City of San José

Data Usage Protocol (DUP) for Covert Security Cameras

Owning department(s): San José Police Department (SJPD)
Department owner: Intelligence Unit Commander

1) Purpose

Covert security cameras are used by the Police Department to covertly record video in public or private spaces where there is known or suspected criminal activity (e.g., investigate repeat violent shootings). Since placing investigative personnel on site at all times is not practical, covert security cameras are installed to document activity that would further establish criminal action or exonerate the allegation. This Data Usage Protocol (DUP) defines for the City of San José's (hereafter referred to as "City") Police Department ("hereafter referred to as "Department"):

1. Authorized usage of covert security camera technology that complies with state and local laws;
2. Annual reporting requirements on covert security camera usage; and
3. An ongoing avenue for public feedback on covert security camera usage.

2) Authorized Uses:

Covert security cameras shall only be used for the purposes outlined below. Any other usage by the Department or by a third party on behalf of the Department is prohibited. Third parties may only access the data from City cameras if authorized by the City to act on behalf of the City. The Department and authorized third parties may utilize covert security cameras and any data generated to do the following:

1. Support investigations on criminal activity and/or as a mechanism to follow-up on reported incidents;
2. Be positioned in an area open to the public, or be positioned in an area not open to the public only if accompanied by consent of the person or business in control of that area or through the issuance of a warrant; or
3. Protect infrastructure installed by the City and other critical infrastructure as defined by California Office of Emergency Services (Cal OES).[1]

[1] From California Office of Emergency Services: "Critical infrastructure is the assets, systems, and networks, whether physical or virtual, so vital to the California that their incapacitation or destruction would have a debilitating effect on security, economic security, public health or safety, or any combination of these." Some examples of critical infrastructure include schools, hospitals, voting centers, community centers, and utility facilities vital to service (e.g., electricity, water).
Definition from Cal OES: https://www.caloes.ca.gov/office-of-the-director/operations/homeland-security/state-threat-assessment-center/critical-infrastructure-protection/
Non-exhaustive list of critical infrastructure: https://www.pacificpower.net/outages-safety/wildfire-safety/critical-facilities-infrastructure.html

3) Prohibited Uses:

Covert security cameras will not be used for the following purposes:

1. Share with federal immigration authorities for use in the investigation of any matter related to the immigration status of an individual; or
2. Sale of camera-generated data to any entity.

4) Data Collection

Covert security cameras record video and audio. They may be placed in fixed locations, such as a street light pole, or in a moving location, such as a vehicle or on a person. The cameras may capture video and conversations of individuals.

5) Notice

There will not be notice that the City of San José is using covert security cameras.

Residents can find general information about covert security cameras and their governing policies, including this Data Usage Protocol, on the City website.

6) Retention and Minimization

Data collected from covert security cameras will be retained for a time period consistent with the City's retention policies.[2] Once the retention period has expired, the record shall be purged entirely from all active and backup systems unless the data is related to an active investigation.

Data associated with a criminal investigation may be stored for longer on an electronic storage device or printed and retained in accordance with applicable state and federal evidentiary laws, to include retaining the data through the adjudication of a case in a recognized court of law, as well as allotment of time for an appeals process and statute of limitations.

7) Access and Accuracy

Except for audits, only authorized personnel, meaning Department personnel with a legitimate need and right to access the information, shall be allowed access to covert security camera data.

Raw camera data, including video, audio, location, and timestamp will not be available for public access unless required pursuant to city, state, or federal law, or a court order. Some information may be redacted prior to public disclosure pursuant to state and federal regulations.

8) Accountability

All Department members who use or access information from covert security cameras shall be accountable for knowledge of this protocol.

[2] As of last update to this document, that is one year. Refer to the City retention schedule for up-to-date information: https://www.sanjoseca.gov/your-government/departments-offices/office-of-the-city-manager/official-city-records/records-retention-schedule

Periodic, random audits may be conducted at the direction of the Chief of Police or their designee to ensure and evaluate compliance with system requirements and with the provisions of this protocol and applicable law. Audit trails shall be maintained by the Department for the time period consistent with the City's retention policy. Additional audits or reviews may be triggered at the direction of the Office of the City Manager or Digital Privacy Officer (DPO), consistent with state law and authorized access to information.

The results of the audits are subject to the law and potential California Public Records Act requests. Some information may be redacted prior to public disclosure pursuant to state and federal regulations.

Before a Department member accesses or provides access to a covert security camera, the Department member shall create a record that includes the following information:

1. Date/Time the camera was provided or acquired
2. The event or relevant case number of the investigation
3. The name, department, and badge or employee number of the person who acquired or returned the camera

9) Sharing

The City does not share covert security camera data with any contracted, commercial, or private entity. The provision of data hosting shall not be considered the sale, sharing, or transferring of public security camera information.

Information gathered or collected, and records retained by the City will not be:

1. Sold, published, exchanged, or disclosed for commercial purposes;
2. Disclosed or published without authorization; or
3. Disseminated to persons not authorized to access or use the information.

The City shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information unless otherwise required by law. The City may agree to share access to its covert security camera data by law enforcement agencies within the State of California on an agency-by-agency basis. Law enforcement agencies provided data from the Department will not share with federal immigration authorities or use in the investigation of any matter related to immigration status of an individual.

The data will not be shared beyond the approved agencies. All agencies must request SJPD covert security camera data directly from SJPD (e.g., if SJPD shares covert security camera data with Santa Clara PD, Sunnyvale PD must request SJPD data through SJPD rather than Santa Clara). The requesting agency may only access the data for an authorized purpose as noted in this protocol.

A log will be generated every time an outside agency is provided access to data from SJPD's covert security camera system, which will include:

1. Date/Time the information was requested;

2. The event number or case number of the investigation, if no case number is available, then the purpose of requesting the data; and
3. The name and agency of the person who requested the information

10) Equity and Community Engagement

The City will make a reasonable effort to identify and mitigate any inequity inherent in covert security cameras and its implementation. Members of the public may submit any concerns via the public comment feature at sanjoseca.gov/digitalprivacy. Comments may also be submitted by emailing digitalprivacy@sanjoseca.gov or mailing the Digital Privacy Officer at 200 E Santa Clara St. San Jose CA 95113, 11th Floor. Covert security camera implementations can impact certain populations more than others. The City of San Jose is cognizant of that concern and will field potential complaints when submitted by emailing: digitalprivacy@sanjoseca.gov. After receiving a complaint, the City will perform an investigation and determine a corrective action plan, if necessary.

11) Storage and Security

Data collected by covert security cameras shall be stored securely by police or through a third-party hosting environment. With the exception of audits, access to the raw data (video or audio recording of public space) shall be limited to law enforcement staff with a legitimate need and right to access the information. The Department will utilize reasonable physical, technological, administrative, procedural, and personnel security measures to prevent unauthorized access to covert security camera data. Authorized sworn personnel or authorized civilian personnel (such as a crime analyst) shall have general user access to the SJPD covert security camera data, as appropriate, to query information. Entities authorized to audit the covert security camera system (see "Accountability" section for who can authorize) do not need to be a part of the Department to access the data.

In the event of a confirmed data breach where personal information such as video recordings of identifiable individuals have been accessed by an unauthorized party, the Department will follow the City of San José's Information Technology Incident Response Plan. This security protocol and further security details are overseen by the City's Cybersecurity Office.[3]

12) Training

Department members will be trained in how to:

1. Install a camera;
2. Securely access the information collected;
3. Document access to the information; and
4. Adhere to current Department Data Usage Protocol regarding authorized use of covert security camera technology.

[3] An overview of Information Technology's Incident Response plan can be found in the City's Information Security Standards Handbook Section 8.7, "Incident Response": https://www.sanjoseca.gov/home/showdocument?id=85853#page=32

13) Annual Data Usage Report requirements

Covert security cameras rely on secrecy to collect evidence for criminal investigations. Publicly reporting where the cameras are used would substantially diminish the Department's effectiveness in gathering evidence, and may put undercover operations at risk (e.g., in the event of an informant gathering evidence within a criminal organization). Because of this, annual reporting requirements are waived, but audits will still be conducted to ensure compliance with this policy (see "Accountability" section).