# Article 10: Transparent and Responsible Use of Surveillance Technology

*("Transparent and Responsible Use of Surveillance Technology" added 8-10-2022 by O-21514 N.S; effective 9-9-2022.)*

## Division 1: Approval Process for Use of Surveillance Technology

*("Approval Process for Use of Surveillance Technology" added 8-10-2022 by O-21514 N.S; effective 9-9-2022.)*

### §210.0101 Purpose and Intent

The Transparent and Responsible Use of Surveillance Technology ("TRUST") Ordinance requires an informed public and transparent discussion related to the *City's* acquisition and use of *surveillance technology*, as defined by this Division. The City Council finds that while *surveillance technology* is critical to managing and providing *City* services and protecting public safety, it can also be used to infringe upon the civil rights and civil liberties of members of the public. The City Council intends to balance these interests by determining through a public process that (1) the benefits to the community of the *City's* acquisition and use of the *surveillance technology* outweigh the costs, (2) the proposed use of the *surveillance technology* will safeguard civil rights and civil liberties, and (3) based on the facts and information presented to the City Council, there is no effective alternative to the proposed *surveillance technology* that provides a lesser financial cost to the *City* and impact on civil rights or civil liberties. If the City Council determines that the proposed use of the *surveillance technology* meets the standard set forth in this Division, then the City Council may authorize the use of the *surveillance technology* by adopting a legally enforceable *Surveillance Use Policy*.

*("Purpose and Intent" added 2-14-2024 by O-21762 N.S.; effective 3-15-2024. Former Section 210.0101 "Definitions" amended and renumbered to Section 210.0102.)*

## §210.0102 Definitions

For purposes of this Division, the following definitions apply and appear in italicized letters:

(a) *Annual Surveillance Report* means a written report concerning specific *surveillance technology* that includes all of the following elements:

(1) A description of how the *surveillance technology* was used, including the type and quantity of data gathered or analyzed by the *surveillance technology*.

(2) Whether and how often data acquired through the use of the *surveillance technology* was shared with any non-*City* entities, the name of any recipient entity, the types of data disclosed, under what legal standards the information was disclosed, and the justification for the disclosure, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the *City*.

(3) A description of the physical objects to which the *surveillance technology* hardware was installed, if applicable, and without revealing the specific location of the hardware, and a breakdown of the data sources applied or related to the *surveillance technology* software.

(4) A list of the software updates, hardware upgrades, and system configuration changes that expanded or reduced the *surveillance technology* capabilities, as well as a description of the reason for the changes, except that no confidential or sensitive information should be disclosed that would violate any applicable law or undermine the legitimate security interests of the *City*.

(5) A description of where the *surveillance technology* was deployed geographically, by each City Council District or *police area*, in the applicable year.

(6) A summary of any community complaints or concerns about the *surveillance technology* and an analysis of its *Surveillance Use Policy*, including whether it is adequate in protecting civil rights and civil liberties, and whether, and to what extent, the use of the *surveillance technology* disproportionately impacts certain groups or *individuals*.

(7) The results of any internal audits or internal investigations relating to *surveillance technology*, information about any violation of the *Surveillance Use Policy*, and any action taken in response. To the extent that the public release of this information is prohibited by law, *City staff* shall provide a confidential report to the City Council regarding this information to the extent allowed by law.

(8) Information about any data breaches or other unauthorized access to the data collected by the *surveillance technology*, including information about the scope of the breach and the actions taken in response, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the *City*.

(9) A general description of all methodologies used to detect incidents of data breaches or unauthorized access, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the *City*.

(10) Information, including crime statistics, that helps the community assess whether the *surveillance technology* has been effective at achieving its identified purposes.

(11) Statistics and information about California Public Records Act requests regarding the specific *surveillance technology*, including response rates, such as the number of California Public Records Act requests on the *surveillance technology* and the open and close date for each of these California Public Records Act requests.

(12) Total annual costs for the *surveillance technology*, including any specific personnel-related and other ongoing costs, and what source will fund the *surveillance technology* in the coming year.

(13) Any requested modifications to the *Surveillance Use Policy* and a detailed basis for the request.

(b) *Board* means the Privacy Advisory Board established by Chapter 2, Article 6, Division 00, section 26.42, of the San Diego Municipal Code.

(c) *City* means any department, division, office, unit, or program of the City of San Diego.

(d) *City staff* means personnel employed by the *City* to engage in activities on behalf of any *City* department, division, office, unit, or program. *City* personnel assigned to *federal task force* activities by the Chief of Police or designee are exempt from the requirements of this Division related to the acquisition, procurement, use, reporting, and contractual obligations, solely to the extent of their duties and work related to their assignment to the *federal task force*.

(e) *Community meeting* means a publicly held meeting that is accessible, noticed at least seventy-two hours in advance in at least two languages, for the purpose of educating communities, answering questions, and learning about potential impacts of *surveillance technology* on disadvantaged groups.

(f) *Exigent circumstances* means an emergency involving danger of death or serious physical injury to any *individual*, or imminent danger of significant property damage, that requires the use of *surveillance technology*, as determined by *City staff* acting in good faith upon known facts.

(g) *Existing surveillance technology* means technology that the *City* possessed, used, or had a contract in force and effect for its use before September 9, 2022.

(h) *Facial recognition technology* means an automated or semi-automated process that assists in identifying or verifying an *individual* based on an *individual's* face.

(i) *Federal task force* means any group or collaboration with and between *City* employees and federal or state employees, or any group or body established or codified by federal or state statute, regulation, or rule.

(j) *Individual* means a natural person.

(k) *New surveillance technology* means technology that the *City* did not possess, use, or have a contract in force and effect for its use before September 9, 2022.

(l) *Personal communication device* means a mobile telephone, a personal digital assistant, a wireless capable tablet, or a similar wireless two-way communications or portable internet-accessing device, whether procured or subsidized by the *City* or personally owned, that is used in the regular course of *City* business.

(m) *Police area* means each of the geographic districts assigned to a San Diego Police Department captain or commander.

(n) *Surveillance* or *surveil* means to observe or analyze the movements, behavior, data, or actions of *individuals*, including those whose identity can be revealed by data or combinations of data, such as license plate data, images, IP addresses, user identifications, unique digital identifiers, or data traces left by the *individual*.

(o) *Surveillance technology* means any software (for example, scripts, code, or Application Programming Interfaces), electronic device, system utilizing an electronic device, or similar device, which is used, designed, or primarily intended to observe, collect, retain, analyze, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any *individual* or group. It also includes the product (for example, audiovisual recording, data, analysis, or report) of the *surveillance technology*. Examples of *surveillance technology* include the following: cell site simulators (Stingrays); automatic license plate readers; gunshot detectors (ShotSpotter); drone-mounted data collection; *facial recognition technology*; thermal imaging systems; body-worn cameras; social media analytics software; gait analysis software; and video cameras that record audio or video and transmit or can be remotely accessed. It also includes software designed to monitor social media services or forecast criminal activity or criminality, and biometric identification hardware or software.

(1) *Surveillance technology* does not include the following devices, software, or hardware:

(A) Office hardware and software, including televisions, computers, credit card machines, badge readers, copy machines, printers, firewalls, *City* network infrastructure, *City* operational business applications, social media applications for *City* public communications, general internet search engines, and open-source databases, in widespread use by the general public and routinely used by *City staff* to gather data and information to assist in the performance of their duties.

(B) Parking ticket devices used solely for parking enforcement-related purposes, including any sensors embedded in parking sensors to detect the presence of a car in the space.

(C) Manually-operated, non-wearable, handheld digital cameras, audio recorders, and video recorders that are not designed to be used surreptitiously and whose functionality is limited to manually capturing and manually downloading video or audio recordings or both.

(D) *Surveillance* devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles.

(E) Manually-operated technological devices used primarily for internal municipal entity communications that are not designed to surreptitiously collect *surveillance* data, such as radios and email systems.

(F) *City* databases, software, or enterprise systems used by *City staff* to prepare, receive, or retain, or all three, legally required records and information; manage internal operational activities, including *City* payroll, accounting, and other fiscal operations; conduct *City* marketing, donor, media, and constituent relations; and engage in communications initiated by *individuals* directed to *City staff* to request *City* services, file complaints, or communicate information about *City* services.

(G) Medical equipment used to diagnose, treat, or prevent disease or injury, provided that any information obtained from this equipment is used solely for medical purposes.

(H) San Diego Police Department interview room cameras.

(I) *City* department case management and records management systems.

(J) *Personal communication devices* that have not been modified beyond stock manufacturer capabilities.

(K) *Surveillance technology* used by the *City* to monitor and conduct internal investigations and evaluations of the conduct of *City* employees, contractors, and volunteers, including GPS and automatic vehicle locators installed in *City* equipment and San Diego Police Department early warning systems.

(L) Systems, software, databases, and data sources used for revenue collection, cost recovery, or both, on behalf of the *City* by the City Treasurer or other *City* departments required to collect revenue or costs on behalf of the *City*, provided that no information from these sources may be shared by the *City* with any third party except as part of efforts to collect money that is owed to the *City*.

(M) Physical access control systems, employee and contractor identification management systems, and other security systems, including fixed security cameras, used to safeguard the *City's* buildings, facilities, utilities, reservoirs, and other physical assets.

(N) Systems used for computer-aided dispatch (CAD), Live Scan, and in-custody bookings; Department of Motor Vehicles databases; California Law Enforcement Telecommunications System (CLETS); other federal, state, and local summary criminal history databases; and 9-1-1 communications and related systems for dispatch and law enforcement operations and emergency services.

(O) Databases under the management and control of other governmental agencies and used by the *City* for emergency response, law enforcement, regulatory, and *City* personnel-related purposes, such as ARJIS, SDLaw, Parole LEADS, Offender Watch, California Pawn and Secondhand Dealers System (CAPSS), and Automated Fingerprint Identification System (AFIS).

(P) Equipment designed to detect the presence of, or identify the source of, or dispose of hazardous material, such as chemical, biological, radiological, or explosive materials.

(Q) Software that the San Diego Police Department uses to analyze approved or exempted *surveillance technology* and its associated data.

(p) *Surveillance Impact Report* means a publicly released written report regarding specific *surveillance technology* that includes all of the following elements:

(1) Description: Information describing the *surveillance technology* and how it works, including product descriptions from manufacturers, if available.

(2) Purpose: Information on the proposed purposes and outcomes for the *surveillance technology*.

(3) Location: The physical or virtual locations where the *surveillance technology* may be deployed, using general descriptive terms and crime statistics for the locations.

(4) Impact: An assessment of the *Surveillance Use Policy* for the particular *surveillance technology*, including whether there is adequate protection of civil rights and civil liberties and whether the *surveillance technology* may be used or deployed, intentionally or inadvertently, in a manner that may disproportionately affect marginalized communities.

(5) Mitigation: Identification of specific, affirmative technical and procedural measures that will be implemented to safeguard the public from each identified impact.

(6) Data Types and Sources: A list of all types and sources of data to be collected, analyzed, or processed by the *surveillance technology*, including scores, reports, the logic or algorithm used, and any additional information derived from the *surveillance technology*, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the *City*.

(7) Data Security: Information about the controls that will be designed and implemented to safeguard the data collected or generated by the *surveillance technology* from unauthorized access or disclosure, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the *City*.

(8) Fiscal Cost: The forecasted, prior, and ongoing fiscal costs for the *surveillance technology*, if known and available, including known or projected initial purchase costs, personnel costs, and other ongoing costs, and any current or potential sources of funding.

(9) Third Party Dependence: Whether use or maintenance of the *surveillance technology* will require data gathered by the *surveillance technology* to be handled or stored by a third-party vendor at any time.

(10) Alternatives: A summary of the alternative means to achieve the proposed purposes considered, including alternative means that do not involve the use of *surveillance technology*, before deciding to use the proposed *surveillance technology*, including the costs and benefits associated with each alternative considered and an explanation of the reasons why each alternative is inadequate or less effective.

(11) Track Record: A summary of the experience, if any, of other entities, especially government entities, with the proposed *surveillance technology*, including, if available, quantitative information about the effectiveness of the proposed *surveillance technology* in achieving its stated purpose in other jurisdictions and any known adverse information about the *surveillance technology*, such as unanticipated costs, failures, or abuses of civil rights or civil liberties, existing publicly reported controversies, and any court rulings in favor or in opposition to the *surveillance technology*.

(12) Public Engagement and Comments: A description of any community engagement held and any future community engagement plans, number of attendees, a compilation of all comments received and *City* departmental responses given, and *City* departmental conclusions about potential neighborhood impacts and how the impacts that may result from the acquisition and use of the *surveillance technology* may differ as they pertain to different members of the community.

(q) *Surveillance Use Policy* means a publicly released and legally enforceable policy for the use of specific *surveillance technology* that includes all of the following elements:

(1) Purpose: The specific purposes that the *surveillance technology* is intended to advance.

(2) Use: The specific uses that are authorized and the rules and processes required prior to the use, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the *City*.

(3) Data Collection: The information that can be collected, captured, recorded, intercepted, or retained by the *surveillance technology*, data that may be inadvertently collected during the authorized uses of the *surveillance technology* and what measures will be taken to minimize and delete the data, and any data sources the *surveillance technology* will rely upon, as applicable, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the *City*.

(4) Data Access: The job classification of *individuals* who can access or use the collected information, and the rules and processes required prior to access or use of the information, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the *City*.

(5) Data Protection: The safeguards that protect information from unauthorized access, including system logging, encryption, and access control mechanisms, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the *City*.

(6) Data Retention: The time period, if any, for which information collected by the *surveillance technology* will be routinely retained, the reason the retention period is appropriate to further the purposes, the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period.

(7) Public Access: A description of how collected information can be accessed or used by members of the public, including criminal defendants.

(8) Third Party Data Sharing: If and how information obtained from the *surveillance technology* can be accessed or used, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information.

(9) Training: The training required for any individual authorized to use the *surveillance technology* or to access information collected by the *surveillance technology*.

(10) Auditing and Oversight: The procedures used to ensure that the *Surveillance Use Policy* is followed, including identification of internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the *surveillance technology* and access to information collected by the *surveillance technology*, technical measures to monitor for misuse, identification of any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy.

(11) Maintenance: The procedures used to ensure that the security and integrity of the *surveillance technology* and collected information will be maintained.

*("Definitions" added 8-10-2022 by O-21514 N.S; effective 9-9-2022.)*
*(Amended 8-8-2023 by O-21711 N.S.; effective 9-7-2023.)*
*(Renumbered from former Section 210.0101 to Section 210.0102 and amended 2-14-2024 by O-21762 N.S.; effective 3-15-2024. Former Section 210.0102 "Board Notification and Review Requirements" retitled, amended, and renumbered to Section 210.0104.)*

## §210.0103 Preparation and Presentation of the Surveillance Use Policy to the Members of the Public

Before providing notice to the Chair of the *Board* of the proposed acquisition and use of *new surveillance technology* or the continued use of *existing surveillance technology*, *City staff* shall complete at least one publicly noticed *community meeting*, accessible to residents and other community members, in every City Council District where the *surveillance technology* will be used, to discuss the *new surveillance technology* or *existing surveillance technology*. *City staff* may use internet-based technology to make the community meeting accessible, so long as reasonable public accommodations are made for those community members who do not have access to the internet-based technology. *City staff* shall use the *community meeting* or *community meetings* to gather public comment related to the *surveillance technology*. *City staff* shall also implement a process to receive written comments from members of the public related to the *surveillance technology*.

*("Preparation and Presentation of the Surveillance Use Policy to the Members of the Public" added 2-14-2024 by O-21762 N.S.; effective 3-15-2024. Former Section 210.0103 "City Council Approval for New and Existing Surveillance Technology" retitled and renumbered to Section 210.0106.)*

## §210.0104 Board Review of New Surveillance Technology

(a) *City staff* shall notify the Chair of the *Board* by written memorandum and provide a *Surveillance Impact Report* and a proposed *Surveillance Use Policy*, with the elements required by San Diego Municipal Code section 210.0102, before:

1) soliciting proposals from any entity to acquire, share, or otherwise use *new surveillance technology*; or

(2) formally or informally facilitating or implementing *new surveillance technology* in collaboration with other entities, including *City* ones.

(b) Upon receipt of the notification by *City staff*, the Chair of the *Board* shall place the proposed acquisition and use of the *new surveillance technology* on the agenda at the next *Board* meeting for discussion and advisory review and recommendation to the City Council. The *Board* shall publicly notice the meeting in accordance with applicable laws, including the Ralph M. Brown Act.

(c) By majority vote, the *Board* may take one of the following actions:

(1) the *Board* may recommend that the City Council authorize *City staff* to proceed with the proposed acquisition and use of the *new surveillance technology* under the proposed *Surveillance Use Policy*;

(2) the *Board* may recommend that the City Council authorize *City staff* to proceed with the proposed acquisition and use of the *new surveillance technology*, but under a modified *Surveillance Use Policy*, with the proposed modifications expressly recommended by the *Board*;

(3) the *Board* may object to the proposed *Surveillance Use Policy* and state the reasons for the objection; or

(4) the *Board* may take no position related to the *new surveillance technology*.

(d) After the *Board* takes action on the proposed acquisition and use of the *new surveillance technology*, *City staff* may seek City Council approval of the proposed *new surveillance technology* under the requirements of this Division. *City staff* shall present to the City Council the result of the *Board's* advisory review and recommendation, if any.

(e) If the *Board* does not take action on the proposed acquisition and use of the *new surveillance technology* within 90 calendar days of the notification to the *Board* Chair, *City staff* may seek a determination on the proposed *Surveillance Use Policy* by the City Council.

*("Board Notification and Review Requirements" added 8-10-2022 by O-21514 N.S; effective 9-9-2022.)*
*(Renumbered from former Section 210.0102 to Section 210.0104, retitled from "Board Notification and Review Requirements" to "Board Review of New Surveillance Technology" and amended 2-14-2024 by O-21762 N.S.; effective 3-15-2024. Former Section 210.0104 "Use of Unapproved Surveillance Technology During Exigent Circumstances" amended and renumbered to Section 210.0107.)*

## §210.0105 Board Review of Existing Surveillance Technology

(a) Before September 9, 2026, *City staff* may continue to use *existing surveillance technology*, under existing contracts, contract amendments, or contract options, or new contracts entered into under the *City's* procurement processes, without seeking the *Board's* advisory review and recommendation related to the *existing surveillance technology* or City Council review of a *Surveillance Impact Report* and approval of a *Surveillance Use Policy*. This grace period allows *City staff* and the *Board* to fully implement the necessary procedures to comply with this Division.

(b) On and after September 9, 2026, for *existing surveillance technology*, *City staff* shall follow the same requirements related to preparation of *Surveillance Impact Reports* and *Surveillance Use Policies* and notification to the *Board* that applies to *new surveillance technology*, as described in San Diego Municipal Code sections 210.0102 through 210.0104.

(c) On and after September 9, 2026, the *Board* shall follow the same advisory review and recommendation process for *existing surveillance technology* that applies to *new surveillance technology*, as described in San Diego Municipal Code section 210.0104.

(d) Before September 9, 2026, *City staff* shall submit to the *Board* Chair a comprehensive list of *existing surveillance technology* in possession or use, under existing contracts, including under contract amendments or options, as of September 9, 2026, for which *City staff* will seek *Board* advisory review and recommendation and City Council approval for continued use.

(e) The *Board* shall rank the *existing surveillance technology* listed by *City staff* in order of potential impact to civil rights and civil liberties to provide a recommended sequence for the items of *existing surveillance technology* to be heard at *Board* meetings. The *Board* shall take into consideration input from *City staff* on the operational importance of the *existing surveillance technology* in determining the ranking for *Board* consideration to allow matters to be heard in a timely manner.

(f) Within 60 calendar days of the *Board's* ranking of the list of *existing surveillance technology* as detailed in subsection (e), *City staff* shall submit at least one notification memorandum to the Chair of the *Board,* along with the applicable *Surveillance Impact Report* and proposed *Surveillance Use Policy,* each month for the *Board*'s advisory review and recommendation, generally beginning with the highest-ranking items as determined by the *Board,* and continuing each month until a notification memorandum, *Surveillance Impact Report,* and proposed *Surveillance Use Policy* have been submitted for each item of *existing surveillance technology* on the list.

(g) If the *Board* does not take action on any item of *existing surveillance technology* within 90 calendar days of *City staff's* notification memorandum to the Chair of the *Board, City staff* may proceed to the City Council for approval of the *existing surveillance technology*.

*(Renumbered from former Section 210.0109 to Section 210.0105, retitled from "Grace Period for Use of Existing Surveillance Technology" to "Board Review of Existing Surveillance Technology" and amended 2-14-2024 by O-21762 N.S.; effective 3-15-2024. Former Section 210.0105 "Oversight Following City Council Approval" retitled, amended, and renumbered to Section 210.0108.)*

## §210.0106 City Council Approval of New Surveillance Technology and Existing Surveillance Technology

(a) *City staff* shall obtain City Council approval prior to any of the following:

(1) accepting or using local, state, or federal funds or in-kind or other donations to acquire *surveillance technology*;

(2) acquiring *new surveillance technology,* including procuring it without the exchange of consideration; or

(3) using *new surveillance technology* or *existing surveillance technology,* for a purpose, in a manner, or in a location not previously described in an approved *Surveillance Use Policy* by the City Council in accordance with the requirements of this Division.

(b) City Council Approval Process

(1) After the applicable requirements in San Diego Municipal Code sections 210.0103 through 210.0105 have been satisfied, *City staff* seeking City Council authorization of *surveillance technology* shall request a date for City Council consideration of the *Surveillance Impact Report* and proposed *Surveillance Use Policy*.

(2) The City Council shall only approve any action as required by this Division after first considering the advisory recommendation of the *Board*, if any, and determining that

(A) the benefits to the community of the *City's* acquisition and use of the *surveillance technology* outweigh the costs;

(B) the proposed use of the *surveillance technology* will safeguard civil rights and civil liberties; and

(C) based on the facts and information presented to the City Council, there is no effective alternative to the proposed *surveillance technology* that provides a lesser financial cost to the *City* and impact on civil rights or civil liberties.

(3) If the City Council determines that the proposed use of the *surveillance technology* meets the standard set forth in this Division, then the City Council may authorize the use by adopting a legally enforceable *Surveillance Use Policy*. The City Council may modify a proposed *Surveillance Use Policy*, if the City Council determines the modification is necessary to meet the standard for approval of the use of the *surveillance technology* established in this Division.

(4) Once the City Council has approved a *Surveillance Use Policy*, it will remain in effect as the *City's* legally enforceable policy until modified by the City Council.

(5) If the City Council has not authorized an item of *existing surveillance technology* within four City Council meetings from the date the City Council initially considers the *existing surveillance technology*, then the *City* shall cease the use of the *existing surveillance technology* until the review and approval of the proposed *Surveillance Use Policy* occurs.

(c) Unless otherwise provided in this Division, *Surveillance Impact Reports* and approved *Surveillance Use Policies* are public records. *City staff* shall make all *Surveillance Impact Reports* and approved *Surveillance Use Policies*, as updated from time to time, available and accessible to the public as long as the *City* uses the *surveillance technology*.

(d) *City staff* shall post all *Surveillance Impact Reports* and approved or pending *Surveillance Use Policies* to the *City's* website with an indication of the current approval status of the *surveillance technology* and the planned City Council date for action, if available.

*("City Council Approval for New and Existing Surveillance Technology" added 8-10-2022 by O-21514 N.S; effective 9-9-2022.)*
*(Renumbered from former Section 210.0103 to Section 210.0106, retitled from "City Council Approval for New and Existing Surveillance Technology" to "City Council Approval of New Surveillance Technology and Existing Surveillance Technology" and amended 2-14-2024 by O-21762 N.S.; effective 3-15-2024. Former Section 210.0106 "Enforcement" amended and renumbered to Section 210.0109.)*

## §210.0107 Use of Unapproved Surveillance Technology During Exigent Circumstances

(a) *City staff* may temporarily acquire or use *surveillance technology* in a manner not in compliance with this Division only in a situation involving *exigent circumstances*.

(b) If *City staff* acquires or uses a *surveillance technology* in a situation involving *exigent circumstances*, *City staff* shall:

(1) immediately report in writing the use of the *surveillance technology* and its justifications to the City Council and the *Board*;

(2) use the *surveillance technology* solely to respond to the *exigent circumstances*;

(3) cease using the *surveillance technology* when the *exigent circumstances* end; and

(4) destroy any data that is not relevant to an ongoing investigation or the *exigent* circumstances, in a manner consistent with applicable laws.

(c) *City staff* shall return any *surveillance technology* acquired in accordance with *exigent circumstances* to the entity that provided it to the *City* within 30 calendar days following the end of the *exigent circumstances*, unless *City staff* initiates the *Board* review and recommendation process set forth in San Diego Municipal Code sections 210.0103 and 210.0104 for the use of *new surveillance technology* by submitting a notification memorandum to the Chair of the *Board*, a *Surveillance Impact Report,* and proposed *Surveillance Use Policy* within this 30-day time period. If *City staff* is unable to meet the 30-day deadline, *City staff* shall notify the City Council, which may grant an extension. In the event that *City staff* complies with the 30-day deadline or the deadline as may be extended by the City Council, *City staff* may retain possession of the *surveillance technology*, but may only use it consistent with the requirements of this Division.

*("Use of Unapproved Surveillance Technology During Exigent Circumstances" added 8-10-2022 by O-21514 N.S; effective 9-9-2022.)*
*(Renumbered from former Section 210.0104 to Section 210.0107 and amended 2-14-2024 by O-21762 N.S.; effective 3-15-2024. Former Section 210.0107 "Contracts for Surveillance Technology" amended and renumbered to Section 210.0110.)*

## §210.0108 Oversight Following City Council Approval of New Surveillance Technology and Existing Surveillance Technology

(a) *City staff* shall submit to the *Board* and to the City Council by February 1 of each year an *Annual Surveillance Report* that discusses the *new surveillance technology* and *existing surveillance technology* approved on or after January 1 of the prior year and that provides additional, necessary updates to the *surveillance technology* approved in prior years. This annual reporting requirement continues as long as the *surveillance technology* is used.

(b) In its review of the *Annual Surveillance Report*, the *Board* shall provide its advisory recommendation to the City Council regarding whether

(1) the benefits to the community of each item of approved *surveillance technology* outweigh the costs;

(2) civil rights and civil liberties are being safeguarded; and

(3) use of the *surveillance technology*, in accordance with the approved *Surveillance Use Policy*, should continue, cease, or be modified to address identified concerns.

(c) If the *Board* does not make a recommendation on each item of approved *surveillance technology* within 90 calendar days of *City staff*'s submission of the *Annual Surveillance Report* to the *Board*, *City staff* may proceed to the City Council for determination of whether the approved *Surveillance Use Policies* should remain in effect, be modified, or be rescinded.

(d) *City staff* may provide an annual report to the City Council in closed session as permitted by state law on cybersecurity threats involving *surveillance technology* and how the *City* is managing risk to include the following:

(1) a list and description of any major *surveillance technology* updates that resulted in the expansion or contraction of system access, data retention, or data access, as well as a description of the reason for the change;

(2) information about any data breaches or unauthorized access to the data collected by the *surveillance tech*nology, including information about the scope of the breach and the actions taken in response; and

(3) a description of the standards and industry best practices that the *City* uses to detect incidents of data breaches or unauthorized access to *surveillance technology*.

*("Oversight Following City Council Approval" added 8-10-2022 by O-21514 N.S; effective 9-9-2022.)*
*(Renumbered from former Section 210.0105 to Section 210.0108, retitled from "Oversight Following City Council Approval" to "Oversight Following City Council Approval of New Surveillance Technology and Existing Surveillance Technology" and amended 2-14-2024 by O-21762 N.S.; effective 3-15-2024. Former Section 210.0108 "Whistleblower Protections" amended and renumbered to Section 210.0111.)*

## §210.0109 Enforcement

(a) Violations of this Division are subject to the following remedies:

(1) Any person who has been subjected to the use of *surveillance technology* in material violation of this Division or an approved *Surveillance Use Policy*, or about whom information has been obtained, retained, accessed, shared, or used in material violation of this Division or an approved *Surveillance Use Policy*, may institute proceedings in the Superior Court of the State of California against the *City* and shall be entitled to recover actual damages (but not less than liquidated damages of $1,000 or $100 per day for each day of violation, whichever is greater). Before filing a lawsuit against the *City* for damages from an alleged violation of this Division or an approved *Surveillance Use Policy*, a claimant shall provide a written claim, including written notice, to the *City* that provides details of the alleged violation. The *City* shall have 30 days from receipt of that written claim in which it may cure any alleged violation, which would act as an affirmative defense in litigation, or otherwise negotiate and resolve any claim with the claimant.

(2) A court may award costs and reasonable attorney's fees to a prevailing party plaintiff in an action brought under this Division. An award of attorney's fees to a prevailing party plaintiff is limited to an amount not to exceed $15,000.

*("Enforcement" added 8-10-2022 by O-21514 N.S; effective 9-9-2022.) (Renumbered from former Section 210.0106 to Section 210.0109 and amended 2-14-2024 by O-21762 N.S.; effective 3-15-2024. Former Section 210.0109 "Grace Period for Use of Existing Surveillance Technology" retitled, amended, and renumbered to Section 210.0105.)*

## §210.0110 Contracts for Surveillance Technology

It shall be unlawful for the *City* to enter into any contract or other agreement for *surveillance technology* after the effective date of this Division that conflicts with the provisions of this Division or any City Council-approved *Surveillance Use Policy*. Any conflicting provisions in any contract or agreement, including non-disclosure agreements, shall be deemed void and legally unenforceable. To the extent permitted by law, the *City* shall publicly disclose all of its *surveillance technology* contracts, including all related non-disclosure agreements, executed after the effective date of this Division. Once the City Council approves a *Surveillance Use Policy*, the *City* may exercise its contracting authority under established procurement processes without additional public review under this Division, unless the proposed contract seeks to expand the capabilities of the *surveillance technology*.

*("Contracts for Surveillance Technology" added 8-10-2022 by O-21514 N.S; effective 9-9-2022.)*
*(Renumbered from Section 210.0107 to Section 210.0110 and amended 2-14-2024 by O-21762 N.S.; effective 3-15-2024. Former Section 210.0110 "Compliance with City Charter or Applicable State Law" retitled, amended, and renumbered to Section 210.0112.)*

## §210.0111 Whistleblower Protections

(a) The *City* or anyone acting on the *City's* behalf shall not discriminate or retaliate against any employee or applicant for employment with respect to compensation, terms or conditions of employment, access to information, due process, or other rights, because:

(1) the employee or applicant made, attempted to make, was perceived to have made, or assisted in any lawful disclosure of information concerning an alleged violation of this Division related to the funding, acquisition, or use of *surveillance technology* or *surveillance* data; or

(2) the employee or applicant participated, attempted to participate, was perceived to have participated, or assisted in any proceeding or action to carry out the purposes of this Division.

(b) It shall be grounds for disciplinary action for a *City* employee to discriminate or retaliate against another *City* employee or applicant for *City* employment who makes a good faith complaint that there has been a failure to comply with an approved *Surveillance Use Policy* or administrative instruction promulgated under this Division.

(c) Any *City* employee or applicant for *City* employment who is injured by a violation of section 210.0111 may institute a proceeding for monetary damages and injunctive relief against the *City* in any court of competent jurisdiction.

*("Whistleblower Protections" added 8-10-2022 by O-21514 N.S; effective 9-9-2022.)*
*(Renumbered from former Section 210.0108 to Section 210.0111 and amended 2-14-2024 by O-21762 N.S.; effective 3-15-2024.)*

## §210.0112 Reporting to Law Enforcement

Nothing in this Division is intended to prevent, restrict, or interfere with any person providing evidence or information derived from *surveillance technology* to a law enforcement agency for the purposes of conducting a criminal investigation, or the law enforcement agency from receiving evidence or information.

*("Compliance with City Charter or Applicable State Law" added 8-10-2022 by O-21514 N.S; effective 9-9-2022.)*
*(Renumbered from former Section 210.0110 to Section 210.0112, retitled from "Compliance with City Charter or Applicable State Law" to "Reporting to Law Enforcement" and amended 2-14-2024 by O-21762 N.S.; effective 3-15-2024.)*