Surveillance Technology Policy

People Counting System
Recreation and Parks

The City and County of San Francisco values 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 People Counting 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 Department's mission is to

provide enriching recreational activities, maintain beautiful parks, and preserve the environment for the well-being of everyone in our diverse community.

The Surveillance Technology Policy ("Policy") defines the manner in which the People Counting System will be used to support this mission, by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all to department personnel that use, plan to use, or plan to secure People Counting System, 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

The authorized use of People Counting System technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

- *Obtain occupancy data on visitors into and out of parks and facilities*

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

Departments may use information collected from technology 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.

BUSINESS JUSTIFICATION

Reason for Technology Use

The surveillance technology supports the Department's mission and provides important operational value in the following ways:

People counters help the department provide enriching recreational activities by 1) providing estimates of the popularity of drop-in programming and events, for which we do not have registration data; 2) helping calibrate cleaning schedules so our enriching recreational activities may be provided in facilities that are as well-kept as possible; 3) enabling us to provide timely, robust estimates of visitorship to key stakeholders and partners.

Description of Technology

A sensor mounted above an entry point obtains 3D stereo vision image data of activity within a pre-determined field of vision. A software algorithm analyzes this field of vision and when an image meets the algorithm's definition of a human shape, it is tracked. If the shape traverses a plane within the sensor's field of vision pre-defined as an entry or exit point, a data point is recorded as an 'In' or 'Out'. This data is then transmitted via XML to a cloud-based database. This aggregated count data is accessible to end users via API and a web-based content management system.

Resident Benefits

The surveillance technology promises to benefit residents in the following ways:

	Benefit	Description
☐	Education	
☐	Community Development	
X	Health	Recreational programs and activities benefit residents' health by providing readily available, low to no-cost opportunities to keep active. By using data to inform our service offerings we are able to incentivize residents to participate in healthy activities by offering programs and activities they will enjoy at locations that are convenient to them
☐	Environment	
☐	Criminal Justice	
☐	Jobs	
☐	Housing	
X	Other: Recreation	These technologies help the department improve its recreational offerings by allowing us to estimate attendance at unstructured, drop-in events, programs, and activities. With occupancy data we are better able to advocate for funding of recreational programs and activities.

Department Benefits

The surveillance technology will benefit the department in the following ways:

	Benefit	Description
X	Financial Savings	Occupancy sensors are less costly than full-time employee equivalents for counting visitors into and out of facilities, thus providing the department financial savings.
X	Time Savings	Data collected by occupancy sensors are automatically uploaded to a database and rendered into pre-formatted reports, saving the department considerable time from having to perform data entry and report generation manually.
☐	Staff Safety	
X	Data Quality	Occupancy sensors provide robust, reliable data on occupancy and are less prone to error and mismeasurement than in-person surveys, thus improving data quality.
☐	Other	

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 the surveillance technology must be up to date and maintained.

Data Collection: Department shall only collect data required to execute the authorized use cases. 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 type(s):

Data Type(s)	*Format(s)*	*Classification*
Scanned humanoid shapes	XML	Level 3
Numerical Data (date, time, count,	XML	Level 1

and a direction component (in or out)		
Live Monitoring	Not recorded or stored – only used for calibration	Level 3
Live Recording	.xvr (proprietary and only used for calibration)	Level 3

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

Department includes the following items in its public notice:

- Contact information
- Data Retention
- Description of the authorized use
- Information on the surveillance technology
- Type of data collected

Access: All parties requesting access must adhere to the following rules and processes:

- Prior to accessing or using data, authorized individuals receive training and instruction regarding authorized uses, accessing data, and running reports.

A. Department employees

Once collected, the following roles and job titles are authorized to access and use data collected, retained, processed or shared by the surveillance technology:

- 1054: Principal IS Business Analyst; 1052: Sr. IS Business Analyst; 1820 Admin. Analyst Series; 0941 Manager VI; 1040 IS engineer series; 1090 IT Operations Support series

B. Members of the public

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.

Collected data that is classified as Level 1-Public data may be made available for public access or release via DataSF's Open Data portal. Open Data has a Public Domain Dedication and License, and makes no warranties on the information provided. Once public on Open Data, data can be freely shared, modified, and used for any purpose without any restrictions. Any damages resulting from use of public data are disclaimed.

Members of the public may also request access by submission of a request pursuant to San Francisco's Sunshine Ordinance. No record shall be withheld from disclosure in its entirety unless all information contained in it is exempt from disclosure under express provisions of the California Public Records Act or some other statute.

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.

At the very least, department shall require all elected officials, employees, consultants, volunteers, and vendors working with the technology on its behalf to read and formally acknowledge all authorized and prohibited uses. Department shall also require that all individuals requesting data or regularly requiring data access receive appropriate training before being granted access to systems containing PII.

All staff accessing Sensource data are given one-time training and instruction regarding authorized uses, accessing data, and running reports.

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.

Department shall ensure compliance with these security standards through the following:

Access to data will be limited only to the Chief Information Officer or designee.

Data Storage: Data will be stored in the following location:

- X Local storage (e.g., local server, storage area network (SAN), network attached storage (NAS), backup tapes, etc.)
- ☐ Department of Technology Data Center

X Software as a Service Product

☐ Cloud Storage Provider

Reports are stored as local storage files; count data recorded by the sensors are stored within a cloud-based content management system.

Data Sharing:

Department will endeavor to ensure that other agencies or departments that may receive data collected by the surveillance technology will act in conformity with this Policy.

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 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. *(See Data Security)*

Department shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded from entities that do not have authorized access under this policy.

Further, in sharing data, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual person, data concerning health or data concerning an individual person's sex life or sexual orientation shall be prohibited.

Each department that believes another agency or department receives or may receive data collected from its use of surveillance technologies should consult with its assigned deputy city attorney regarding their legal obligations.

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

- Confirm the purpose of the data sharing aligns with the department's mission.
- Consider alternative methods other than sharing data that can accomplish the same purpose.
- Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies.
- Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.
- 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.

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

A. Internal Data Sharing:

The department shares the following data with recipients within the City and County of San Francisco:

Data Type	Data Recipient
Aggregate data on the number of people entering and exiting a facility by date, time, and location. No personally identifiable information is accessed or shared.	Planning; BOS; Mayor's Office; SFCTA; DPW. All by request on an ad-hoc basis.

Frequency - Data sharing occurs at the following frequency:
Once per month on average.

B. External Data Sharing:

The department shares the following data with recipients external to the City and County of San Francisco:

Data Type	Data Recipient
Aggregate data on the number of people entering and exiting a facility by date, time, and location. No personally identifiable information is accessed or shared.	Non-profit & philanthropic organizations; analytics services; only aggregate count data is provided--no PII.

Frequency - Data sharing occurs at the following frequency:
Once per month on average.

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:

Retention Period	Retention Justification
Count data provided by the sensors will be retained long-term to maintain a historical record of visits to parks and facilities in order to facilitate comparisons over time. Reports and analyses compiled from the data are current records which may be but are not required to be retained. The department does not record or store PII captured by these systems.	The long-term time period is necessary in order to analyze historical trends in facility usage.

PII data shall not be kept in a form which permits identification of data subjects for any longer than is necessary for the purposes for which the personal data are processed.

Exceptions to Retention Period - PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s):

- There are no exceptions to the retention period.

Departments must establish appropriate safeguards for PII data stored for longer periods.

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

- Practices: Count data recorded by the sensors will be retained long-term. Reports compiled from the data may be retained or manually deleted as necessary. No personally identifiable information is recorded or stored.
- Processes and Applications: No personal identifiable information is retained.

COMPLIANCE

Department Compliance

Department shall oversee and enforce compliance with this Policy using the following methods:

The Chief Information Officer or designee will be responsible for enforcing the Surveillance Technology policy by 1) reviewing at the time of purchase the vendor's privacy protections and policies to ensure PII is redacted and/or not retained during the vendor's quality assurance process; and 2) ensuring the technology is only used for approved use cases.

Interdepartmental, Intergovernmental & Non-Governmental Entity Compliance

To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall:

The Chief Information Officer or designee will be responsible for enforcing the Surveillance Technology policy through recurring review of functionality and use.

Oversight Personnel

Department shall be assigned the following personnel to oversee Policy compliance by the Department and third-parties:

- Chief Information Officer (0941) or designee
- Administrative Analyst (1820 series)
- Planner (5291 series)

Sanctions for Violations - Sanctions for violations of this Policy include the following:

Violation of the policy will be subject to departmental policies, including Human Resources policies governing professional conduct. Disciplinary action up to and including termination may be invoked to enforce violations of the Surveillance Technology Policy.

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.

EXCEPTIONS

Only in exigent circumstances or in circumstances where law enforcement requires surveillance technology data for investigatory or prosecutorial functions may data collected, retained or processed by the surveillance technology be shared with law enforcement.

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.

Raw Data:	Information collected by a surveillance technology that has not been processed and cleaned of all personal identifiable information. The distribution and use of raw data is tightly restricted.
Exigent Circumstances	An emergency involving imminent danger of death or serious physical injury to any person that requires the immediate use of Surveillance Technology or the information it provides.

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."

QUESTIONS & CONCERNS

Public Inquiries

Members of the public may register complaints or concerns, or submit questions about the deployment of the Surveillance Technology via written correspondence to McLaren Lodge in Golden Gate Park, 501 Stanyan Street, San Francisco 94117; the department's main telephone line at 415-831-2700; email at rpdinfo@sfgov.org; or via 311.

Department shall acknowledge and respond to complaints and concerns in a timely and organized response, and in the following manner:

Calls, emails, written correspondence and 311 requests regarding the surveillance technology policy are routed to the department's information technology division's HelpDesk and logged in the the department's request management system. Once a request is logged, the information technology division will work with relevant parties to resolve the issue. Review of open/closed requests occurs with the department's Chief Information Officer on a weekly basis.

Inquiries from City and County of San Francisco Employees

All questions regarding this policy should be directed to the employee's supervisor or to the director. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the employee's supervisor or the director.

APPENDIX: SenSource SaaS Services Agreement Section 4.2—use of de-identified or aggregated customer data

4.2 Notwithstanding anything to the contrary, Sensource shall have the right to collect, analyze and aggregate data and other information relating to the provision, use and performance of various aspects of the Solution and related systems and technologies (including, without limitation, information concerning de-identified or aggregated Customer Data and data derived therefrom, but excluding any statistical information specific to You obtained or generated from Your use of the Solution and Software), and SenSource will be free (during and after the term hereof) to (i) use such information and data to improve and enhance the Solution and for other development, diagnostic and corrective purposes in connection with the Solution and other SenSource offerings, and (ii) disclose such data solely in aggregate or other de-identified form in connection with its business. No rights or licenses are granted except as expressly set forth herein.