Surveillance Technology Policy

Recreation & Parks Department
Automatic License Plate Reader (ALPR)

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 ALPR 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 our diverse community.

The Surveillance Technology Policy ("Policy") defines the manner in which the ALPR 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 ALPR, 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 ALPR technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

1. To support local, state, federal, and regional public safety departments in the identification of vehicles associated with targets of criminal investigations, including investigations of serial crimes
2. To protect the public and our staff at special events from misconduct and/or violent confrontations.
3. To protect critical infrastructure sites from vandalism, theft and damage.

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

Departments may use information collected 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

ALPR supports the Department's mission and provides important operational value in the following ways:

- ALPRs are used to protect the public and our staff in our parks and playgrounds and at special events. In addition, ALPRs are used to protect our critical infrastructure sites.

In addition, ALPR promises to benefit residents in the following ways:

	▪ Education	
	▪ Community Development	
	▪ Health	
	▪ Environment	
X	Criminal Justice	Coordination with law enforcement or first responders for all approved requests. Approved requests include criminal activities such as auto burglaries, personal theft, assaults, robberies, vehicle theft, and vehicle accidents.
	▪ Jobs	
	▪ Housing	
X	Other	Public Safety - to protect the public and our staff in our parks and playgrounds and at special events.

In addition, the following benefits are obtained:

Benefit		Description
	▪ Financial Savings	
	▪ Time Savings	
X	Staff Safety	To protect our staff in our parks and playgrounds, and at special events.
	▪ Data Quality	
	▪ Service Levels	

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 kept up to date and maintained.
Safety:	Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage.
Data Collection:	Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology. 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. Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data. The surveillance technology collects the following data types:

Data Type(s)	*Format(s)*	*Classification*
Images of license plates	AVI, MOV, MP3, JPG	Level 3
Date & time image taken	AVI, MOV, MP3, JPG	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. 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:

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

Access:

All parties requesting access must adhere to the following rules and processes: RecPark does not consistently monitor the cameras. RecPark only reviews the video files after an incident has occurred. Request may come from RecPark or law enforcement.

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.

- 8210 - Head Park Ranger, SF Rec Park

The following providers are required to support and maintains the surveillance technology and its associated data to ensure it remains functional:

B. Members of the public

Recreation and Parks 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. Anyone, including criminal defendants, may access such data. 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, including by criminal defendants.

Members of the public, including criminal defendants, 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.

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). To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards: ALPR data shall only be utilized for legitimate park enforcement purposes, or at the request other law enforcement agencies. Access to ALPR data is limited to 8210 and above management levels in the Park Ranger unit.
Data Sharing:	Recreation and Parks 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. Recreation and Parks will endeavor to ensure that other agencies or departments that may receive data collected by [the Surveillance Technology Policy that it operates] will act in conformity with this Surveillance Technology 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. Recreation and Parks 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) Recreation and Parks shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded. Each department that believes another agency or department receives or may receive data collected from its use of STs should consult with its assigned deputy city attorney regarding their response. *A. Internal Data Sharing* Department shares the following data with the recipients: The department does not share surveillance technology data with other departments or entities inside the City and County of San Francisco. Data sharing occurs at the following frequency: Upon request. Before sharing data with any recipients, the Department will use the following procedure to ensure appropriate data protections are in place:

The Department currently participates in the following sharing practices:

X	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.
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.

B. External Data Sharing

Department shares the following data with the recipients:

- Approved requests from other law enforcement agencies e.g. SFPD, District Attorney, Public Defender. Approved requests include criminal activities such as auto burglaries, personal theft, assaults, robberies, vehicle theft, and vehicle accidents.

Data sharing occurs at the following frequency:

- Upon request

Data Retention:

Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose.

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

- ALPR video files will be retained for 30-60 days (depending upon the hardware capacity).
- Hardware capacity (files are overwritten when storage is full).

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. PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s):

	Any requested files will be saved in the request management software used to manage all requests for surveillance technology. The files will be maintained for up to two years or if a case has been closed. Departments must establish appropriate safeguards for PII data stored for longer periods. Data may be stored in the following location: ▪ 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
Data Disposal:	Upon completion of the data retention period, Department shall dispose of data in the following manner: Practices: All ALPR data is stored in the local hardware and is delated 30-60 days from the date it was collected. The system overwrites the data when hard drive is full. There is no manual deletion of any data. For any requested data that is stored in the request management software used to manage all requests for surveillance technology, there will be a process to delete the data after two years if still available. Processes and Applications: None
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. Training is provided by the installation vendor - Microbiz.

COMPLIANCE

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

IT will work closely with the Park Rangers to ensure that the Surveillance Technology Policy for ALPRs will be supported. Procurement of all technical hardware and software is led by IT. Additionally, asset and request management of all ALPRs is led by IT.

Department shall assign the following personnel to oversee Policy compliance by the Department and third-parties.

Lieutenant Marcus Santiago (SFRPRD Park Ranger), Christine Nath (SFRPRD CIO)

Sanctions for violations of this Policy include the following:

Violation of the policy will be subject to standard RecPark departmental policies, which may include disciplinary action up to and including termination.

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.
Sensitive Data:	Data intended for release on a need-to-know basis. Data regulated by privacy laws or regulations or restricted by a regulatory agency or contract, grant, or other agreement terms and conditions.

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:

Complaints or concerns can be submitted to the Department by

Members of the public can register complaints/concerns or submit questions to San Francisco Recreation and Parks through several ways: 1.) Send written correspondence to McLaren Lodge in Golden Gate Park, 501 Stanyan Street, San Francisco, CA 94117; 2.) Call to the RPD Front Desk 415-831-2700; 3.) Send an email to rpdinfo@sfgov.org; 4.)Contact 311.

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall:

All ALPR calls/complaints from the public received via mail or via call to the RPD Front Desk are routed to the RPD IT HelpDesk and logged in our department's request management system. Any requests from 311 are received in our department's dispatch system and routed to the RPD IT HelpDesk which then is logged in the request management system.

Once the request is tracked in the request management system, IT will work with all relevant parties to ensure completion.

Review of open / closed requests occur with the CIO on a weekly basis.

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.