

DOWNTOWN SF

PARTNERSHIP

Downtown SF Partnership Video Network Usage Policies & Procedures Adopted December 1, 2025 (Revised September 1, 2026)

Purpose of System

The purpose of SafeCity Connect DSFP (the “Network”) is to enhance public safety in Downtown San Francisco for visitors, businesses, residents, and employees through networked surveillance of key public space areas. The primary purpose of the Network is to allow retrospective investigation and evidentiary use of recordings in conjunction with crimes committed within public space or when the perpetrator has fled into public space.

This document outlines the general policies and procedures for usage of the Network.

Change of Usage Policy Terms

Downtown SF Partnership (“DSFP”) reserves the right to modify or change these policies at any time, with or without notice.

General Information

- A. Cameras belonging to private property owners, businesses, and others are currently installed throughout Downtown San Francisco. These cameras overlook the public spaces in and around the Downtown Community Benefit District (the “District”). In the future, additional cameras may be added to other public spaces in the district, including but not limited to sidewalks, alleys, public plazas, and parks, and may become part of the network described herein.
- B. The following signage (or signage similar in nature) should be posted in or near areas that are under surveillance to inform the public that they may be recorded:

"THIS AREA MAY BE SUBJECT TO VIDEO RECORDING"

- C. Cameras are not intended to specifically protect private properties within the district and are not intended to record activity in areas where the public might have a reasonable expectation of privacy (e.g., public restrooms). The Network will not use covert cameras or “dummy” or fake cameras, though there is no guarantee that any camera will be functional at any particular time. The Network should also neither record any sounds or voices, nor use any biometric or other monitoring software.
- D. The Network is not intended to be actively or continuously monitored. However, a monitoring station has been or will be set up at Downtown SF Partnership Operations Center ("DSFPOC") and will be operated by Block by Block ("BBB") at 221 Sansome Street, San Francisco, CA 94104. The dispatcher on duty may monitor the live feed from time to time and may have the ability to control some of the cameras. DSFPOC usually operates 7 days a week between the hours of 6:00AM and 8:00PM.
- E. The general public and DSFP stakeholders should not have an expectation that they are under continuous surveillance when they are within the range of a camera. For example, a crime victim should not expect someone to come to their rescue merely because they are in front of a camera; they should still contact law enforcement and/or emergency services immediately.
- F. The general public and DSFP stakeholders should not have an expectation that the Network has cameras covering more than a small fraction of the public space within the District, or that such camera coverage as does exist will provide the level of detail necessary to identify suspicious activity or criminals.
- G. The system is managed by DSFP and its contractors, SafeCity Connect ("SCC") and BBB. Ownership of the system equipment and its content belong to the camera owner unless and until a recording is created by DSFP or its designee in accordance with the policies set forth herein.

Sec. 1 - Video Usage and Privacy

- A. The general purpose of the networked video system described in and subject to the policies set forth herein is to deter crime, assist in protecting the safety and property of persons and businesses within the District, and assist in the apprehension of persons who have committed crimes. Use of the system for other purposes or in any manner inconsistent with these policies is prohibited.
- B. Use of the system described herein for the purposes identified in these policies will be conducted in a professional, ethical, and legal manner.

- C. Use of the system described herein for the purposes identified in these policies will be conducted in a manner that does not violate reasonable expectations of privacy as defined by law.
- D. To maintain an informed public community and to further the goals of reducing crime and criminal activity in the district, video footage may be released from time to time, including to appropriate public safety agencies and/or legal counsel, at the discretion of DSFP to ensure that this policy's goals are continuously being met and as otherwise set forth in these policies.
- E. System Users (defined below) will operate the system in a manner that relies on suspicious behavior or reports of specific incidents or threats, and not individual characteristics, including race, gender, ethnicity, sexual orientation, or disability.
- F. System Users will not seek out or continuously view private offices, living areas, private spaces, or places of public accommodation not otherwise visible without technological assistance.
- G. System Users will not seek out or continuously view people being intimate in public areas.
- H. All recorded and archived video images, clips, or footage are subject to these policies set forth under this section.

Sec. 2 - Video Surveillance Recordings and Retrieval

- A. All camera content may be recorded continuously by a digital video recording system (currently the Avigilon Network Video Recorder). Recorded video is used exclusively for the investigation of security and safety-related incidents or for the resolution of operational issues related to DSFP's scope and responsibility and otherwise in a manner consistent with these policies, and not for other purposes. DSFP and its contractors, SCC and BBB, as designated by DSFP in its sole discretion, are responsible for the management of the system. Ownership of the system equipment and its content belong to the camera owner unless and until a recording is created by DSFP or its designee in accordance with the policies set forth herein.
- B. Recorded video will be made directly available to the general public only to the extent required by law. DSFP and SafeCity Connect will also comply with all provisions in its contract(s) with the City and County of San Francisco related to DSFP records. In the event of a crime or security incident in the area where video surveillance coverage may be available, individuals should report the crime to the SFPD. The SFPD can then request the appropriate video from SafeCity Connect, who are deemed custodians of record for the DSFP Video Network. If relevant video is available, a permanent video clip of the incident may be produced and made available to the SFPD (or other law enforcement agency or legal counsel) in accordance with the policies set forth herein. All requests for video recordings by law enforcement agencies shall be coordinated by SafeCity Connect. DSFP and its designees will cooperate fully with all court

orders or subpoenas for video recordings, to the extent required by law or by DSFP's reasonable understanding thereof. DSFP, BBB and SCC are not crime investigators and, to the extent permitted by law, will not provide real-time camera access or video recordings, or conduct system searches, for general non-specific inquiries. Video recordings will be provided in response to requests reasonably describing the desired recordings with detailed specificity and in accordance with the criteria and procedures set forth herein. SSC will assist and support with requests for large amounts of video recordings (more than 2 hours) or other complex requests in accordance with the terms and procedures of this usage policy. All other requests will be processed by SafeCity Connect staff in accordance with the criteria and procedures set forth herein.

- C. All requests for real-time video surveillance, review of recorded video footage, and/or copies of recorded video footage will generally be evaluated in accordance with the following policies:

		REQUESTING ENTITY		
		General Public, Stakeholder, & Media	Public Safety & Government Officials (Excluding Legal Counsel)	Legal Counsel (Prosecution or Defense)
N A T U R E O F R E Q U E S T	Request to Observe Real-Time Video Surveillance	Restricted and not subject to requirements set forth by the California Public Records Act. Evaluted on a case-by-case basis.	Will be evaluated on a case-by-case basis.	Restricted and not subject to requirements set forth by the California Public Records Act. Evaluated on a case-by-case basis.
	Request to View Stored Recorded Video Footage and/or for Copies of Recorded Video Footage	Will be evaluated subject to requirements set forth by the California Public Records Act.	Will be approved, barring other applicable legal restrictions.	Will be approved, barring other applicable legal restrictions.

- D. Final decision-making authority to evaluate and determine DSFP’s response to requests for real-time video surveillance, review of recorded video footage, and/or copies of recorded video footage will be vested in program staff (or their designee, in the case of extended absence) in accordance with the following policies:

		REQUESTING ENTITY		
		General Public, Stakeholder, & Media	Public Safety & Government Officials (Excluding Legal Counsel)	Legal Counsel (Prosecution or Defense)
N A T U R E O F R E Q U E S T	Request to Observe Real-Time Video Surveillance	N/A - Restricted	DSFP President & Chief Executive Officer	N/A - Restricted
	Request to View Stored Recorded Video Footage and/or for Copies of Recorded Video Footage	SafeCity Connect	SafeCity Connect	SafeCity Connect

- E. Recorded video is generally stored for a period of 30 days. On the 31st day, recorded video footage is generally deleted, erased, or destroyed in the absence of a request or internal determination to store same for longer or otherwise in accordance with the policies and procedures contained herein. Any video associated with a relevant incident or requiring further evaluation in accordance with the policies set forth herein is generally converted into a permanent video clip and stored for 180 days.

Sec. 3 - Process for Requests for Video Surveillance, Video Footage Review, and Copies of Records

- A. This DSFP policy does not guarantee provision of records upon request.
- B. All internal and external requests for footage review and copies of records are to be documented using DSFP Request for Video Retrieval Form, attached as Exhibit B, or an electronic equivalent thereof which may be posted to DSFP's website and other communication channels. The form is also to be used to document progress of the video retrieval process and is designed to help measure and improve system performance and operating procedures.
- C. DSFP or its designees will typically respond to requests within 10 business days and provide any approved recordings as soon thereafter as possible.
- D. DSFP staff or its designees will provide assistance to persons making Public Records Act requests as required by law and may fill in and submit the form if the person does not wish to do so. Although preferable, the form need not be fully completed to initiate the request. DSFP shall respond to all requests for footage review and copies of records in the timeframes required by applicable laws and regulations.
- E. All video footage review is to be carried out by and/or under direct supervision of authorized System User(s).
- F. All copies of video records are to be made by authorized System User(s) only.
- G. Copies of all video records and images made in accordance with these policies and procedures are to be retained by DSFP (or its designees) either on premises or on remote cloud servers for a period of 180 days or as otherwise set forth herein.
- H. Copies of all request forms may be retained by DSFP or their designees.
- I. Except to the extent prohibited by law, DSFP reserves the right to assess fees for requests for recorded video footage, including personnel costs for conducting a search for recorded video footage and/or images, and the actual costs of media storage devices.

Sec. 4 - Administrative Procedures and Processes

- A. System Users
 - i. System Users are defined as those individuals and groups of individuals who have been authorized to have direct or remote access to live and/or archived video footage captured by DSFP cameras. Attached as Exhibit A is a User Rights Groups chart, identifying the primary user groups and each group's access rights within the system.

- ii. All System Users are to have their own unique login name and password. All credentials are to be kept securely on file by DSFP or its designees.

B. System Administrators

System Administrators possess full administrative rights in the system permitting performance of any system function including all authorized System User functions. System Administrators have access to system settings and can add, modify, and delete System Users. System Administrator passwords are to be kept separately from the System Users credentials.

C. Individuals Authorized to Request Technical Support

All individuals who are authorized to request technical support assistance (all System Users) must attend user training and follow standard service request protocol per terms of support.

D. Network Viewing and Monitoring

- i. All System Users are to use their own unique username/password when accessing the Network and it is their responsibility to protect their username/password and not to share it with other individuals.
- ii. DSFPOC System Users are to login at the beginning of their monitoring session and log out at the end of the session.

Appendix A - Video Network User Groups/User Rights Groups

Group	Group Rights	User Description
Group A (System Admins)	-Live Video Access -Archive Video Access -Export of Video & Images -PTZ Control -Camera Setup -System User Account Creation	-DSFP Chief Operating Officer or designee -SCC
Group B	-Live Video Access -Archive Video On-Site Access -Video Export On-Site -PTZ Control	-DSFPOC Authorized System Users (BBB Staff) -DSFP Chief Operating Officer or designee
Group C	-Live Video Access	-DSFP President & CEO -DSFP Chief Operating Officer or designee
Group D	-Remote Mobile Access	TBD on a case-by-case basis and limited to the individuals specific group rights.
Group E	-Live Video On-Site Access -Live Video Remote Access -Archive Video Access - Video Export On-Site - Video Export Remote - PTZ Controls - Camera Setup - System User Account Creation *User rights to be granted only for cameras owned / controlled by the designated user.	Property owners (or their designees) with ownership of both cameras enrolled in the program and the property on which they are installed. Tenants (or their designees) with ownership of cameras enrolled in the program and a lease for the property on which they are installed.

Appendix B - Video Network Request for Video Retrieval Form

REQUESTOR PROVIDED INFORMATION	
Submission Date	
Requestor Name	
Company/Organization	
Daytime Phone Number	
Email Address	
Approximate Start Date and Time of Video Requested	
Approximate End Date and Time of Video Requested	
Location and/or Cameras Requested	
General Description of Activity/Incident	
Purpose of Request	
Case/File # (if applicable)	
Requestor Signature and/or Terms Agreement	
DSFP STAFF USE ONLY	
Real-Time Viewing Approved	
Release of Recordings Approved	
Justification for Approval	
Camera(s) Exported (Use #s)	
Actual Export Start Date/Time	
Actual Export End Date/Time	
Completed by Authorized System User	

Video Export Procedure Successful (Y/N)	
Time Expended on this Search/Export	
Video Footage Archived	
Response to Submitter	
Days Elapsed	
Notice of Completion to Submitter	
Days Elapsed	
Materials Retrieved by Submitter	