sec. 2-431. Purchase of private surveillance data; monetization.

**(a)** The City and its agencies shall not enter into an agreement that directly or indirectly facilitates the purchase or receipt of privately generated and owned surveillance data, or the sale, licensing, or provision of City surveillance data to a nongovernmental entity, in exchange for money or other consideration supplied by any person or from any source. Consideration includes discounts, free services, and fees, interest, or surcharges imposed on unpaid fines or debts. An intermediary or sponsor paying for City access does not avoid this prohibition. Revenue-sharing surveillance or enforcement arrangements are prohibited. A Council approval cannot waive this section.

**(b)** A fixed or usage-based fee for equipment or a processor's strictly limited service under Section 2-424 is not prohibited consideration if the data are collected exclusively on the City's behalf for an approved purpose, remain under City control, and confer no independent data rights on the provider. This exception does not permit the purchase of an existing private database or private surveillance feed, barter for access to a private camera network, or vendor monetization of City data. A vendor's description of a data purchase as a service does not control.

**(c)** Voluntary provision of a particular recording by a witness or victim without consideration is not prohibited by this section. Receipt and use require an approved policy governing such intake, or a limited authorization under Section 2-418(g) or 2-420. The Council may approve a standing intake policy identifying lawful categories of isolated recordings without voting on each individual submission. The policy shall not authorize requested future surveillance, recurring feeds, automated integration, or continuing access unless separately reviewed and expressly approved under Section 2-418. Agreements predating this article that violate this section shall be terminated as soon as legally permissible; Section 2-420 governs any temporary continuation and does not authorize conduct prohibited by law.

### Sec. 2-432. Severability; construction.

If any provision or application of this article is held invalid, the remaining provisions and applications shall remain in effect to the extent they can operate lawfully. Mandatory confidentiality, court orders, and other controlling law shall be observed only to the extent actually applicable; a claim of conflict shall not be used to avoid unrelated duties. Statutory references include amendments and successor provisions applicable to the conduct at issue.

### Sec. 2-433. Effective date; administration.

This ordinance shall take effect 30 days after passage in accordance with Charter Article III, Section 8. The City Manager, City Clerk, and City Solicitor may prepare forms, inventories, training, and implementation materials between passage and the effective date, within existing lawful authority and appropriations. Administrative guidance may implement but may not waive, enlarge, or reduce this article's requirements. The City Clerk shall record the dates of passage and effectiveness and maintain the public register required by this article.

The City Clerk and codifier may conform article and section numbering, internal references, and formatting before codification, provided that no substantive change is made. Substantive amendments remain for Council action.