LOWER POLK
COMMUNITY BENEFIT DISTRICT

Surveillance Technology Report FY 2020-2021

TECHNOLOGY

- 4x AV-12W-H3-4MH-DP1-B 3 MP, Pendant Multisensor Camera (1 Camera in unit)
- 3x AV-9W-H3-3MH-DP1-B 3 MP, Pendant Multisensor Camera (4 Cameras in unit)
- AV-HD-NVR3-STD-24TB-NA HD NVR3 STD 24TB NA 2U Rack Mnt WES7E (DVR)
- AV-2MN-HD-RMWS Avigilon Control Center Professional high performance onsite remote monitoring workstation for up to two monitors.
- Avigilon Control Center Software
- Additional equipment includes a monitor, keyboard, mouse, etc. Equipment also includes related camera mounts, cables, etc.

ACCESS LOG

Date of Request	Agency / Department	Person	Nature of Request
9/20/2020	SFPD	Sgt Thomas MacMahohn	Camera footage 816 Larkin. Do not have cameras responsive to request.
9/22/2020	SFPD	Sandon Cheung	9/19/20 Assaults/Robbery/Gun Fern and Polk. Video request. Video provided.
10/14/2020	SF Public Defender	Collin Olsen Public Defender	9/20/20 Video Footage Polk Street 0300 to 0745. Video provided.
3/8/2021	SFPD	SFPD officer name unknown	Provide video to responding officers Polk/Fern shooting in early morning hours.
3/22/2021	SF Public Defender	Collin Olsen	3/15/21 Video footage Polk/Golden Gate. Do not have cameras responsive to request.

SURVEILLANCE TECHNOLOGY POLICY

The Lower Polk Community Benefit District, hereinafter “CBD” values the civil rights and civil liberties of all people. This Surveillance Technology Policy thus aims to ensure the responsible and ethical use of our Security Camera System.

This policy is subject to change. The most current version will always be located at our website at: https://lowerpolkcbd.org/documents/

PURPOSE AND SCOPE

This Surveillance Technology Policy (“Policy”) defines the manner in which our Security Camera System will be used to (1) benefit the general public, and (2) support our CBD operations.

This Policy applies to all CBD personnel that use, plan to use, or plan to secure our Security Camera Systems, including employees, contractors, and volunteers.

POLICY STATEMENT

The CBD will limit our use of our Security Camera system to the following authorized use cases and requirements listed in this Policy.

Authorized Use(s):

1. Live monitoring.
2. Recording of video and images.
3. Reviewing camera footage in the event of an incident.
4. Providing video footage/images to law enforcement or other authorized persons following an incident or upon request.

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

Notwithstanding the above, analysis of, and/or the intentional gathering of aggregate or individual data revealing statistics related to any and all legally protected categories, including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, or an individual person’s sex life or sexual orientation, shall be a prohibited use.

BUSINESS JUSTIFICATION

Security Cameras will help the general public with:

Benefit to Public:	Explanation:
Community Development	The CBD will be able to determine what areas may require additional attention, such as increased street lighting.
Health	The CBD will be able to determine what areas may require outreach and assistance.
Environment	The CBD will be able to determine what areas may be sites of illegal dumping, or waste disposal.
Criminal Justice	After violent crimes, the CBD may share camera data with pertinent law enforcement, on a case-by-case basis.
Safety	Benefit to public safety

Security Cameras will help the CBD with:

Benefit to CBD:	Explanation:
Staff Safety	The CBD will be able to proactively monitor situations that may be unsafe for employees.
Increased Service Levels	The CBD will be able to increase service levels.

POLICY REQUIREMENTS

This Policy defines the responsible data management processes and safeguards required by the CBD to ensure transparency, oversight, and accountability measures. CBD 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.

Software:

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

Data Collection:

Our CBD shall only collect the data that is necessary to execute authorized use cases.

Data Types:

Video and images that we collect may include MP4, AVI, MPEG, date and time data may be contained in MP4 or other formats, and geolocation data may be contained in TXT, CSV, DOCX files.

Notification:

We will notify the public that they are under surveillance at the places where the cameras are located.

Training and 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 and recorded footage is restricted to specific trained personnel. Recorded footage is accessed only in response to an incident.

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

Data Sharing:

No live (in real time) camera footage shall be shared outside of the CBD.

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

- Confirm the purpose of the data sharing aligns with the CBD's mission.
- Consider alternative methods other than sharing data that can accomplish the same purpose.
- 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 San Francisco's Sunshine Ordinance.
- Ensure data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

CBD 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:

CBD shall secure all technology and data obtained with that technology against unauthorized or unlawful processing or disclosure; unwarranted access, manipulation or misuse; and accidental loss, destruction, or damage.

The general safeguards that protect information from unauthorized access, including encryption and access control mechanisms include:

- Physical security and software security measures.

Data Disposal:

Upon completion of the data retention period, CBD 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.

Audits:

A data access log will be maintained by the CBD for all Security Camera data that is shared. 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 Retention:

CBD may store and retain data only as long as necessary to accomplish a lawful and authorized purpose. Generally, we store camera and related data for 30 days, but we may retain it for longer or shorter periods of time in specific situations. For example, we may run out of storage space for the data, or a given file may be at issue in a legal case.

Appendix A

1. The specific categories and titles of individuals who are authorized by the CBD to access or use the collected information
    a. CBD Management and CBD Board
    b. Authorized law enforcement
    c. Authorized public defenders
    d. Authorized district attorneys
    e. Authorized insurance companies
    f. Others, only as allowed by our Data Sharing policy
2. 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.
    a. Public can inquire by contacting the CBD directly (listed below) or through the City's Public Records Request process.
        i. Email the CBD at info@lowerpolkcbd.org
3. Specific details on where data will be stored (local, DT, SaaS, Cloud Storage) including name of vendor and retention period.
    a. Local storage
4. Is a subpoena required before sharing with law enforcement?
    a. No