# Surveillance Technology Policy

Biometric Electronic Monitoring for Alcohol Use
Adult Probation

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 Biometric Electronic Monitoring for Alcohol Use 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

achieve excellence in community corrections, public safety, and public service through the integration of evidence-based practices and a victim centered approach into our supervision strategies. The Surveillance Technology Policy ("Policy") defines the manner in which the Biometric Electronic Monitoring for Alcohol Use 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 Biometric Electronic Monitoring for Alcohol Use , 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 Biometric Electronic Monitoring for Alcohol Use technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

*Authorized Use(s):*

– *ADP clients can be placed on electronic use of alcohol monitoring based on Court order*

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**

**Surveillance Oversight Review Dates**
PSAB Review: Recommended: October 28, 2022
COIT Review: TBD (list all dates at COIT, and write "Recommended: MM/DD/202X" for rec date)
Board of Supervisors Approval: TBD

Biometric Electronic Monitoring for Alcohol Use supports the Department's mission and provides important operational value in the following ways:

Use of Electronic monitoring (EM) allows clients on supervision to comply with the law, empowers them to make positive changes in their lifestyle while living freely in the community, reduces the likelihood of reoffending, assists them in successful completion of probation and protects the public.

**Description of Technology**

TAD is an alcohol monitoring device worn around the client's ankle 24/7. TAD uses transdermal technology to sample perspiration that passes through the skin. The TAD samples perspiration every minute and records an average of all samples every five minutes. This frequency of sampling provides 288 data points within a 24-hour testing period. Vendor provides application for ADP to access the monitoring data.

**Resident Benefits**

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

| | Benefit | Description |
|---|---|---|
| ▪ | Education | |
| ▪ | Community Development | |
| ▪ | Health | |
| ▪ | Environment | |
| X | Criminal Justice | EM TAB technology allows ADP to monitor clients' compliance with Court orders thus ensuring the safety of residents and the community. |
| ▪ | Jobs | |
| ▪ | Housing | |
| X | Other: Public Safety | EM/TAD technology allows ADP to monitor clients' who have an extensive history with abuse of alcohol. This device monitors their alcohol consumption and notifies ADP if the alcohol has been consumed for appropriate response thus ensuring the safety of residents and the community |

**Department Benefits**

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

| | Benefit | Description |
|---|---|---|
| ▪ | Financial Savings | |

| | | |
|---|---|---|
| X | Time Savings | Having this technology available enhances the efficiency of supervision and decrease the reliance on other agencies. |
| ▪ | Staff Safety | |
| X | Data Quality | Electronic data enhances the accuracy and efficiency of collected data. |
| ▪ | 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* |
|---|---|---|
| Biometric Data (alcohol readings from perspiration) | Binary | Level 4 |

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

- ADP client can be placed on electronic use of alcohol monitoring based on Court order.
- Probation officer has to complete training prior using EM/TAD.

Data must always be scrubbed of PII as stated above prior to public use.

***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:

- Currently, ADP has (85) Class 8444 Deputy Probation Officers and (1) Class 8434 Supervising Probation Officers that have access to this technology.

***B. Members of the public, including criminal defendants***

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.

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 dictated by this policy. 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.

More specifically, Department training will include:

The initial and on-going training for all sworn personnel on how to install, removed and activate/deactivate a TAD, as well as being able to navigate the web application prior to accessing or using the technology.

**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:

The web application includes security measures that allow only authorized personnel to access and use the data.

**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
- Software as a Service Product
- Cloud Storage Provider

**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.

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 |
|---|---|
| Alcohol consumption data, if alcohol has been consumed. | Pursuant to an ongoing investigation and/or court proceeding, the client's data may be shared on a need-to-know basis and/or pursuant to a court order with the Police Department, District Attorney, and Public Defender. |

**Frequency -** Data sharing occurs at the following frequency:
Case by case basis.

**B. External Data Sharing**

Department shares the following data with the recipients:

| Data Type | Data Recipient |
|---|---|
| Alcohol consumption data, if alcohol has been consumed. | Pursuant to an ongoing investigation and/or court proceeding, data regarding individual client may be shared on a need to know basis and/or pursuant to a court order with the Superior Court, or other Law Enforcement Agencies outside of CCSF. |

**Frequency -** Data sharing occurs at the following frequency:
Case by case basis.

**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 |
|---|---|
| Felony probation files are kept for 7 years and misdemeanors for 5 years. ADP's policy is under California Penal Code section 1203.10 authority. | Penal Code section 1203.10 states that probation records can be destroyed after 7 years (felony cases) and 5 years (misdemeanor cases). |

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):

- Files are not destroyed if the case is still active or if there are new cases pending.

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: The client's physical files are shredded.
- Processes and Applications: N/A
- Vendor is required to dispose City's data in accordions NIST 800-88

## COMPLIANCE

### Department Compliance

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

Supervising Probation Officer (SPO) and Division Director will be responsible for enforcing the Surveillance Technology policy through its incorporation into overall Department's Supervision Policy. All ADP's sworn personnel will be trained on the Surveillance Technology policy.

**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:
Data regarding individual client is only shared on a need to know basis and/or pursuant to a court order with justice system partners who are subject to state laws and DOJ CLETS Policies

**Oversight Personnel**

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

- Division Director – 8588
- Supervising Probation Officer - 8434

**Sanctions for Violations**

Sanctions for violations of this Policy include the following:

Violation of the policy will result in disciplinary action up to and including termination from employment.

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**

Complaints to the Department are accepted in any format, via any means: phone call, verbal to a staff member, email or by written Complaint Form from the ADP website. Members of the public can find more information about how to register complaints on the Department's web site: https://sf.gov/file-complaint-about-adult-probation-department

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

ADP's 2.03.04 policy details the process when complaint from the public is received. All complaints are directed to the Chief Probation Officer wherein each complaint is assigned a number, and tracked according to AB-953 by date. A receipt letter is sent to each complainant upon delivery of the complaint to the Chief Probation Officer verifying their complaint has been received. The complaint investigation is then assigned by the Chief Probation Officer to staff who to reports back directly to the Chief Probation Officer. Once the complaint has been investigated, a follow-up letter shall be sent to the complainant which includes outcomes from the investigation.

**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.