Surveillance Technology Policy

Police Accountability
AI and Algorithms

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 *AI and Algorithms* 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 of Police Accountability is committed to providing the City of San Francisco with independent and impartial law enforcement oversight through investigations, policy recommendations, and performance audits to ensure that policing reflects the values and concerns of the community.

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

Authorized Use(s):

Authorized Use Case #1	*To redact the following:* • *Faces of witnesses and bystanders to conceal identities of complainants and witnesses.* • *Residential addresses of complainants and witnesses to conceal identities of complainants and witnesses.* • *Personally-identifiable information such as the residential addresses of complainants, victims, and witnesses.* • *Personally-identifiable information such as driver licenses of complainants, victims, and witnesses.* • *Other information that would reveal the identity of a complainant, victim, or witness, such as a family photograph appearing inside a residence.*

COIT Policy Dates
Approved:

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

Further, 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.

BUSINESS JUSTIFICATION

AI and Algorithms support the Department's mission and provides important operational value in the following ways:

- To comply with state public records law and will also help support DPA's mission of police accountability through transparency. This technology is needed because Penal Code 832.7 requires DPA to redact and release video related to officer-involved shootings, great bodily injury cases, incidents where an officer commits a sexual assault, and incidents where an officer is dishonest.

- To redact the faces of complainants and witnesses, bystanders, juveniles, and victims. The tool will be used to redact video that already exists. The tool will enable DPA to protect the identities of people who appear in police incident video.

- [Note: The DPA will not use the tool to record anything. The tool will be used to redact videos that were already recorded by the police department and other third parties. Purchasing this tool will not cause any new video to be recorded. DPA will only use the tool on existing video that is sent to DPA in connection with police misconduct investigations. The California Public Records Act requires DPA to publicly disclose witness, surveillance, and body-worn camera video gathered in connection with certain categories of police misconduct cases. Members of the public appear in these videos and, to protect their identities, their faces must be blurred before the records are published. The redaction tool will enable DPA to protect the privacy of community members while complying with state laws requiring the disclosure of video related to police incidents.]

In addition, the Video Redaction Tool promises to benefit residents in the following ways:

Education: *Public record disclosures related to police accountability are used by journalists and educators to inform the public and to educate law enforcement and other oversight agencies by examining the outcomes and impact of police actions.*

Public Safety: *Transparency is one of the four pillars of procedural justice, which is required for effective community policing. A media redaction tool will enable DPA to publicly disclose policing videos so that community members can participate in policing reform initiatives in a meaningful and educated way.*

The Video Redaction Tool will benefit the department in the following ways:

Financial savings: *The video redaction tool automates time-consuming video edits. Billing is based on the length of the edited video, not how long it takes to edit the video. By contrast, vendors charge by the*

number of hours to complete a task. Example. Using vendors to release a 1 hour video would entail: 1) paying $250 to transcribe the video, 2) reviewing the transcript internally and marking it for redaction (2 staff hours), 3) sending the video and transcript to a video redaction vendor for an estimated cost of $400, 4) reviewing the redacted video for accuracy (3 staff hours). Using an in-house tool to release a 1-hour video would entail: 1) a staff person would spend 2-3 hours reviewing and redacting the video, 2) other staff would spend 2 hours checking for accuracy, 3) DPA would be charged approximately $60 in vendor fees.

Time savings: *Based on peer experiences, it is estimated to take five times the length of a video to redact faces and other personally-identifiable information using traditional software. Because of the automatic shape tracking, DPA estimates that it will take only 2-3 times the length of a video to perform redactions. Compared with using a vendor, using an in-house tool will use approximately 50% fewer staff hours per hour of redacted video.*

Improved data quality: *The shape-tracking tool will enable more precise blurring redactions than traditional editing tools.*

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.

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.

Data types can take the form video, audio, still images. Data formats can take the form of XML, PDF, HTML, Plain Text, JPEG, etc. The surveillance technology collects the following data types and formats

- JPEG
- PNG
- MOV
- AVI
- CSV

Notification: N/A

Access: All parties requesting access must adhere to the following rules and processes (Please refer to the data sharing section to ensure all information covered in that section is also included below):

Tool will be used by DPA personnel to remove personally-identifiable information from records prior to public disclosure as required by law. DPA will retain both the raw and redacted footage according to document retention policies.

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.

- *8177 Attorney,*
- *8173 Legal Assistant,*
- *0923 Manager II,*
- *1052 Information Systems Business Analyst*

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

- *Veritone*

A data access log will be maintained by the Department for all Video Redaction Tool data that is processed and utilized. Audit logs will be automatically created by the tool. The audit logs will show who accessed information and data stored in the tool.

The data will not be accessible to Veritone employees.

The tool automatically identifies faces and objects to be redacted and suggests redactions. The tool identifies objects by searching for common shapes. For example, the tool scans videos for faces and then suggests that the face be blurred. DPA staff then review the premarked video and suggested redactions. DPA staff approves, edits, and/or enhances the redactions. Examples of edits DPA

staff might make to the AI suggested redactions: 1) DPA staff would decline the suggestion to redact a face on a public billboard. 2) DPA staff would expand a face redaction to include a distinctive beard that hangs below a face. 3) DPA staff will mark distinctive body tattoos for redaction.

Only DPA personnel already authorized to view media will have access to the redaction tool. Access to the tool will be control by unique usernames and passwords. The system can generate a detailed log of edits made by users.

This log may include but is not limited to the following: date/time data was originally obtained/collected, reasons/intended use for data, Bureau/Section requesting data, name of data editor (ie, person accessing raw data for purpose of editing/scrubbing/blurring PII,) date/time of access of raw data, outcome of data processing and signed verification by data editor that all PII was removed, as well as date processed data was delivered to users."

B. Members of the public

Data collected by surveillance technology will not be made generally available to members of the public.

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.

The Police Accountability 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.

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:

Data will be password protected.

Data Sharing: Police Accountability 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.

Police Accountability 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.

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.

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.

The Department currently participates in the following sharing practices

A. Internal Data Sharing – N/A

Department shares the following data with the recipients:

N/A	

Data sharing occurs at the following frequency:

N/A

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 by other means 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 shared data will be done in a cost-efficient manner and exported in a clean, machine-readable format.

The department does not share surveillance technology data with other departments or entities inside the City and County of San Francisco.

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

Please list data retention schedules (i.e., x type of data will be retained for 1 year) based on the following categories:

- Permanent records (i.e., records that are essential): shall be retained and preserved indefinitely
- Current records (i.e., records for operational necessity, ready reference, convenience): record retention schedules may vary but generally less than 10 years
- Storage records (i.e., records retained offsite): record retentions may vary but generally less than 10 years

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

The DPA retains documents in connection with peace officer personnel records (https://index.sfgov.org/taxonomy/term/69.

Penal Code 832.5 required these records to be retained for a minimum of five years.

The DPA will maintain files consistent with peace officer personnel document retention policies as listed on the Index to Records (https://index.sfgov.org/taxonomy/term/69).

The DPA is currently using the Police Department's record retention policy because the DPA is in the process of creating a record retention policy.

The process of creating a new record retention policy is lengthy and DPA anticipates using the Police Department's through the 2022 calendar year.

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):

Exceptions to the standard must be supported with documentation and a clear rationale, and maintained by department staff to be reviewed by COIT.

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

Data will be stored in the following location:

Cloud Storage Provider*: The files will be stored on CJIS-compliant external cloud servers managed by Veritone.*

Vertione staff will not have access to DPA's files.

DPA staff will have full access to all the files that DPA stores on the Veritone tool.

Local Storage*: DPA will also store videos on DPA servers.*

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

Raw data will be erased from all storage devices and servers after one year.

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 applicable to DPA personnel on using the redaction tool and proper storage of data. To learn how to use the redaction software, DPA staff will watch a tutorial produced by the vendor on how to use the editing tools. They will then practice using the tool and have their work reviewed by a supervisor.

COMPLIANCE

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

- *Staff members who edit video using the redaction tool will receive the same training used to view and edit other personnel, HIPAA, and CJIS protected records. All DPA staff members are already trained to protect personally identifiable information, medical information, personnel information, and criminal history records. Using a redaction tool to blur images and edit audio to protect sensitive information does not pose any additional risks to information security from staff.*

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

- *Information Systems Business Analyst in the Police Accountability Department.*

Sanctions for violations of this Policy include the following:

- *Progressive discipline will be used in response to violations of the STP. Progressive discipline is dependent on applicable employee memorandums of agreement. Suggested penalties are a written reprimand for the first offense, a 3-day suspension or termination for a second offense, and 30-days or termination for a third offense.*

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 <u>not</u> 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

<u>Public:</u>

Complaints or concerns can be submitted to the Department by

Members of the public can register complaints/concerns or submit questions via calls to 415-241-7711.

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

In response to an STP complaint, the DPA will investigate the complaint and make findings.

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 A: Surveillance Technology Policy Requirements

The following section shows all Surveillance Technology Policy requirements in order as defined by the San Francisco Administrative Code, Section 19B.

1. A description of the product and services addressed by the Surveillance Technology, including the identity of any provider(s) whose services are essential to the functioning or effectiveness of the Surveillance Technology equipment or services for the intended purpose.
Whether a public information request or police consent decree, agencies are often required to distribute evidence outside the investigative team. Prior to evidence release, sensitive information is required to be redacted to protect the identity of innocent individuals and preserve investigations. With Veritone Redact, you can quickly redact sensitive items within audio, video and image-based evidence and improve the speed and efficiency of which your agency can respond. *The redaction tool will be used to blur the faces of complainants, victims, witnesses. Witnesses can include bystanders, reporting parties, and arrestees. The redaction technology uses artificial intelligence to identify faces and not individuals. The tool identifies face shapes but does not recognize individual faces. The AI tool that identifies objects for redaction is based on shapes and no personal information is stored.* *The video redaction tool is a CJIS-compliant cloud-based application. Videos are uploaded to a secure cloud server and then an AI tool scans the video to suggest images to redact. A staff member then reviews the suggested redactions and accepts, alters, and augments the images marked for redaction. The required redactions are: the faces of involved parties, witnesses, and bystanders; license plates; identification cards; residential addresses; family photos; and other personally-identifiable information.*
2. A description of the purpose(s) for which the Surveillance Technology equipment or services are proposed for acquisition, including the type of data that may be collected by the Surveillance Technology equipment or services.
This technology is needed because Penal Code 832.7 requires DPA to redact and release video related to officer-involved shootings, great bodily injury cases, incidents where an officer commits a sexual assault, and incidents where an officer is dishonest. The tool will enable DPA to comply with state public records law and will also help support DPA's mission of police accountability through transparency. *The DPA will use the tool to redact the faces of complainants and witnesses, bystanders, juveniles, and victims. The tool will be used to redact video that already exists. The tool will enable DPA to protect the identities of people who appear in police incident video. Purchasing this tool will not cause any new video to be recorded. DPA will only use the tool on existing video that is sent to DPA in connection with police misconduct investigations.* *The California Public Records Act requires DPA to publicly disclose witness, surveillance, and body-worn camera video gathered in connection with certain categories of police misconduct*

cases. Members of the public appear in these videos and, to protect their identities, their faces must be blurred before the records are published. The redaction tool will enable DPA to protect the privacy of community members while complying with state laws requiring the disclosure of video related to police incidents.

3. The uses that are authorized, the rules and processes required prior to such use, and uses of the Surveillance Technology that will be expressly prohibited.

Authorized Use Case #1: To redact the following:

- *Faces of witnesses and bystanders to conceal identities of complainants and witnesses.*
- *Residential addresses of complainants and witnesses to conceal identities of complainants and witnesses.*
- *Personally-identifiable information such as the residential addresses of complainants, victims, and witnesses.*
- *Personally-identifiable information such as driver licenses of complainants, victims, and witnesses.*
- *Other information that would reveal the identity of a complainant, victim, or witness, such as a family photograph appearing inside a residence.*

4. A description of the formats in which information collected by the Surveillance Technology is stored, copied, and/or accessed.

JPEG, PNG, MOV, AVI, CSV

5. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information, including restrictions on how and under what circumstances data collected with Surveillance Technology can be analyzed and reviewed, and the rules and processes required prior to access or use of the information.

These are the categories and titles of individuals authorized to access or use information related to this technology:

- *8177 Attorney,*
- *8173 Legal Assistant,*
- *0923 Manager II,*
- *1052 Information Systems Business Analyst*

Data will only be accessible to authorized DPA personnel.

Tool will be used by DPA personnel to remove personally-identifiable information from records prior to public disclosure as required by law. DPA will retain both the raw and redacted footage according to document retention policies.

6. The general safeguards that protect information from unauthorized access, including encryption and access control mechanisms.

Data will be password protected.

7. The limited time period, if any, that information collected by the Surveillance Technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s) enumerated in the Surveillance Technology Policy, the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period
The DPA retains documents in connection with peace officer personnel records (https://index.sfgov.org/taxonomy/term/69). Penal Code 832.5 required these records to be retained for a minimum of five years. *The DPA will maintain files consistent with peace officer personnel document retention policies as listed on the Index to Records (https://index.sfgov.org/taxonomy/term/69). The DPA is currently using the Police Department's record retention policy because the DPA is in the process of creating a record retention policy. The process of creating a new record retention policy is lengthy and DPA anticipates using the Police Department's through the 2022 calendar year.* *Exceptions to the data retention standard must be supported with documentation and a clear rationale, and maintained by department staff to be reviewed by COIT.* *Raw data will be erased from all storage devices and servers after one year.*
8. How collected information can be accessed or used by members of the public
N/A
9. Which governmental agencies, departments, bureaus, divisions, or units that may receive data collected by the Surveillance Technology operated by the Department, including any required justification or legal standard necessary to share that data and how it will ensure that any entity receiving such data complies with the Surveillance Technology Policy.
N/A
10. The training required for any individual authorized to use the Surveillance Technology or to access information collected by the Surveillance Technology
Training applicable DPA personnel on using the redaction tool and proper storage of data. To learn how to use the redaction software, DPA staff will watch a tutorial produced by the vendor on how to use the editing tools. They will then practice using the tool and have their work reviewed by a supervisor.
11. The mechanisms to ensure that the Surveillance Technology Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the sanctions for violations of the policy

Staff members who edit video using the redaction tool will receive the same training used to view and edit other personnel, HIPAA, and CJIS protected records. All DPA staff members are already trained to protect personally identifiable information, medical information, personnel information, and criminal history records. Using a redaction tool to blur images and edit audio to protect sensitive information does not pose any additional risks to information security from staff.

Internal and external entities will only receive data that qualifies as disclosable public records.

The person in charge of compliance is the Information Systems Business Analyst in the Police Accountability Department.

Progressive discipline will be used in response to violations of the STP. Progressive discipline is dependent on applicable employee memorandums of agreement. Suggested penalties are a written reprimand for the first offense, a 3-day suspension or termination for a second offense, and 30-days or termination for a third offense.

12. 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 via calls to 415-241-7711. In response to an STP complaint, the DPA will investigate the complaint and make findings.