DEPARTMENTAL GENERAL ORDER

I-32.1: Community Safety Camera Systems – Camera Registry and Department Remote Access to Public/Privately Owned Surveillance Camera Systems

Effective Date: XX Nov XX
Coordinator: Bureau of Investigations

The Oakland Police Department believes in protecting and serving its diverse community and city through fair, equitable, and constitutional policing. OPD believes in the usage of technology to aid in this mission and in the investment in contemporary surveillance technology to help improve public safety while still protecting community members' privacy rights. This includes a multipronged approach related to tactics, methodology, and technology that allows for de-escalation in often rapidly evolving situations.

This policy provides guidance for the capture, storage, and use of digital data obtained through the use of Community Safety Camera Systems technology while recognizing the established privacy rights of the public.

A. Definitions

A - 1. Community Safety Camera

A fixed camera device, owned and/or controlled by the City of Oakland or a private/public entity, with the capability of live streaming and/or recording videographic data, where the owner/controller of the device and its associated data has explicitly provided authorization to the Oakland Police Department to access historical and/or live videographic data in the furtherance of a criminal investigation.

Community Safety Cameras Include:

- Any camera owned/managed by the Oakland Police Department that is installed in a public place and accessed by the Department, outside of cameras installed for Department facility security.
- Any camera owned and/or controlled by a private/public entity, not under the control of the Oakland Police Department, that is accessed by the Department pursuant to this policy.

A - 2. Operating System

The Flock Operating System (FlockOS) is a cloud-based public safety platform designed to integrate and manage data from various sources, including video, license plate recognition (LPR), and gunshot detection systems. It provides real-time investigative information and retrospective investigation capabilities to support the full spectrum of Departmental operations. FlockOS has a native Video Management System VMS platform but also is capable of integrating with outside VMS systems.

A - 3. Video Management System (VMS)

A Video Management System (VMS) is software designed to process, store, and manage video footage from multiple surveillance cameras. VMS software operates as a central management system, linking and consolidating multiple camera systems onto a single platform, while offering tools for monitoring, recording, and analyzing video data in real-time or from recorded archives.

B. Description of the Technology

OPD uses the Community Safety Camera Systems (CS Camera Systems) and associated VMS/OS technology as a form of crime deterrence, and when necessary, to capture and store digital image data related to criminal activity and active criminal investigations.

B - 1. Technology Integration Platform - Flock Operating System (FlockOS)

The Flock Operating System is the basis of the Department's Technology Integration platform (TIP). The operating system allows the Department to integrate existing technology in a more cohesive and comprehensive way, while also assisting with the coordination of field operations and investigative bodies to address specific disruptive criminal activities in our community with precision and efficiency.

B - 2. Fixed Line of Sight Camera System

Line of sight cameras are fixed-position surveillance camera devices that capture visual data from a defined area.

B - 3. Pan-Tilt-Zoom (PTZ) Camera Systems

1. Pan: This function allows the camera to rotate horizontally, covering a broad field of view. PTZ cameras can rotate up to 360 degrees, allowing the camera system to replicate the view of a person located in the same position of the camera.

2. Tilt: This feature enables the camera to move vertically. Tilting up and down helps to cover different vertical angles and ensure that both high and low areas can be observed.

3. Zoom: PTZ cameras come equipped with optical zoom lenses that allow you to zoom in on specific objects or areas without losing image quality. This is useful for detailed inspection or the tracking of moving objects.

4. Remote Control: PTZ cameras can be controlled remotely via various interfaces, such as dedicated control panels, computer software, or mobile apps. This flexibility allows operators to adjust the camera's position and zoom level in real time.

C. Purpose of the Technology

OPD accessed CS Camera Systems and associated VMS and Operating Systems are intended to deter criminal activity within specific public areas and enhance the Department's ability to address disruptive criminal activity within the community. These disruptive crimes include theft, vehicle theft, human trafficking, reckless driving, sideshow/takeovers, felony evasion, burglaries, robberies, shootings, and homicides. Many criminal investigations hinge upon the availability and quality of surveillance video as evidence that is later used in the prosecution of criminal cases. While physical surveillance may also accomplish these goals, it is limited due to the financial cost, the availability of resources, and the physical demands upon members of the Department. CS Camera Systems have the capability of enhancing the Department's ability to address the types of criminal activity that are disruptive within the community while also acting as a resource multiplier within the Department. It is the expressed intent of the Department to use this technology to facilitate informed enforcement on those involved in specific disruptive criminal activities and to mitigate collateral impact upon the community.

The Department also recognizes that CS Camera Systems have the capability of assisting with community safety efforts beyond the role of the law enforcement, and intends to utilize CS Camera Systems to assist the Oakland Fire Department and other partnering emergency services in their Public Safety functions.

D. Authorized Uses

D - 1. Authorized Users

Personnel authorized/designated to use CS Camera System equipment or access information collected through the use of such equipment shall be specifically trained in such technology. Sworn personnel, Police Service Technicians (PST), or other authorized/designated Department personnel may use the technology.
Authorized users other than sworn personnel or PSTs must be designated by the Chief of Police or designee.

D - 2. Authorized Use

- **Recording of Public Areas**

  Access to CS Camera Systems that are installed with a view of a public area shall be done so under expressed permission provided by the owner/controller of the device and its associated data. OPD shall only record and retain video data in furtherance of a criminal or administrative investigation.

- **Recording an Area Subject to a Reasonable Expectation of Privacy**

  CS Camera Systems shall not be used in areas where there is a reasonable expectation of privacy unless under exigent circumstances..

- **Recordings During Exigent Circumstances**

  CS Camera Systems may be used during exigent circumstances that include hostage situations, barricaded suspects, kidnappings, and active shooter

situations. If a CS Camera System is used for exigent circumstances, a search warrant shall be sought within 72 hours, and the exigent use shall be documented within the annual report and reported to the Privacy Advisory Committee (PAC) and the next available PAC meeting.

E. Restrictions on Use

E - 1. Permitted/Impermissible Uses

Department personnel may only access and use the CS Camera System consistent with this Policy. Recordings retained by the Department related to criminal investigations are the property of the Oakland Police Department. The following uses of the CS Camera System are specifically prohibited:

- **Invasion of Privacy**: Except when done pursuant to a court order such as a search warrant, it is a violation of this Policy to utilize the CS Camera System to intentionally record or transmit images of any location where a person would have a reasonable expectation of privacy (e.g., residence, enclosed yard, enclosed structure) unless exigent circumstances exist. If a CS Camera System is used for exigent circumstances, a search warrant shall be sought within 72 hours, and the exigent use shall be documented within the annual report (in accordance with Section D-2 of this policy).
- **Harassment or Intimidation**: It is a violation of this Policy to use the CS Camera Systems with the intent to harass and/or intimidate any individual or group.
- **Use Based on a Protected Characteristic**: It is a violation of this policy to use CS Camera Systems to target a person or group solely because of a person's, or group's race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law.
- **Facial Recognition**: It is a violation of this policy for Department members to use CS Camera Systems in conjunction with Facial Recognition technology.
- **Motion Activated Object Tracking Technology**: It is a violation of this policy to utilize motion activated object tracking technology, *if* the technology selectively tracks objects or subjects using Personal Identifying Information (PII) or factors such as race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law.
- **Personal Use**: It is a violation of this Policy to use the CS Camera Systems or associated data for any personal purpose.
- **First Amendment Rights**: It is a violation of this policy to use the CS Camera Systems or associated data for the intended purpose of infringing upon First Amendment rights.

- **Audio Data:** It is a violation of this policy to utilize Department owned CS Camera Systems to capture or store audio data.

Department members shall not use, or allow others to use, the equipment or database records for any unauthorized purpose.

1. No member of this department shall operate CS Camera System equipment or access CS Camera System data without first completing department-approved training.
2. No CS Camera System operator may access department, state or federal data unless otherwise authorized/designated to do so pursuant to Section G "Data Access" below.
3. Accessing data collected by CS Camera Systems requires a right to know and a need to know. A right to know is the legal authority to receive information pursuant to a state or federal statute, applicable case law, or a court order. A need to know is a compelling reason to request information such as involvement in an active investigation.

The Department should make reasonable efforts to avoid viewing CS Camera Systems that inadvertently capture public areas outside of sensitive facilities, such as medical clinics, reproductive health facilities, houses of worship, or other sensitive locations; absent an investigative need to do. When technologically possible, the Department should consider utilizing "masking" or "blurring" features available on certain VMS platforms to mask entrances or buildings determined to be sensitive facilities. CS Camera Systems shall not be used to specifically target a person or group solely because of a person's, or group's race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law.

F. Data Collection

CS Camera Systems live-streams and records photographic and videographic data utilizing mounted camera systems. The data is stored through a Video Management System (VMS), which may only be accessed by authorized personnel and requires an individual username/password.

G. Data Access

G - 1. General Data Access Guidelines

Department sworn personnel, police service technicians, or other authorized/designated Department personnel may use the technology. Authorized/designated users other than sworn personnel or PSTs must be designated by the Chief of Police or designee.

The Oakland Police Department does not permit the sharing of CS Camera System data gathered by the city or its contractors/subcontractors for the purpose of federal

immigration enforcement, pursuant to the California Values Act (Government Code § 7282.5; Government Code § 7284.2 et seq) – these federal immigration agencies include Immigration and Customs Enforcement (ICE) and Customs and Border Patrol (CPB).

All data and images gathered and retained by CS Camera Systems related to criminal investigations are for the official use of this department. Some information may not be disclosable to the general public. Investigatory records are not generally disclosable in response to a public records request. Non-investigatory and otherwise non-exempt records shall be disclosed in response to a public records request.

G - 2. Tiered CS Camera Data Access

The CS Camera System is segmented into tiers of access, to provide robust community safety capabilities while also ensuring privacy safeguards are present. By assigning access levels based on roles and responsibilities, sensitive footage can be restricted to authorized personnel, reducing the risk of misuse or breaches. It also allows for more efficient monitoring, as different sections within the Department can focus on the data relevant to their needs without being overwhelmed by unnecessary information. This structured approach balances transparency, accountability, and privacy protection.

Real-Time Camera Access – Only specific Department members designated by the CS System Administrator(s) and/or Chief of Police shall have access to Real-time (live) camera access while supporting field operations. Real-time access shall be utilized strictly in the furtherance of an active investigation. The CS System Administrator shall keep a record of Department members who are authorized real-time camera access. Access to real-time cameras shall be limited to members who have been approved by the Operations Center Commander, Ceasefire Commander, CID Commander, or Chief of Police. The Operations Center Commander is responsible for maintaining a list of authorized members who are provided access to real-time camera data.

Authorized Department members may live-stream real-time surveillance video to any member of the Department (with a need-to-know, right-to-know) related to incidents where the live surveillance video may assist in enhancing the member(s) ability to safely address a critical incident related to the following:

- Where a subject(s) is believed to be armed with a weapon capable of inflicting injury.
- Where a subject has demonstrated violent behavior, made threats of violence towards themselves or others, and/or the previous actions of the subject pose a danger to the public, officers, or themselves[1].

[1] This includes but is not limited to, flight (on foot or utilizing a vehicle), assault, self-harm, and/or a history of barricading themselves.

- To assist with detaining a subject(s) related to a felony investigation.

Live-stream surveillance video may assist members with establishing additional time and distance with engaged subjects, maximizing the use of available cover, and fostering conditions that enable effective de-escalation during enforcement efforts.

Historical Data Access – Any member of the Department who is trained and provided access to the CS Camera System may access historical video data related to a specific criminal or administrative investigation; similar to the current process of conducting a physical canvass for video surveillance. Physically canvassing for video is time and resource-consuming. It often requires the owner/controller of the device to be present and either the Department member or possessor of the equipment to be familiar with how to access and export the video data.

If the owner/controller provides explicit consent by opting in to sharing video data through the VMS and/or FlockOS system, Department members can access historical video data remotely, making the process more efficient for the member and owner/controller of the physical camera system.

Historical Data access shall be documented by recording the following:

1. The date and time the information is accessed,
2. The associated report or incident number,
3. The username of the person who accesses the information,
4. The purpose for accessing the information.

H. Data Protection

All data shall be safeguarded and protected by both procedural and technological means. OPD shall observe the following safeguards regarding access to and use of stored data:

- All CS Camera System server data shall be accessible only through a login/password-protected system capable of documenting all access of information by username or other data elements used such as date and time of access.
- All data shall be accessed via a Department approved securely connected device.

I. Data Retention

It is understood by the Department that CS Camera Systems and their associated data, not under the control of the Department, may have different retention schedules than that of the Department.

All CS Camera System data uploaded to a Video Management System (VMS) owned by the Department shall be purged 30 days from the initial upload. CS Camera

System information may be retained outside this retention limit solely for the following purposes:

1. Active Criminal Investigations
2. Active Administrative Investigations
3. Missing or at-risk Persons Investigations
4. Investigations from other law enforcement or prosecutorial agencies where there is a legal obligation to retain information.

Any data retained for the above-described investigative purposes shall be stored on Evidence.com in accordance with Appendix A of this policy.

J. Public Access

All images and recordings uploaded by the CS Camera System and retained related to an investigation are for the official use of this department. Some information may not be disclosable to the general public. Investigatory records are not generally disclosable in response to a public records request. Non-investigatory records shall be disclosed in response to a public records request. Requests for information by non-law enforcement or non-prosecutorial agencies will be processed in accordance with Government Code §7920 et seq, this policy, and applicable case law and court orders.

K. Third Party Data Sharing of Data Retained by the Department

K - 1. CS Camera System Sharing with Legal Obligation

OPD personnel may share downloaded retained recorded CS Camera System data and associated metadata when there is a legal obligation to do so, such as the following:

- a federal, state, or local criminal prosecutor's office for use as evidence to aid in prosecution, in accordance with laws governing evidence;
- a Public Defender's Office or criminal defense attorney via the District Attorney's Office in accordance with applicable California criminal discovery laws;
- California law enforcement agencies as part of a formal criminal or administrative investigation;
- a party to civil litigation, or other third parties, in response to a valid court order only.

CS Camera System server data may be shared only as otherwise permitted by law and this policy. All data and images gathered by the CS Camera System are for the official use of this Department.

K - 2. CS Camera System Sharing without Legal Obligation

When there is no legal obligation to provide the requested data, requests for downloaded retained recorded CS Camera System data and associated metadata from other California law enforcement agencies shall be made in writing and may only be approved by the Ceasefire Commander or designee per the 3-step protocol below. These requests shall be maintained in a secure folder so that information about these requests can be shared in required annual reports with the PAC. Server access shall be restricted only to authorized/designated Department personnel who will extract the required information and forward it to the requester.

- The requesting party shall have a right to know, and a need to know. A right to know is the legal authority to receive information pursuant to a court order, statutory law, case law, or sworn officer status. A need to know is a compelling reason to request information such as direct involvement in an investigation.

- The Department shall record the requesting party's name and document the right and need to know the requested information.
- The Department shall record whether the request was honored or denied, the reason for such action, and the name of the Department officer that processed the request.

L. Training

The Training Section shall ensure that members receive department-approved training for those authorized/designated to use or access the CS Camera System and shall maintain a record of all completed trainings.

Training requirements for employees shall include the following:

- Applicable policy
- Functionality of equipment
- Accessing data
- Sharing of data

M. Auditing and Oversight

Login/Log-Out Procedure. To ensure proper operation and facilitate oversight of the CS Camera System, all users will be required to have individual credentials for access and use of the systems and/or data, which has the ability to be fully audited. It is the responsibility of the Department under this policy to actively pursue software and hardware upgrades that are needed to maintain full compliance with Section K of the use policy.

The records of the number of deployments of Department owned CS Camera Systems, Third Party Data Sharing related to Section K – 2 of this Policy, and any exigent use of CS Camera Systems shall be incorporated into the annual report required by O.M.C. 9.64 et seq.

CS Camera System audits shall be conducted annually to ensure proper system functionality and that designated personnel are using the system according to policy rules via sample audits, and reviews of training records. The size of these audits shall be large enough to provide a statistically significant representation of the data collected.

N. Maintenance and Administration

N - 1. CS Camera System Administration

All installation and maintenance of Department owned CS Camera equipment, as well as CS Camera System data retention and access, shall be managed by the Ceasefire Section and Assistant Chief of Police.

N - 2. CS Camera System Administrators

The Ceasefire Commander and CGIC/Operations Center Commander shall be the administrators of the CS Camera System program and shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code § 1798.90.5 et seq. The Ceasefire Captain is responsible for ensuring systems and processes are in place for the proper collection, and retention of CS Camera System data.

N - 3. CS Camera System Coordinator:

The title of the official custodian of the CS Camera System is the CS Camera System Coordinator.

N - 4. Monitoring and Reporting

The Oakland Police Department will ensure that the system remains functional according to its intended use and monitor its use of CS Camera System technology to ensure the proper functionality of the system as defined in the policy guidelines of this document, including required audits, training, and data access records.

The CS Camera System Coordinator shall provide the Chief of Police, Privacy Advisory Commission, and Public Safety Committee with an annual report pursuant to OMC 9.64 (Oakland Surveillance Technology Ordinance).

By Order of

Floyd Mitchell
Chief of Police Date Signed:

Appendix A

Category Name	Retention Period	Legal Retention Requirements
Violent Felony / DOA	Indefinite	Statute of Limitations (SOL)
Misdemeanor Case (including report, statements, cite, or arrest)	2 yrs	SOL
Felony Case (including report, statements, cite, or arrest - no violent felonies or sex crimes)	3 yrs	SOL
Missing Person / Runaway	Indefinite	SOL (Possible homicide)
Sex Crimes	Indefinite	SOL
Vehicle Pursuit	5 yrs	Administrative SOL
Sergeants / Commanders Admin	2 yrs	Possible IA/DLI - Sergeant/etc. to update category if so
IA/DLI	Indefinite	Administrative SOL
Use of Force - Levels 1 and 2	Indefinite	Administrative SOL

Use of Force - Levels 3 and 4	Indefinite	Administrative SOL
Felony - Filed by DA	20 yrs	SOL plus appeals
Homicide	Indefinite	SOL
Misdemeanor - Filed by DA	10 yrs	SOL plus appeals
Legal - OCA/Records/Authorized Users Only	Indefinite	City Attorney's Office (CAO) Order
Collision - 901C	Indefinite	CAO Order
Collision - Major Injury / Fatal	Indefinite	SOL