

BOARD of SUPERVISORS



City Hall
1 Dr. Carlton B. Goodlett Place, Room 244
San Francisco 94102-4689
Tel. No. (415) 554-5184
Fax No. (415) 554-5163
TDD/TTY No. (415) 554-5227

MEMORANDUM

TO: Michael Makstman, Executive Director, Department of Technology

FROM: Victor Young, Assistant Clerk *Victor Young*

DATE: May 28, 2026

SUBJECT: LEGISLATION INTRODUCED

The Board of Supervisors' Rules Committee received the following proposed Ordinance:

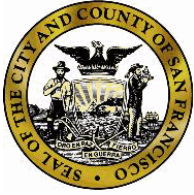
File No. 260272

Ordinance approving the amended Surveillance Technology Policy for the Department of Election's continued use of security cameras and making required findings in support of said approvals.

If you have comments or reports to be included with the file, please forward them to Victor Young at the Board of Supervisors, City Hall, Room 244, 1 Dr. Carlton B. Goodlett Place, San Francisco, CA 94102 or by email at: victor.young@sfgov.org.

(attachment)

c. Karen Hong Yee, Department of Technology



City and County of San Francisco

Master Report

City Hall
1 Dr. Carlton B. Goodlett Place
San Francisco, CA 94102-4689

File Number: 260272 **File Type:** Ordinance **Status:** 30 Day Rule

Enacted: _____ **Effective:** _____

Version: 1 **In Control:** Rules Committee

File Name: Administrative Code - Department of Elections
Amended Surveillance Technology Policy **Date Introduced:** 03/24/2026

Requester: Elections Department **Cost:** _____ **Final Action:** _____

Comment: _____ **Title:** Ordinance approving the amended Surveillance Technology Policy for the Department of Election's continued use of security cameras and making required findings in support of said approvals.

History of Legislative File 260272

Ver	Acting Body	Date	Action	Sent To	Due Date	Result
1	Clerk of the Board	03/09/2026	RECEIVED FROM DEPARTMENT			
1	President	03/24/2026	ASSIGNED UNDER 30 DAY RULE	Rules Committee	04/23/2026	

1 [Administrative Code - Department of Elections Amended Surveillance Technology Policy]

2

3 **Ordinance approving the amended Surveillance Technology Policy for the Department**
4 **of Election's continued use of security cameras and making required findings in**
5 **support of said approvals.**

6

7

NOTE: **Unchanged Code text and uncodified text** are in plain Arial font.
8 **Additions to Codes** are in *single-underline italics Times New Roman font*.
9 **Deletions to Codes** are in ~~*strikethrough italics Times New Roman font*~~.
10 **Board amendment additions** are in double-underlined Arial font.
11 **Board amendment deletions** are in ~~strikethrough Arial font~~.
12 **Asterisks (* * * *)** indicate the omission of unchanged Code
13 subsections or parts of tables.

11

12 Be it ordained by the People of the City and County of San Francisco:

13

14 Section 1. Background.

15

16 (a) Terms used in this ordinance have the meaning set forth in Administrative Code
17 Chapter 19B ("Chapter 19B").

18

19

20 (b) Chapter 19B regulates City Departments' acquisition and use of Surveillance
21 Technology. Under Section 19B.5, City Departments that possessed or were using
22 Surveillance Technology before Chapter 19B took effect in July 2019 must obtain Board of
23 Supervisors ("Board") approval by ordinance of a Surveillance Policy for each type of existing
24 Surveillance Technology. Under Section 19B.2(a), a Department must obtain Board approval
25 by ordinance of a Surveillance Technology Policy before: (1) seeking funds for Surveillance
Technology; (2) acquiring or borrowing new Surveillance Technology; (3) using new or
existing Surveillance Technology for a purpose, in a manner, or in a location not specified in a
Surveillance Technology Policy ordinance approved by the Board in accordance with Chapter

1 19B; (4) entering into agreement with a non-City entity to acquire, share, or otherwise use
2 Surveillance Technology; or (5) entering into an oral or written agreement under which a non-
3 City entity or individual regularly provides the Department with data or information acquired
4 through the entity's use of Surveillance Technology.

5 (c) Under Administrative Code Section 19B.2(b), the Board may approve a
6 Surveillance Technology Policy ordinance under Section 19B.2(a) if: (1) the Department
7 seeking Board approval under subsection (a) creates a Surveillance Technology Policy and
8 Surveillance Impact Report for the Surveillance Technology to be acquired or used; and (2) at
9 a public hearing at which the Committee on Information Technology ("COIT") considers the
10 Surveillance Technology Policy, COIT recommends that the Board adopt, adopt with
11 modifications, or decline to adopt the Surveillance Technology Policy for the Surveillance
12 Technology to be acquired or used.

13 (d) Under Administrative Code Section 19B.2(m), any amendment to an existing
14 Surveillance Technology Policy shall be submitted directly to the Board and not to COIT.

15 (e) The Amended Surveillance Technology Policy ("Amended Policy") revises and
16 replaces the Department of Elections' ("Elections") current Surveillance Technology Policy
17 regarding indoor security cameras, to live stream ballot processing and election-related
18 operations, which the Board approved in Ordinance No. 245-22, on file with the Clerk of the
19 Board in File No. 221043. The Amended Policy is on file with the Clerk of the Board in File
20 No. ___ and incorporated herein by reference.

21 (f) This ordinance sets forth the Board's findings in support of the Amended Policy and
22 its approval of the Amended Policy.

23
24 Section 2. Use of Indoor Security Cameras.
25

1 (a) As authorized by Ordinance No. 245-22, Elections currently possesses and uses
2 indoor security cameras.

3 (b) Elections uses the indoor security cameras to: (1) conduct live monitoring of voting
4 center lines; (2) conduct live monitoring of ballot processing and election-related operations;
5 (3) share live streaming footage of the Department ballot processing and election-related
6 operations with the public to promote transparency into elections operations, and (4) review
7 camera footage in the event of an incident.

8 (c) The current policy specifies a particular vendor, Google, that Elections has used to
9 provide indoor security cameras. The Amended Policy allows Elections the flexibility to use
10 other vendors that offer the same services and are approved by the City.

11 (d) The current policy provides for a retention period of 10 days on Google's Cloud,
12 after which recorded footage is automatically deleted. The Amended Policy reduces the
13 retention period from 10 days to four days and allows Elections the flexibility to use any cloud-
14 based platform approved by the City.

15 (e) The current policy specifies that recordings are accessible only to authorized staff
16 of Elections. The Amended Policy updates the list with current applicable job codes.

17
18 Section 3. Findings and Approval of the Amended Policy.

19 (a) The Board hereby finds that the benefits that Elections' Amended Policy authorizes
20 outweigh the costs and risks; that the Amended Policy will safeguard civil liberties and civil
21 rights; and that the uses and deployments by Elections of indoor security cameras, as set
22 forth in the Amended Policy, will not be based upon discriminatory or viewpoint-based factors
23 or have a disparate impact on any community or Protected Class.

24 (b) The Board hereby approves the Department of Elections' Amended Policy for use
25 of indoor security cameras.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

Section 4. Effective Date. This ordinance shall become effective at 12:00 a.m. on the 31st day after enactment. Enactment occurs when the Mayor signs the ordinance, the Mayor returns the ordinance unsigned or does not sign the ordinance within 10 days of receiving it, or the Board of Supervisors overrides the Mayor’s veto of the ordinance.

APPROVED AS TO FORM:
DAVID CHIU, City Attorney

By: /s/ Ana Flores _____
ANA I. FLORES
Deputy City Attorney

4917-1187-7259, v. 3

LEGISLATIVE DIGEST

[Administrative Code - Department of Elections Amended Surveillance Technology Policy]

Ordinance approving the amended Surveillance Technology Policy for the Department of Election's continued use of security cameras and making required findings in support of said approvals.

Background Information

Administrative Code Chapter 19B (Chapter 19B) regulates City Departments' acquisition and use of Surveillance Technology. The Department of Elections (Elections) seeks to amend its Surveillance Technology Policy for Use of Indoor Security Cameras (Amended Surveillance Technology Policy).

Under the existing ordinance, Elections uses the Indoor Security Cameras to: (1) conduct live monitoring of voting center lines; (2) conduct live monitoring of ballot processing and election-related operations; (3) share live streaming footage of the Department ballot processing and election-related operations with the public to promote transparency into elections operations, and (4) review camera footage in the event of an incident. The existing ordinance lists a particular vendor, Google, to provide security cameras and cloud-based platform needed for retention.

The Amended Surveillance Technology Policy allows Elections: (1) the flexibility to use other vendors that offer the same services and are approved by the City, (2) reduces the retention period from 10 days to four days, and (3) use any cloud-based platform to store the recorded footage.

The Amended Surveillance Technology Policy is detailed in Section 2 of the proposed ordinance. The Surveillance Technology Policy is available in Board File No. _____.



Surveillance Technology Policy

Security Cameras
Department of Elections

The City and County of San Francisco values the privacy and protection of San Francisco residents' civil rights and civil liberties. As required by San Francisco Administrative Code, Section 19B, the Surveillance Technology Policy aims to ensure the responsible use of Department's Camera System itself as well as any associated data, and the protection of City and County of San Francisco residents' civil rights and liberties.

PURPOSE AND SCOPE

The Surveillance Technology Policy ("Policy") defines the manner in which the Camera System (fixed or mobile) will be used to support department operations.

This Policy applies to all department personnel that use, plan to use, or plan to secure Camera Systems, including employees, contractors, and volunteers. Employees, consultants, volunteers, and vendors while working on behalf of the City with the Department are required to comply with this Policy.

POLICY STATEMENT

City departments using this policy will limit their use of Cameras to the following authorized use cases and requirements listed in this Policy.

Authorized Use(s):

1. Live monitoring of voting center lines.
2. Live monitoring of ballot processing and election-related operations.
3. Live streaming of ballot processing and election-related operations.
4. Reviewing camera footage in the event of an incident.
- 5.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Departments may use information collected from security cameras only for legally authorized purposes, and may not use that information to unlawfully discriminate against people based on race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, sexual orientation or activity, or genetic and/or biometric data. Additionally, departments may not use automated systems to scan footage and identify individuals based on any of the categories listed in the preceding sentence.

Surveillance Oversight Review Dates

COIT Review: November 21, 2021

Board of Supervisors Review: Upcoming

BUSINESS JUSTIFICATION

In support of Department operations, Security Cameras promise to help with:

- | | | |
|---|--|--|
| X | Education | Allows the public to watch and learn about the election process in San Francisco. |
| | <ul style="list-style-type: none"> ▪ Community Development | |
| X | Health | Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment. |
| | <ul style="list-style-type: none"> ▪ Environment ▪ Criminal Justice ▪ Jobs ▪ Housing | |
| X | Other | Transparency is a key component of free, fair, and functional elections. To that end, the Department of Elections welcomes members of the public to observe its operations and offer feedback. |

In addition, the following benefits are obtained:

Benefit	Description
X	Financial Savings Streaming cameras allow the Department to provide remote observation of election activities while minimizing deployment of personnel to staff each observation area to support potential observers.
X	Time Savings Streaming cameras enable monitoring of election processes happening in different areas of the city at the same time from a central location.
X	Staff Safety Cameras help identify violations of Department Patron Code of Conduct and provide assurance that staff safety is emphasized and will be protected at their place of employment.
X	Data Quality Web streaming cameras may run 24/7 during an election cycle regarding ballot processing and election-related operations. Cameras linked to the security system in the Department's Warehouse operate when the system is engaged. Data resolution can be set by level and is currently set to standard resolutions.
X	Service Levels Cameras will enhance transparency of elections operations to the public.

POLICY REQUIREMENTS

This Policy defines the responsible data management processes and legally enforceable safeguards required by the Department to ensure transparency, oversight, and accountability measures. Department use of surveillance technology and information collected, retained, processed or shared by surveillance technology must be consistent with this Policy; must comply with all City, State, and Federal laws and regulations; and must protect all state and federal Constitutional guarantees.

Specifications: The software and/or firmware used to operate security cameras must be kept up-to-date and maintained.

Data Collection: Department shall only collect data required to execute the authorized use case. All data collected by the surveillance technology, including PII, shall be classified according to the City's [Data Classification Standard](#).

The surveillance technology collects some or all of the following data types:

<i>Data Type(s)</i>	<i>Format(s)</i>	<i>Classification</i>
Video and Images	MP4, AVI, MPEG	Level 3
Date and Time	MP4 or other format	Level 3
Geolocation data	TXT, CSV, DOCX	Level 3

Notification: Departments shall notify the public of intended surveillance technology operation at the site of operations through signage in readily viewable public areas in accordance to Section 19.5 of the Administrative Code. Department notifications shall identify the type of technology being used and the purpose for such collection.

The Department's public notice will include the following items:

- X Information on the surveillance technology
- X Description of the authorized use
 - Type of data collected
 - Will persons be individually identified
 - Data retention
- X Department identification
- X Contact information

Access: Prior to accessing or using data, authorized individuals receive training in system access and operation, and instruction regarding authorized and prohibited uses.

Access to live views are available to the public via a live-stream video feed, for the duration of the election activities which include voting and vote tallying. Live video footage is made available to the public to provide transparency surrounding city and county elections. Recorded footage is restricted to specific trained personnel. Any footage that is recorded is accessed only in response to an incident and is automatically deleted up to 4 days after the recording is made.

Details on department staff and specific access are available in Appendix A.

Data Security: Department shall secure PII against unauthorized or unlawful processing or disclosure; unwarranted access, manipulation or misuse; and accidental loss, destruction, or damage. Surveillance technology data collected and retained by the Department shall be protected by the safeguards appropriate for its classification level(s) as defined by the National Institute of Standards and Technology (NIST) security framework 800-53, or equivalent requirements from other major cybersecurity framework selected by the department.

Departments shall, at minimum, apply the following safeguards to protect surveillance technology information from unauthorized access and control, including misuse:

- Encryption: Data retained by the Department will be encrypted. Raw data may be retained by the Department only for the authorized use case of sharing with law enforcement or the public.
- Storage: Any use of a third-party service provider must meet City's cyber security requirements.
- Audits: A data access log will be maintained by the Department for all Security Camera data that is processed and utilized. This log will include but is not limited to the following: date/time data was originally obtained/collected, reasons/intended use for data, department requesting data, date/time of access of raw data, outcome of data processing, as well as date processed data was delivered to users.

Data Sharing: For internal and externally shared data, shared data shall not be accessed, used, or processed by the recipient in a manner incompatible with the authorized use cases stated in this Policy. Department will endeavor to ensure that other agencies or departments that may receive data collected by their own Camera Systems will act in conformity with this Surveillance Technology Policy.

Department shall ensure proper administrative, technical, and physical safeguards are in place before sharing data with other CCSF departments, outside government entities, and third-party providers or vendors. Because this footage is streamed live

to the public, it is possible that viewers of the footage will retain, share, or and use the footage in ways that do not comply with this policy.

Each department that believes another agency or department receives or may receive data collected from its use of Cameras should consult with its assigned Deputy City Attorney regarding their response.

Before sharing data with any recipients, the Department will use the following procedure to ensure appropriate data protections are in place:

X Confirm the purpose of the data sharing aligns with the department's mission.

X Consider alternative methods other than sharing data that can accomplish the same purpose.

X Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies.

X Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.

X Evaluation of what data can be permissibly shared with members of the public should a request be made in accordance with the San Francisco's Sunshine Ordinance.

X Ensure data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

Department will comply with the California Public Records Act, the San Francisco Sunshine Ordinance, the requirements of the federal and State Constitutions, and federal and State civil procedure laws and rules.

The Department may share Camera footage with the following entities:

A. *Internal Data Sharing:*

In the event of an incident, Camera images may be live-streamed or shared by alternative methods to the following agencies:

- Within the operating Department
- Police
- City Attorney
- District Attorney
- Sheriff

Data sharing occurs at the following frequency:

- On request following an incident.

B. External Data Sharing:

- Other local law enforcement agencies

Data sharing occurs at the following frequency:

- As needed.

Data Retention: Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose. Department data retention standards should align with how the department prepares its financial records and should be consistent with any relevant Federal Emergency Management Agency (FEMA) or California Office of Emergency Services (Cal OES) sections.

The Department's data retention period and justification are as follows:

- Camera data from security system at the Department's Warehouse may be stored for a minimum of one (1) year to be available to authorized staff for operational necessity and ready reference, subject to technical limitations.

If data is associated with an incident, it may be kept for longer than the standard retention period.

- Justification: This retention period conforms with the available server system storage space and allows for ample time for security staff to review footage related to security incidents and/or external requests for records.

Data may be stored in the following location:

- X Local storage (e.g., local server, storage area network (SAN), network-attached storage (NAS), backup tapes, etc.)
- X Department of Technology Data Center
- X Software as a Service Product
- X Cloud Storage Provider

Data Disposal: Upon completion of the data retention period, Department shall dispose of data in the following manner:

- Automatic overwrite of all existing files when standard data retention period ends. This may take the form of a delete/reformat, wipe, overwrite of existing data, or degaussing.

Training: To reduce the possibility that surveillance technology or its associated data will be misused or used contrary to its authorized use, all individuals requiring access must receive training on data security policies and procedures.

- Annual cybersecurity training (COIT Policy Link)

COMPLIANCE

Department shall oversee and enforce compliance with this Policy according to the respective memorandum of understanding of employees and their respective labor union agreement.

If a Department is alleged to have violated the Ordinance under San Francisco Administrative Code Chapter 19B, Department shall post a notice on the Department's website that generally describes any corrective measure taken to address such allegation.

Department is subject to enforcement procedures, as outlined in San Francisco Administrative Code Section 19B.8.

DEFINITIONS

Personally Identifiable Information:	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.
--------------------------------------	--

AUTHORIZATION

Section 19B.4 of the City's Administrative Code states, "It is the policy of the Board of Supervisors that it will approve a Surveillance Technology Policy ordinance only if it determines that the benefits the Surveillance Technology ordinance authorizes outweigh its costs, that the Surveillance Technology Policy ordinance will safeguard civil liberties and civil rights, and that the uses and deployments of the Surveillance Technology under the ordinance will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class."

Appendix A: Department Specific Responses

1. A description of the product, including vendor and general location of technology.
 - Indoor security cameras. Deployed during election cycle at Department of Elections for live streaming ballot processing and election-related operations in City Hall and the Department's Warehouse, and to record incidents occurring after-hours in the Warehouse
2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information
 - Streams of Election processes are available to the public.
 - Streams used for line management at City Hall Vote Center is accessible by all Department of Elections staff.
 - Recordings are accessible to the following authorized staff of the Department:
 - 1092 IT Operations Support Admin II
 - 1043 IS Engineer-Senior
 - 0962 Dept Head II
 - 0952 Deputy Director II
 - 0951 Deputy Director I
3. What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.
 - Members of the public can register complaints / concerns or submit questions at San Francisco Department of Elections City Hall 1 Dr. Carlton B. Goodlett Place, Room 48 San Francisco, CA 94102, 415-558-6100, SFVote@sfgov.org, Contact form: <https://sfelections.gov/sfvote/>
 - The Department responds to all inquiries within 10 days of receipt, regardless of method of submission. During the election cycle, all inquiries are logged in a Public Inquiry Tracking Application, assigned to a division or staff member, and tracked to completion.
4. Specific details on where data will be stored (local, DT, SaaS, Cloud Storage) including name of vendor and retention period.
 - Recordings are automatically saved to a cloud based platform for a period of up to 4 days as part of a subscription plan. After the retention period, the recordings are automatically deleted.
- 5.



Surveillance Technology Policy

Security Cameras
Department of Elections

The City and County of San Francisco values the privacy and protection of San Francisco residents' civil rights and civil liberties. As required by San Francisco Administrative Code, Section 19B, the Surveillance Technology Policy aims to ensure the responsible use of Department's Camera System itself as well as any associated data, and the protection of City and County of San Francisco residents' civil rights and liberties.

PURPOSE AND SCOPE

The Surveillance Technology Policy ("Policy") defines the manner in which the Camera System (fixed or mobile) will be used to support department operations.

This Policy applies to all department personnel that use, plan to use, or plan to secure Camera Systems, including employees, contractors, and volunteers. Employees, consultants, volunteers, and vendors while working on behalf of the City with the Department are required to comply with this Policy.

POLICY STATEMENT

City departments using this policy will limit their use of Cameras to the following authorized use cases and requirements listed in this Policy.

Authorized Use(s):

1. Live monitoring of voting center lines.
2. Live monitoring of ballot processing and election-related operations.
- ~~2. Live monitoring of Department staff during elections operations.~~
3. Live streaming footage of ballot processing and election-related operations.
- ~~3. Recording of video and images of Department staff during elections operations.~~
4. Reviewing camera footage in the event of an incident.
- ~~4. Reviewing camera footage of Department staff in the event of an incident.~~
5. Sharing camera footage of Department staff with the public to promote transparency into elections operations.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Departments may use information collected from security cameras only for legally authorized purposes, and may not use that information to unlawfully discriminate against people based on race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, sexual orientation or activity, or genetic and/or biometric data. Additionally, departments may not use automated systems to scan footage and identify individuals based on any of the categories listed in the preceding sentence.

Surveillance Oversight Review Dates

COIT Review: November 21, 2021

Board of Supervisors Review: Upcoming

BUSINESS JUSTIFICATION

In support of Department operations, Security Cameras promise to help with:

- | | | |
|---|-------------------------|--|
| X | Education | Allows the public to watch and learn about the election process in San Francisco. |
| | ▪ Community Development | |
| X | Health | Protect safety of staff, patrons, and facilities while promoting an open and welcoming environment. |
| | ▪ Environment | |
| | ▪ Criminal Justice | |
| | ▪ Jobs | |
| | ▪ Housing | |
| X | Other | Transparency is a key component of free, fair, and functional elections. To that end, the Department of Elections welcomes members of the public to observe its operations and offer feedback. |

In addition, the following benefits are obtained:

Benefit	Description
X	Financial Savings Streaming cameras allow us the Department to provide remote election-observation of election activities while minimizing deployment of personnel to staff each observation area to support potential observers .
X	Time Savings Streaming cameras enable monitoring of election processes happening in different areas of the city at the same time from a central location.
X	Staff Safety Cameras help identify violations of Department Patron Code of Conduct and provide assurance that staff safety is emphasized and will be protected at their place of employment.
X	Data Quality Web streaming cameras may run 24/7/365 during an election cycle regarding ballot processing and election-related operations. Cameras linked to the security system in the Department's Warehouse operate when the system is engaged. Data resolution can be set by level and is currently set to standard resolutions. Cameras run 24/7/365 so full-time staffing is not required to subsequently review footage of security incidents. Data resolution can be set by level and is currently set to high resolution.
X	Service Levels Cameras will enhance transparency of elections operations to the public.

POLICY REQUIREMENTS

This Policy defines the responsible data management processes and legally enforceable safeguards required by the Department to ensure transparency, oversight, and accountability measures. Department use of surveillance technology and information collected, retained, processed or shared by surveillance technology must be consistent with this Policy; must comply with all City, State, and Federal laws and regulations; and must protect all state and federal Constitutional guarantees.

Specifications: The software and/or firmware used to operate security cameras must be kept up-to-date and maintained.

Data Collection: Department shall only collect data required to execute the authorized use case. All data collected by the surveillance technology, including PII, shall be classified according to the City's [Data Classification Standard](#).

The surveillance technology collects some or all of the following data types:

<i>Data Type(s)</i>	<i>Format(s)</i>	<i>Classification</i>
Video and Images	MP4, AVI, MPEG	Level 3
Date and Time	MP4 or other format	Level 3
Geolocation data	TXT, CSV, DOCX	Level 3

Notification: Departments shall notify the public of intended surveillance technology operation at the site of operations through signage in readily viewable public areas in accordance to Section 19.5 of the Administrative Code. Department notifications shall identify the type of technology being used and the purpose for such collection.

The Department's public notice will include the following items:

- X Information on the surveillance technology
- X Description of the authorized use
 - Type of data collected
 - Will persons be individually identified
 - Data retention
- X Department identification
- X Contact information

Access: Prior to accessing or using data, authorized individuals receive training in system access and operation, and instruction regarding authorized and prohibited uses.

Access to live views are available to the public via a live-stream video feed, for the duration of the election activities which include voting and vote tallying. Live video footage is made available to the public to provide transparency surrounding city and county elections. Recorded footage is restricted to specific trained personnel. ~~Any Recorded~~-footage that is recorded is accessed only in response to an incident and is automatically deleted 10-up to 4 days after the recording is made.

Details on department staff and specific access are available in Appendix A.

Data Security: Department shall secure PII against unauthorized or unlawful processing or disclosure; unwarranted access, manipulation or misuse; and accidental loss, destruction, or damage. Surveillance technology data collected and retained by the Department shall be protected by the safeguards appropriate for its classification level(s) as defined by the National Institute of Standards and Technology (NIST) security framework 800-53, or equivalent requirements from other major cybersecurity framework selected by the department.

Departments shall, at minimum, apply the following safeguards to protect surveillance technology information from unauthorized access and control, including misuse:

- Encryption: Data retained by the Department will be encrypted. Raw data may be retained by the Department only for the authorized use case of sharing with law enforcement or the public.
- Storage: Any use of a third-party service provider must meet City's cyber security requirements.
- Audits: A data access log will be maintained by the Department for all Security Camera data that is processed and utilized. This log will include but is not limited to the following: date/time data was originally obtained/collected, reasons/intended use for data, department requesting data, date/time of access of raw data, outcome of data processing, as well as date processed data was delivered to users.

Data Sharing: For internal and externally shared data, shared data shall not be accessed, used, or processed by the recipient in a manner incompatible with the authorized use cases stated in this Policy. Department will endeavor to ensure that other agencies or departments that may receive data collected by their own Camera Systems will act in conformity with this Surveillance Technology Policy.

Department shall ensure proper administrative, technical, and physical safeguards are in place before sharing data with other CCSF departments, outside government entities, and third-party providers or vendors. Because this footage is streamed live

to the public, it is possible that viewers of the footage will retain, share, or and use the footage in ways that do not comply with this policy.

Each department that believes another agency or department receives or may receive data collected from its use of Cameras should consult with its assigned Deputy City Attorney regarding their response.

Before sharing data with any recipients, the Department will use the following procedure to ensure appropriate data protections are in place:

- X Confirm the purpose of the data sharing aligns with the department's mission.
- X Consider alternative methods other than sharing data that can accomplish the same purpose.
- X Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies.
- X Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.
- X Evaluation of what data can be permissibly shared with members of the public should a request be made in accordance with the San Francisco's Sunshine Ordinance.
- X Ensure data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

Department will comply with the California Public Records Act, the San Francisco Sunshine Ordinance, the requirements of the federal and State Constitutions, and federal and State civil procedure laws and rules.

The Department may share Camera footage with the following entities:

A. *Internal Data Sharing:*

In the event of an incident, Camera images may be live-streamed or shared by alternative methods to the following agencies:

- Within the operating Department
- Police
- City Attorney
- District Attorney
- Sheriff

Data sharing occurs at the following frequency:

- On request following an incident.

B. *External Data Sharing:*

- Other local law enforcement agencies

Data sharing occurs at the following frequency:

- As needed.

Data
Retention:

Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose. Department data retention standards should align with how the department prepares its financial records and should be consistent with any relevant Federal Emergency Management Agency (FEMA) or California Office of Emergency Services (Cal OES) sections.

The Department's data retention period and justification are as follows:

- Camera data from security system at the Department's Warehouse may be stored for a minimum of one (1) year to be available to authorized staff for operational necessity and ready reference, subject to technical limitations.
- ~~— Camera data will be stored for a minimum of one (1) year to be available to authorized staff for operational necessity and ready reference, subject to technical limitations.~~

If data is associated with an incident, it may be kept for longer than the standard retention period.

- Justification: This retention period conforms with the available server system storage space and allows for ample time for security staff to review footage related to security incidents and/or external requests for records.

Data may be stored in the following location:

- X Local storage (e.g., local server, storage area network (SAN), network-attached storage (NAS), backup tapes, etc.)
- X Department of Technology Data Center
- X Software as a Service Product
- X Cloud Storage Provider

Data Disposal: Upon completion of the data retention period, Department shall dispose of data in the following manner:

- Automatic overwrite of all existing files when standard data retention period ends. This may take the form of a delete/reformat, wipe, overwrite of existing data, or degaussing.

Training: To reduce the possibility that surveillance technology or its associated data will be misused or used contrary to its authorized use, all individuals requiring access must receive training on data security policies and procedures.

- Annual cybersecurity training (COIT Policy Link)

COMPLIANCE

Department shall oversee and enforce compliance with this Policy according to the respective memorandum of understanding of employees and their respective labor union agreement.

If a Department is alleged to have violated the Ordinance under San Francisco Administrative Code Chapter 19B, Department shall post a notice on the Department's website that generally describes any corrective measure taken to address such allegation.

Department is subject to enforcement procedures, as outlined in San Francisco Administrative Code Section 19B.8.

DEFINITIONS

Personally Identifiable Information:	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.
--------------------------------------	--

AUTHORIZATION

Section 19B.4 of the City's Administrative Code states, "It is the policy of the Board of Supervisors that it will approve a Surveillance Technology Policy ordinance only if it determines that the benefits the Surveillance Technology ordinance authorizes outweigh its costs, that the Surveillance Technology Policy ordinance will safeguard civil liberties and civil rights, and that the uses and deployments of the Surveillance Technology under the ordinance will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class."

Appendix A: Department Specific Responses

1. A description of the product, including vendor and general location of technology.
 - Indoor security cameras. Deployed during Election cycle at Department of Elections for live streaming ballot processing and election--related operations in City Hall and the Department's Warehouse, and to record incidents occurring after-hours in the Warehouse
 - ~~Google Nest Cam Indoor security cameras. Deployed during Election cycle at Department of Elections in City Hall and Department's Warehouse at Pier 31.~~
2. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information
 - Streams of Election processes are available to the public.
 - Streams used for line management at City Hall Vote Center is accessible by all Department of Elections staff.
 - Recordings are accessible to the following authorized staff of the Department:
 - 1092 IT Operations Support Admin II
 - 1043 IS Engineer-Senior
 - 0962 Dept Head II
 - 0952 Deputy Director II
 - 0951 Deputy Director I
 - ~~1092-1095 IS Administrator Series~~
 - ~~1840-1844 Management Assistant series~~
 - ~~1115 Director~~
 - ~~0951-0955 Deputy Director series~~
3. What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.
 - Members of the public can register complaints / concerns or submit questions at San Francisco Department of Elections City Hall 1 Dr. Carlton B. Goodlett Place, Room 48 San Francisco, CA 94102, ~~415-558-6100~~415-554-4375, SFVote@sfgov.org, Contact form: <https://sfelections.gov/org/sfvote/>
 - The Department responds to all inquiries within 10 days of receipt, regardless of method of submission. During the election cycle, all inquiries are logged in a Public Inquiry Tracking Application, assigned to a division or staff member, and tracked to completion.
4. Specific details on where data will be stored (local, DT, SaaS, Cloud Storage) including

name of vendor and retention period.

- ~~Recordings are automatically saved to Google's Cloud for a period of 10 days as part of the Nest Cam subscription plan. After 10 days, the recordings are deleted.~~ Recordings are automatically saved to a cloud based platform for a period of up to 4 days as part of a subscription plan. After the retention period, the recordings are automatically deleted.

5. ~~Questions & Concerns~~



CITY AND COUNTY OF SAN FRANCISCO
DEPARTMENT OF ELECTIONS

John Arntz, Director

March 9, 2026

Angela Calvillo
Clerk of the Board of Supervisors
1 Dr. Carlton B. Goodlett Place, Room 244
San Francisco, California 94102

Dear Ms. Calvillo:

Attached please find the necessary documents for a department submission to amend its policies regarding surveillance technology for the Board of Supervisors' review and approval.

The Department of Elections seeks to amend its policies regarding the use of surveillance technology. The amendments are based on the Department using cameras other than the Google Nest cameras referenced in the Department's existing policy. The reason for the change is the Nest cameras will no longer receive software updates.

This amended policy allows more flexibility in the cameras used since a specific vendor is not stated as the provider. The amendments also reduce the timeframe for retaining any recorded footage from 10 days to four.

I will gladly answer any questions.

Respectfully,


John Arntz, Director

Encl:

Attachment 1: Amended Surveillance Technology Policy

Attachment 2: Redline version of Amended Surveillance Policy

From: [Arntz, John \(REG\)](#)
To: [BOS Legislation, \(BOS\)](#)
Cc: [FLORES, ANA \(CAT\)](#)
Subject: RE: Checklist for submitting amendments to ordinance regarding surveillance technology
Date: Monday, March 9, 2026 1:34:55 PM
Attachments: [Cover Letter - Amended Tech Policy - Elections - March 2026.pdf](#)
[Amended Surveillance Tech Policy - Leg. Digest.docx](#)
[Amended Surveillance Tech Policy Ordinance - Dept. of Elections - Final.docx](#)
[image001.png](#)
[Attachment 1 - Elections Security Camera Policy \(2026\) - FINAL.pdf](#)
[Attachment 2 - Elections Security Camera \(2026\) Redlined.pdf](#)

Hello. The Department of Elections seeks amendments to its policy on surveillance technology. The attached documents provide the leg digest, ordinance, cover letter, and two attachments.

I cc'd DCA Ana Flores so that she can respond to any questions regarding the ordinance being appropriate according to form.

Please let me know if there are any questions.

Thanks,
-John.

John Arntz, Director
San Francisco Department of Elections
1 Dr. Carlton B. Goodlett Place
City Hall, Room 48
San Francisco, CA 94102
(415) 588-6100
www.sfelections.gov

From: BOS Legislation, (BOS) <bos.legislation@sfgov.org>
Sent: Friday, February 6, 2026 11:35 AM
To: Arntz, John (REG) <john.arntz@sfgov.org>; BOS Legislation, (BOS) <bos.legislation@sfgov.org>
Subject: RE: Checklist for submitting amendments to ordinance regarding surveillance technology

Hi Director Arntz,

Please see a list of documents needed for introduction:

- Cover Letter on Department letterhead (pdf)
- Proposed Ordinance in Word
- Email approving as to form the proposed Ordinance and confirming signature from the

Deputy City Attorney

- Legislative Digest in Word for Ordinances longer than two pages
- Any supporting documents (PDF) referenced in the Ordinance

Department introductions should be emailed to bos.legislation@sfgov.org. Please let us know if you have any further questions. Thank you.

Best regards,

Jocelyn Wong

Legislative Clerk

San Francisco Board of Supervisors

1 Dr. Carlton B. Goodlett Place, Room 244

San Francisco, CA 94102

T: 415.554.7702 | F: 415.554.5163

jocelyn.wong@sfgov.org | www.sfbos.org



Click [here](#) to complete a Board of Supervisors Customer Service Satisfaction form

The [Legislative Research Center](#) provides 24-hour access to Board of Supervisors legislation, and archived matters since August 1998.

***Disclosures:** Personal information that is provided in communications to the Board of Supervisors is subject to disclosure under the California Public Records Act and the San Francisco Sunshine Ordinance. Personal information provided will not be redacted. Members of the public are not required to provide personal identifying information when they communicate with the Board of Supervisors and its committees. All written or oral communications that members of the public submit to the Clerk's Office regarding pending legislation or hearings will be made available to all members of the public for inspection and copying. The Clerk's Office does not redact any information from these submissions. This means that personal information—including names, phone numbers, addresses and similar information that a member of the public elects to submit to the Board and its committees—may appear on the Board of Supervisors' website or in other public documents that members of the public may inspect or copy.*

From: Arntz, John (REG) <john.arntz@sfgov.org>

Sent: Friday, February 6, 2026 11:28 AM

To: BOS Legislation, (BOS) <bos.legislation@sfgov.org>

Subject: Checklist for submitting amendments to ordinance regarding surveillance technology

Hello. Elections needs to submit a proposed ordinance to amend its surveillance technology policy and needs the checklist of items and procedures to follow regarding such submissions.

Please let me know if I can answer any questions regarding this request.

Thanks,

-John.

John Arntz, Director
San Francisco Department of Elections
1 Dr. Carlton B. Goodlett Place
City Hall, Room 48
San Francisco, CA 94102
(415) 554-4375
www.sfelections.gov

From: [Flores, Ana \(CAT\)](#)
To: [BOS Legislation, \(BOS\)](#); [Arntz, John \(REG\)](#); [BOS Legislation, \(BOS\)](#)
Subject: RE: Checklist for submitting amendments to ordinance regarding surveillance technology
Date: Monday, March 9, 2026 2:35:43 PM
Attachments: [image003.png](#)

This is approved as to form. You have my permission to use my electronic signature.

Thanks,



Ana I. Flores
Deputy City Attorney
Office of City Attorney David Chiu
(415) 554-4661 Direct
1 Dr. Carlton B. Goodlett Place, Suite 234
San Francisco, CA 94102
www.sfcityattorney.org

CONFIDENTIALITY NOTICE: This communication and its contents may contain confidential and/or legally privileged information. It is solely for the use of the intended recipient(s). Unauthorized interception, review, use or disclosure is prohibited and may violate applicable laws, including the Electronic Communications Privacy Act. If you are not the intended recipient, please contact the sender and destroy all copies of the communication.

From: BOS Legislation, (BOS) <bos.legislation@sfgov.org>
Sent: Monday, March 9, 2026 1:43 PM
To: Arntz, John (REG) <john.arntz@sfgov.org>; BOS Legislation, (BOS) <bos.legislation@sfgov.org>
Cc: Flores, Ana (CAT) <Ana.Flores@sfcityatty.org>
Subject: RE: Checklist for submitting amendments to ordinance regarding surveillance technology

Thank you Director Arntz. We are seeking the approval from Deputy City Attorney Ana Flores for use of her electronic signature and approval as to form for the proposed Ordinance, by reply to this email. This is slated to be introduced for March 24, 2026.

Best regards,

Jocelyn Wong

Legislative Clerk

San Francisco Board of Supervisors

1 Dr. Carlton B. Goodlett Place, Room 244

San Francisco, CA 94102

T: 415.554.7702 | F: 415.554.5163

jocelyn.wong@sfgov.org | www.sfbos.org



Click [here](#) to complete a Board of Supervisors Customer Service Satisfaction form

The [Legislative Research Center](#) provides 24-hour access to Board of Supervisors legislation, and archived matters since August 1998.

***Disclosures:** Personal information that is provided in communications to the Board of Supervisors is subject to disclosure under the California Public Records Act and the San Francisco Sunshine Ordinance. Personal information provided will not be redacted. Members of the public are not required to provide personal identifying information when they communicate with the Board of Supervisors and its committees. All written or oral communications that members of the public submit to the Clerk's Office regarding pending legislation or hearings will be made available to all members of the public for inspection and copying. The Clerk's Office does not redact any information from these submissions. This means that personal information—including names, phone numbers, addresses and similar information that a member of the public elects to submit to the Board and its committees—may appear on the Board of Supervisors' website or in other public documents that members of the public may inspect or copy.*

From: Arntz, John (REG) <john.arntz@sfgov.org>
Sent: Monday, March 9, 2026 1:35 PM
To: BOS Legislation, (BOS) <bos.legislation@sfgov.org>
Cc: FLORES, ANA (CAT) <Ana.Flores@sfcityatty.org>
Subject: RE: Checklist for submitting amendments to ordinance regarding surveillance technology

Hello. The Department of Elections seeks amendments to its policy on surveillance technology. The attached documents provide the leg digest, ordinance, cover letter, and two attachments.

I cc'd DCA Ana Flores so that she can respond to any questions regarding the ordinance being appropriate according to form.

Please let me know if there are any questions.

Thanks,
-John.

John Arntz, Director
San Francisco Department of Elections
1 Dr. Carlton B. Goodlett Place
City Hall, Room 48
San Francisco, CA 94102
(415) 588-6100
www.sfelections.gov

From: BOS Legislation, (BOS) <bos.legislation@sfgov.org>
Sent: Friday, February 6, 2026 11:35 AM

To: Arntz, John (REG) <john.arntz@sfgov.org>; BOS Legislation, (BOS) <bos.legislation@sfgov.org>
Subject: RE: Checklist for submitting amendments to ordinance regarding surveillance technology

Hi Director Arntz,

Please see a list of documents needed for introduction:

- Cover Letter on Department letterhead (pdf)
- Proposed Ordinance in Word
- Email approving as to form the proposed Ordinance and confirming signature from the Deputy City Attorney
- Legislative Digest in Word for Ordinances longer than two pages
- Any supporting documents (PDF) referenced in the Ordinance

Department introductions should be emailed to bos.legislation@sfgov.org. Please let us know if you have any further questions. Thank you.

Best regards,

Jocelyn Wong

Legislative Clerk

San Francisco Board of Supervisors

1 Dr. Carlton B. Goodlett Place, Room 244

San Francisco, CA 94102

T: 415.554.7702 | F: 415.554.5163

jocelyn.wong@sfgov.org | www.sfbos.org



Click [here](#) to complete a Board of Supervisors Customer Service Satisfaction form

The [Legislative Research Center](#) provides 24-hour access to Board of Supervisors legislation, and archived matters since August 1998.

***Disclosures:** Personal information that is provided in communications to the Board of Supervisors is subject to disclosure under the California Public Records Act and the San Francisco Sunshine Ordinance. Personal information provided will not be redacted. Members of the public are not required to provide personal identifying information when they communicate with the Board of Supervisors and its committees. All written or oral communications that members of the public submit to the Clerk's Office regarding pending legislation or hearings will be made available to all members of the public for inspection and copying. The Clerk's Office does not redact any information from these submissions. This means that personal information—including names, phone numbers, addresses and similar information that a member of the public elects to submit to the Board and its committees—may appear on the Board of Supervisors' website or in other public documents that members of the public may inspect or copy.*

From: Arntz, John (REG) <john.arntz@sfgov.org>

Sent: Friday, February 6, 2026 11:28 AM

To: BOS Legislation, (BOS) <bos.legislation@sfgov.org>

Subject: Checklist for submitting amendments to ordinance regarding surveillance technology

Hello. Elections needs to submit a proposed ordinance to amend its surveillance technology policy and needs the checklist of items and procedures to follow regarding such submissions.

Please let me know if I can answer any questions regarding this request.

Thanks,
-John.

John Arntz, Director
San Francisco Department of Elections
1 Dr. Carlton B. Goodlett Place
City Hall, Room 48
San Francisco, CA 94102
(415) 554-4375
www.sfelections.gov

1 [Administrative Code - Department of Elections Amended Surveillance Technology Policy]

2
3 **Ordinance approving the amended Surveillance Technology Policy for the Department**
4 **of Election's continued use of security cameras and making required findings in**
5 **support of said approvals.**

6
7 NOTE: **Unchanged Code text and uncodified text** are in plain Arial font.
8 **Additions to Codes** are in *single-underline italics Times New Roman font*.
9 **Deletions to Codes** are in ~~*strikethrough italics Times New Roman font*~~.
10 **Board amendment additions** are in double-underlined Arial font.
11 **Board amendment deletions** are in ~~Arial font~~.
12 **Asterisks (* * * *)** indicate the omission of unchanged Code
13 subsections or parts of tables.

14 Be it ordained by the People of the City and County of San Francisco:

15 Section 1. Background.

16 (a) Terms used in this ordinance have the meaning set forth in Administrative Code
17 Chapter 19B ("Chapter 19B").

18 (b) Chapter 19B regulates City Departments' acquisition and use of Surveillance
19 Technology. Under Section 19B.5, City Departments that possessed or were using
20 Surveillance Technology before Chapter 19B took effect in July 2019 must obtain Board of
21 Supervisors ("Board") approval by ordinance of a Surveillance Policy for each type of existing
22 Surveillance Technology. Under Section 19B.2(a), a Department must obtain Board approval
23 by ordinance of a Surveillance Technology Policy before: (1) seeking funds for Surveillance
24 Technology; (2) acquiring or borrowing new Surveillance Technology; (3) using new or
25 existing Surveillance Technology for a purpose, in a manner, or in a location not specified in a
Surveillance Technology Policy ordinance approved by the Board in accordance with Chapter

1 19B; (4) entering into agreement with a non-City entity to acquire, share, or otherwise use
2 Surveillance Technology; or (5) entering into an oral or written agreement under which a non-
3 City entity or individual regularly provides the Department with data or information acquired
4 through the entity’s use of Surveillance Technology.

5 (c) Under Administrative Code Section 19B.2(b), the Board may approve a
6 Surveillance Technology Policy ordinance under Section 19B.2(a) if: (1) the Department
7 seeking Board approval under subsection (a) creates a Surveillance Technology Policy and
8 Surveillance Impact Report for the Surveillance Technology to be acquired or used; and (2) at
9 a public hearing at which the Committee on Information Technology (“COIT”) considers the
10 Surveillance Technology Policy, COIT recommends that the Board adopt, adopt with
11 modifications, or decline to adopt the Surveillance Technology Policy for the Surveillance
12 Technology to be acquired or used.

13 (d) Under Administrative Code Section 19B.2(m), any amendment to an existing
14 Surveillance Technology Policy shall be submitted directly to the Board and not to COIT.

15 (e) The Amended Surveillance Technology Policy (“Amended Policy”) revises and
16 replaces the Department of Elections’ (“Elections”) current Surveillance Technology Policy
17 regarding indoor security cameras, to live stream ballot processing and election-related
18 operations, which the Board approved in Ordinance No. 245-22, on file with the Clerk of the
19 Board in File No. 221043. The Amended Policy is on file with the Clerk of the Board in File
20 No. ___ and incorporated herein by reference.

21 (f) This ordinance sets forth the Board’s findings in support of the Amended Policy and
22 its approval of the Amended Policy.

23
24 Section 2. Use of Indoor Security Cameras.
25

1 (a) As authorized by Ordinance No. 245-22, Elections currently possesses and uses
2 indoor security cameras.

3 (b) Elections uses the indoor security cameras to: (1) conduct live monitoring of voting
4 center lines; (2) conduct live monitoring of ballot processing and election-related operations;
5 (3) share live streaming footage of the Department ballot processing and election-related
6 operations with the public to promote transparency into elections operations, and (4) review
7 camera footage in the event of an incident.

8 (c) The current policy specifies a particular vendor, Google, that Elections has used to
9 provide indoor security cameras. The Amended Policy allows Elections the flexibility to use
10 other vendors that offer the same services and are approved by the City.

11 (d) The current policy provides for a retention period of 10 days on Google's Cloud,
12 after which recorded footage is automatically deleted. The Amended Policy reduces the
13 retention period from 10 days to four days and allows Elections the flexibility to use any cloud-
14 based platform approved by the City.

15 (e) The current policy specifies that recordings are accessible only to authorized staff
16 of Elections. The Amended Policy updates the list with current applicable job codes.

17
18 Section 3. Findings and Approval of the Amended Policy.

19 (a) The Board hereby finds that the benefits that Elections' Amended Policy authorizes
20 outweigh the costs and risks; that the Amended Policy will safeguard civil liberties and civil
21 rights; and that the uses and deployments by Elections of indoor security cameras, as set
22 forth in the Amended Policy, will not be based upon discriminatory or viewpoint-based factors
23 or have a disparate impact on any community or Protected Class.

24 (b) The Board hereby approves the Department of Elections' Amended Policy for use
25 of indoor security cameras.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

Section 4. Effective Date. This ordinance shall become effective at 12:00 a.m. on the 31st day after enactment. Enactment occurs when the Mayor signs the ordinance, the Mayor returns the ordinance unsigned or does not sign the ordinance within 10 days of receiving it, or the Board of Supervisors overrides the Mayor’s veto of the ordinance.

APPROVED AS TO FORM:
DAVID CHIU, City Attorney

By: /s/ Ana Flores
ANA I. FLORES
Deputy City Attorney

4917-1187-7259, v. 3