ADENA ISHII
MAYOR OF BERKELEY

2180 Milvia Street
Berkeley, CA 94704
Tel: (510) 981-7100
TDD: (510) 981-6903
mayor@berkeleyca.gov

REVISED AGENDA MATERIAL
for Supplemental #2

Meeting Date: May 7, 2026

Item Number: 1a

Item Description: Public Safety Technology: Surveillance Technology Ordinance and Police Equipment Ordinance Approvals, Policy Updates, and Contract Authority

Submitted by: Mayor Adena Ishii (Co-Author), Councilmember Cecilia Lunaparra (Co-Author), and Councilmember Igor Tregub (Co-Sponsor)

This supplemental material only reorganizes the content from the March 24th, 2026, supplemental to align with the staff report. It aims to balance the value of surveillance technology with Berkeley's commitment to privacy, civil liberties, and Sanctuary City status. Additionally, in response to reported security failures in neighboring jurisdictions, this supplemental clarifies how these technologies work and codifies legislative intent. These recommendations stem from comprehensive community engagement, feedback from the Police Accountability Board (PAB), and extensive conversations with the Office of the Director of Police Accountability and the Berkeley Police Department. In light of these considerations, this item refers the Community Video Stream (CVS) acquisition report and surveillance use policy to the Public Safety Committee for review; recommends limiting the retention period for non-evidentiary footage and strengthening oversight for Unmanned Aerial Systems (UAS); increase auditing and reporting cadence for Fixed Cameras in Surveillance Use Policy; and explicitly opposes the renewal, approval, or authorization of any contract with Flock Safety.

The original item requests authorization for acquisition, use, and/or contracting of the following technologies: Unmanned Aerial System (UAS), Community Video Stream (CVS), Fixed cameras, Investigative software, and Automatic License Plate Readers. The following table summarizes this supplemental's recommendations.

	Approve/approve with amendments	Refer back to Staff	Reject
Unmanned Aerial System (UAS)	✔Surveillance Use Policy ✔Military Equipment Use Policy	↩Acquisition Report ↩Military Equipment Impact Statement	✗ Flock Contract
Community Video Stream (CVS)	—	↩Acquisition Report ↩Surveillance Use Policy	✗ Flock Contract
Fixed cameras	✔Surveillance Use Policy	—	✗ Flock Contract
Investigative software	—	—	✗ Flock Contract
Automatic License Plate Readers (ALPR)	—	—	✗ Flock Contract

Proposed revisions and recommendations:

Surveillance Technology Ordinance (BMC 2.99)

1. **Amend the Surveillance Use Policy for the Unmanned Aerial System to include the following provisions:**
    a. **Reduce the non-evidentiary drone footage retention period to five (5) days**
    Pursuant to the proposed UAS surveillance use policy, uses of the UAS are limited to de-escalation, tactical safety, emergency response, operational efficiency related to calls for services, and investigation. As a result, much of the footage captured by drones is responsive, not passive, and therefore distinct from other surveillance technologies and retention timelines. To balance data security with operational efficiency, we propose a reduced footage retention period of five (5) days, aligning with Oakland's policy.

    b. **Amend audit timelines to require a monthly audit and a semiannual audit report**
    Require monthly audits with a semiannual (twice a year) published audit report. The PAB recommended a monthly audit to ensure potential violations are caught early. The City Council directed staff to change the audit report timeline from biennial (once every two years) to semiannual at their July 2025 meeting.[1] These audits should be sent to the PAB.

[1]https://berkeleyca.gov/sites/default/files/city-council-meetings/2025-07-22%20Annotated%20Agenda%20-%20Council.pd,

c. **Add supervisory approval for all UAS deployments except for DFR**
To enhance internal oversight for drone use, supervisory approval for all deployment protocols should be added. DFR protocols may be excluded from these specific service constraints to maintain operational speed.

d. **Specify authorized use cases**
It is important to reduce ambiguity around when a UAS deployment is permitted. Accordingly, this supplemental material proposes amending the language from "Authorized operators may deploy the UAS in the following circumstances" to: "Authorized operators ***shall only*** deploy the UAS in the following circumstances."

e. **Refer to the City Manager to develop defined performance metrics to measure and report on the efficacy of the technology**
BPD should develop performance metrics aligned with the goals of the use policy to better evaluate the technology's effectiveness. The performance metrics should relate to the stated goals of the technology and should quantify the program's success in:
   i. Operational efficiency: Reducing officer overtime.
   ii. Personnel safety: Enhancing officer protection.
   iii. Crime mitigation: Deterring both violent and non-violent offenses.
   iv. Investigative success: Improving clearance rates and solving crimes.

f. **Refer to the City Manager to create a consolidated UAS operations and data governance policy**
Consolidate Policies 611 and 1303 to create a single UAS Operations and Data Governance Policy to ensure clear lines of accountability and enhance document and version control.

g. **Refer to the City Manager the UAS Surveillance Acquisition Report for research and analysis of alternative surveillance technology vendors capable of meeting the City of Berkeley's safety and surveillance needs while balancing the need for privacy and civil liberties protections**
The UAS Surveillance Acquisition Report references Flock technology. As a result, this supplemental material recommends referring the report to the City Manager to identify alternative vendors. The accompanying Use Policy is recommended for approval with the recommendations enumerated in bullet 2.

Provisions 2f, 2g, and 2h may be taken up after Council approval of the UAS Surveillance Use Policy.

2. **Refer the Community Video Stream Acquisition Report and Surveillance Use Policy to the Public Safety Policy Committee (PSPC) for further review;**

request that the City Manager work at the committee level to address the PAB's concerns and clarify operational ambiguity:
This is the first time this item has been presented to the Berkeley City Council. Given the unknown operational implications, additional clarification and feedback are advantageous for a more robust understanding. During review at the PSPC, staff should address the following Police Accountability Board[2] recommendations and authors' questions:

a. Add an explicit prohibition on surveillance of First Amendment activity, unless there is a clear, articulable, and imminent public safety threat that is actively occurring;
b. Specify concrete data retention periods with the four elements required by BMC 2.99.020.4(g);
c. Conduct a disparate impact analysis addressing whether camera coverage is concentrated in areas with particular demographic characteristics;
d. Supplement Section 11 of the Acquisition Report to disclose adverse findings from comparable jurisdictions;
e. Update immigration-related search reporting to match the 72-hour standard and named recipients in Policy 351 section 351.6 per our Sanctuary City Ordinance;
f. Consider developing a use policy to address combined cross-platform use of all integrated technologies, regardless of vendor used, including ALPR, fixed cameras, community video streams, and drones;
g. Institute semiannual audits of CVS–similar to Council directive on fixed cameras established in July 2025[3];
h. Analyze the data governance and security risks of community camera integration.

3. **Amend the Surveillance Use Policy for Fixed Cameras to include the following provision:**
   a. **Amend audit timelines to require a monthly audit and a semiannual audit report**
   Require monthly audits with a semiannual (twice a year) published audit report. The PAB recommended a monthly audit to ensure potential violations are caught early. The City Council directed staff to change the audit report timeline from biennial to semiannual at their July 2025 meeting.[4] The monthly audit reports should be shared with the PAB.

---

[2]https://berkeleyca.gov/sites/default/files/2026-03/March%2018%2C%202026%20PAB%20Recommendations_Surveillance%20Tech.pdf
[3]https://berkeleyca.gov/sites/default/files/city-council-meetings/2025-07-22%20Annotated%20Agenda%20-%20Council.pdf
[4]https://berkeleyca.gov/sites/default/files/city-council-meetings/2025-07-22%20Annotated%20Agenda%20-%20Council.pd,

Police Equipment Ordinance (2.100)

4. **Amend the UAS Equipment Use Policy to include the same revisions as the recommendations for the UAS Surveillance Use Policy.**
    - **a.** Reduce footage retention period to five (5) days
    - **b.** Amend audit timelines to require a monthly audit of data sharing permissions and a semiannual audit report
    - **c.** Add supervisory approval for all deployments except for DFR
    - **d.** Establish a thorough protocol for decertification
    - **e.** Specify authorized use cases

5. **Refer the following request for information to the City Manager to quantify the need for UAS**
   Provide Berkeley-specific data to prove "no reasonable alternative" exists. The following should be considered:
    - **a.** Frequency of incidents for which aerial perspective has historically been needed by call type
    - **b.** Documented historical delays/availability issues when relying on external aerial support
    - **c.** Establish baseline officer injury rates and documented officer safety issues relevant to articulated use cases (quantitative, not just qualitative)
    - **d.** Baseline Call-For-Service (CFS) response time data by call type
    - **e.** Baseline crime clearance rate data by crime type

Approval of the UAS Equipment Use Policy is not contingent upon completion of 5a-5e.

6. **Refer the UAS Military Equipment Impact Statement to the City Manager for research and analysis of alternative surveillance technology vendors capable of meeting the City of Berkeley's safety and surveillance needs while balancing privacy and civil liberties protections**
   The UAS Military Equipment Impact Statement references Flock technology. As a result, this supplemental material recommends referring the report to the City Manager to identify alternative vendors. (The accompanying but distinct UAS Equipment Use Policy is recommended for approval, subject to incorporation of revisions enumerated in recommendation #4 above.)

Contract Authority

7. **Reject any renewal, authorization, approval, or execution of the Flock Safety contract**
   Flock's violations are numerous. In recent years, at least 30 jurisdictions have paused or terminated their Flock contracts due to concerns about impermissible data sharing with federal law enforcement agencies, including federal

immigration enforcement agencies.[5] Within California, at least 7 jurisdictions have deactivated their cameras or canceled their contracts with Flock. Most alarmingly, in Ventura, CA, an audit found that "out-of-state agencies accessed the Ventura County Sheriff's Office's data more than 364,000 times between February and March [2025] without the department's approval or knowledge."[6] The Sheriff's Office in Ventura County confirmed that it had disabled the "National Look Up" feature within the Flock system, in order to comply with California law, but that the feature had been reactivated without any notice or explanation from Flock.[7]

Several Bay Area cities, including Santa Cruz, Mountain View, and Los Altos Hills, have paused their flock cameras after "discovering that federal agencies could search the camera data, despite the firm's assurances otherwise."[8] The Mountain View Police Department stated in a January 2026 news release that several federal law enforcement agencies accessed its ALPR system data through the use of the "nationwide" search setting that was turned on by Flock without Mountain View Police Department's permission or knowledge[9]. In Los Altos Hills, the City Council voted to "remove its Flock Safety automated license plate reader cameras around town, citing concerns about data privacy, cost considerations, and overall effectiveness."[10] In each of these cities, Flock made contractual commitments to its clients and failed to abide by them.

As a Sanctuary City, the repeated violations of Flock contract terms pose a risk to the community, including but not limited to Berkeley's immigrant residents.

Single-vendor consolidation introduces additional risks. In its March 18, 2026, letter to the City Council, the PAB explains that while there can be operational benefits to a single vendor ecosystem, there are also significant risks in integrating surveillance data and creating dependency on one private company.

Additional Recommendations

8. **Refer to the City Manager to amend Ordinance 2.99 to include a violation/termination clause for surveillance technology vendors.** Establish enforceable mechanisms to sanction surveillance technology vendors for misuse, unauthorized access, or data security failures.

---

[5]https://www.npr.org/2026/02/17/nx-s1-5612825/flock-contracts-canceled-immigration-survillance-concerns

[6]https://www.cbsnews.com/losangeles/news/flock-license-plate-readers-shared-data-with-out-of-state-federal-agencies/

[7] *Ibid.*

[8] https://localnewsmatters.org/2026/02/11/alameda-county-flock-cameras-privacy-debate/

[9]https://www.cbsnews.com/sanfrancisco/news/mountain-view-alpr-cameras-use-suspended-automated-license-plate-reader/

[10]https://www.losaltosonline.com/news/los-altos-hills-to-remove-alpr-cameras/article_59f90aa8-14c1-4309-9f7f-12d16c649d9e.html

9. **Refer to the City Manager and City Attorney additional contractual language to require a vendor to inform the City of any request for information (including but not limited to subpoenas, discovery requests, or requests under any federal or state statute to the extent permitted by law) it receives related to City-controlled data and safeguard it to the fullest extent allowed by law.**

RESOLUTION NO. ##,###-N.S.

APPROVING SURVEILLANCE TECHNOLOGY, ~~AND~~ POLICE EQUIPMENT ORDINANCE REQUIREMENTS, AND , ~~AND~~ UPDATED USE POLICIES~~, AND AUTHORIZING CONTRACTS WITH FLOCK SAFETY~~ FOR PUBLIC SAFETY TECHNOLOGY

~~WHEREAS, the City of Berkeley has adopted BMC 2.99, the Surveillance Technology Ordinance, which requires City Council approval of a Surveillance Acquisition Report and Surveillance Use Policy prior to the acquisition or use of new surveillance technology; and~~

~~WHEREAS, the City of Berkeley has adopted BMC 2.100, the Police Equipment Ordinance, which requires City Council approval of a Police Equipment Impact Statement and Police Equipment Use Policy for controlled military equipment, consistent with AB 481; and~~

~~WHEREAS, the Drone as First Responder (DFR) portion of the Unmanned Aerial Systems program constitutes both a new surveillance technology under BMC 2.99 and controlled military equipment under BMC 2.100, and the Police Department has prepared and published the required Surveillance Acquisition Report, Surveillance Use Policy, Impact Statement, and Police Equipment Use Policy for Council review; and~~

~~WHEREAS, Community Video Streams constitute a new surveillance technology under BMC 2.99, and the Police Department has prepared and published the required Surveillance Acquisition Report and Surveillance Use Policy for Council review; and~~

~~WHEREAS, fixed video cameras were previously approved by Council, and updated Surveillance Use Policies reflecting Council-directed revisions are presented for approval; and~~

~~WHEREAS, the Police Department held a community information session on January 15, 2026, to present and gather feedback on the full suite of public safety technologies, and the Police Accountability Board has had an opportunity to review and provide input on each technology through multiple public meetings; and~~

~~WHEREAS, the City Council accepted the Byrne State Crisis Intervention Program (SCIP) grant award of $1,000,000 on July 29, 2025, which identified investigative software as an eligible expenditure, and Flock Nova falls within that allocation; and~~

~~WHEREAS, the City's existing Flock Safety ALPR contract expires in July 2026, and renewal authority is required to maintain continuity of service; and~~

~~WHEREAS, the City Attorney's Office has negotiated a Master Services Agreement with Flock Safety that includes protections for City data ownership, restrictions on federal access consistent with the City's sanctuary policies, financial penalties for unauthorized~~

~~disclosures, security incident notification requirements, and post-termination data protections, and Flock Safety has accepted every revision proposed by the City Attorney's Office; and~~

~~WHEREAS, funding for the technology suite will come from eliminating up to 6 sworn officer positions, as supported by the Berkeley Police Association, resulting in a net savings to the General Fund; funding for fixed cameras is available in the General Fund allocation designated for surveillance cameras; funding for Flock Nova is available from the BSCC SCIP grant with no General Fund impact; and~~

~~WHEREAS, all prices meet or are below those listed for the same products on the Omnia cooperative purchasing consortium, satisfying the City's competitive procurement requirements; and~~

~~WHEREAS, Flock Safety has offered a 10% discount on new product lines if contracts are executed by the end of March 2026, representing over $100,000 in savings.~~

WHEREAS, the original staff recommendation for Item 26 requested authorization for the acquisition and use of multiple surveillance technologies and the execution of a master services contract with Flock Safety; and

WHEREAS, over the past year, documented security failures and unauthorized data-sharing incidents involving Flock Safety in jurisdictions such as Mountain View and Ventura County have raised significant concerns regarding the vendor's ability to comply with Berkeley's stated goals; and

WHEREAS, the original item requests authorization for acquisition, use, and/or contracting of the following technologies: Unmanned Aerial System (UAS), Community Video Stream (CVS), Fixed cameras, Investigative software, and Automatic License Plate Readers (ALPRS); and

WHEREAS, the revised material recommends that the City Council approve the amended UAS Surveillance Use Policy, the amended UAS Military Equipment Use Policy, and the amended Fixed Camera Surveillance Use Policy; and

WHEREAS, the revised material recommends that Council refer to staff the UAS Acquisition Report and UAS Military Equipment Impact Statement to identify alternative vendors other than Flock Safety; and

WHEREAS, the revised material recommends that Council refer to staff the CVS Acquisition Report and the CVS Surveillance Use Policy for further review and feedback by the Public Safety Policy Committee; and

WHEREAS, the revised material recommends that Council reject any contract renewal, authorization, approval, or execution with Flock Safety.

NOW THEREFORE, BE IT RESOLVED by the Council of the City of Berkeley as follows:

Surveillance Technology Ordinance Approvals

1. The City Council hereby accepts the Surveillance Acquisition Report and approves the amended Surveillance Use Policy for the Unmanned Aerial Systems program.

2. ~~The City Council hereby accepts the Surveillance Acquisition Report and approves the Surveillance Use Policy for Community Video Streams.~~

3. The City Council hereby approves the updated Surveillance Use Policies for fixed video cameras.

Police Equipment Ordinance Approvals

4. The City Council hereby ~~accepts the Police Equipment Impact Statement and~~ approves the Police Equipment Use Policy for unmanned aerial systems.

5. BE IT FURTHER RESOLVED that the Berkeley City Council directs the following referrals to the City Manager for action:

    a. Refer the Community Video Stream Acquisition Report and Surveillance Use Policy to the Public Safety Policy Committee (PSPC) for further review; request that the City Manager work at the committee level to address the PAB's concerns and clarify operational ambiguity.

    b. Refer the UAS Surveillance Acquisition Report to the City Manager for research and analysis of alternative surveillance technology vendors capable of meeting the City of Berkeley's safety and surveillance needs while balancing privacy and civil liberties protections.

    c. Refer the UAS Military Equipment Impact Statement to the City Manager for research and analysis of alternative surveillance technology vendors capable of meeting the City of Berkeley's safety and surveillance needs while balancing privacy and civil liberties protections.

    ~~a.~~d. Refer to the City Manager to amend Ordinance 2.99 to include a violation/termination clause for surveillance technology vendors.

Contract Authority

BE IT FURTHER RESOLVED that the Berkeley City Council finds it in the public interest to reject any renewal, authorization, approval, or execution of a contract with Flock Safety.

~~4. The City Manager is authorized to amend the existing Contract #32400088 with Flock Group, Inc. (Flock Safety) to add Drone as First Responder hardware, software, and services for an initial three-year term, in an amount not to exceed $750,000.~~

~~5. The City Manager is authorized to amend the existing Contract #32400088 with Flock Group, Inc. (Flock Safety) to add fixed surveillance cameras for an initial four-year term, in an amount not to exceed $310,000, with an option to extend for one additional three-year term, for a total amount not to exceed $600,000.~~

~~6. The City Manager is authorized to amend the existing Contract #32400088 with Flock Group, Inc. (Flock Safety) to add Nova investigative software for a one-year term, in an amount not to exceed $75,000, funded by the Byrne State Crisis Intervention Program (SCIP) grant.~~

~~7. The City Manager is authorized to amend the existing Contract #32400088 with Flock Group, Inc. (Flock Safety) to renew Automated License Plate Readers (ALPRs) for a two-year term, in an amount not to exceed $330,000, with an option to extend for an additional two-year term, for a total amount not to exceed $660,000.~~

~~BE IT FURTHER RESOLVED that the total aggregate amount authorized under items 5 through 8 of this Resolution shall not exceed $1,465,000 for the initial contract terms, and shall not exceed $2,085,000 in the event all optional extension terms are exercised, with no individual contract term extending beyond seven years from the date of execution.~~

~~BE IT FURTHER RESOLVED that the City Manager is authorized to execute any amendments to the above contracts and the Master Services Agreement with Flock Safety, provided that any amendments do not increase the total amounts authorized herein and are consistent with the approved Use Policies and Impact Statements.~~

~~BE IT FURTHER RESOLVED that the authorized sworn officer strength of the Berkeley Police Department is hereby reduced by 3 full-time equivalent positions, effective July 1, 2026, with the resulting salary and benefit savings to fund the ongoing technology subscription costs authorized herein, the Senior Crime Analyst conversion, and the permanent funding of the Crime Analyst position that is currently grant-funded.~~

~~BE IT FURTHER RESOLVED that grant funds received under the SCIP grant and used for the Flock Nova contract shall not be used to supplant expenditures controlled by this body.~~

The foregoing Resolution was adopted by the Berkeley City Council on March 24, 2026, by the following vote:

Ayes: Bartlett, Blackaby, Humbert, Kesarwani, Lunaparra, O'Keefe, Taplin, Tregub, and Ishii.

Noes: None.

Absent: None.

_____
Adena Ishii, Mayor

Attest: _____
Mark Numainville, City Clerk

Surveillance Use Policy-Unmanned Aerial System (UAS)

1303.1 PURPOSE

The purpose of this policy is to establish guidelines for the use of an unmanned aerial system (UAS) and for the storage, retrieval and dissemination of images and data captured by the UAS. Department personnel shall adhere to requirements for Unmanned Aerial Systems covered in this policy as well as the corresponding Use Policy - 611.

1303.2 AUTHORIZED USE

Authorized operators shall only ~~may~~ deploy the UAS in the following circumstances, subsequent to supervisory approval for all deployments with the sole exception of Drone as First Responder (DFR) deployments:

1. To provide real-time situational awareness during high-risk or critical incidents, such as barricaded suspects, hostage situations, active shooters, the apprehension of armed and dangerous suspects, the pre-planning and service of a warrant allowing officers to create time and distance to formulate de-escalation strategies, facilitate safe tactical planning, and reduce the need for immediate physical engagement.

2. To assist in locating lost, missing, or injured persons during search and rescue operations.

3. To rapidly respond to calls for service to verify the nature of the incident, potentially determining that a law enforcement response is unnecessary for unfounded reports or low-priority incidents, thereby acting as a resource multiplier and keeping patrol officers available for other calls.

4. To locate fleeing suspects to effectively contain perimeters and reduce the need for dangerous ground-based foot pursuits.

5. To track fleeing vehicles from a safe distance, allowing patrol units to de-escalate or terminate dangerous ground pursuits while maintaining visual contact.

6. To clear interior buildings or confined spaces remotely to prevent potentially violent encounters between officers and hidden suspects.

7. To assist the Fire Department with fire mitigation and suppression, hazardous materials releases, or disaster response and recovery.

8. To remotely inspect potential explosive devices or hazardous objects.

9. To document complex crime scenes, accident scenes, or areas where an aerial perspective is critical for the investigation.

10. To respond to active criminal activity at mass gatherings or special events.

11. To mitigate hazards caused by other UAS interfering with emergency operations.

12. For pilot certification training and maintenance of proficiency.

13. To address other unforeseen exigent circumstances where there is an imminent threat to public safety, provided the deployment is consistent with the general privacy and safety principles of this policy.

1303.3 PROHIBITED USE

The UAS shall not be used:

1. To conduct random or arbitrary surveillance activities. This prohibition includes, but is not limited to, first amendment assemblies in accordance with Policy 428 First Amendment Assemblies.

2. To target a person based solely on actual or perceived characteristics, such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, or disability.

3. To harass, intimidate, or discriminate against any individual or group.

Furthermore, the UAS shall not be equipped with:

1. Facial recognition software

2. Biometric analysis capabilities

3. Weapons of any kind, including lethal or non-lethal munitions.

1303.4 DATA COLLECTION

Data collection shall be limited to video (visible and infrared) and associated telemetry (e.g., flight path, altitude) necessary for safe flight operations and situational awareness. The UAS will capture real-time video to assist pilots in navigating safely and assessing authorized scenes. These recordings shall be utilized solely for legitimate law enforcement purposes, including criminal investigations, administrative reviews, and training, in strict accordance with state laws and Department policy.

1303.5 DATA ACCESS

Access to videos shall be limited to authorized personnel with a legitimate law enforcement or administrative need. Any release or access to videos by third parties requires prior authorization and shall be limited to legally authorized agencies or pursuant to a valid court order.

1303.6 DATA PROTECTION

The Department shall implement and maintain comprehensive data security protocols to preserve the integrity, confidentiality, and lawful use of UAS videos. Video recording shall occur only during authorized operations and shall not include continuous or passive surveillance.

1303.7 CIVIL LIBERTIES AND RIGHTS PROTECTIONS

The Department acknowledges that UAS operations involve inherent privacy considerations, specifically the risk of inadvertently capturing footage of private areas (e.g., backyards or through windows) or uninvolved community members. To address this, the Department prioritizes civil liberties by restricting recording to authorized missions and strictly adhering to the restrictions on random surveillance outlined in Section 611.6 (Prohibited Use).

To safeguard these rights, UAS operations shall adhere to the following restrictions:

1. Absent a warrant or exigent circumstances, operators and observers shall adhere to FAA regulations and shall not intentionally record or transmit images of any location where a person would have a reasonable expectation of privacy (e.g., residence, yard, enclosure).

2. Operators and observers shall take reasonable precautions to avoid inadvertently recording or transmitting images of uninvolved community members or areas where there is a reasonable expectation of privacy. Cameras shall be diverted away from private spaces when not actively engaged in a permitted use.

3. For DFR operations, cameras shall be programmed to orient toward the horizon (preventing ground recording) while in transit to a call for service and shall only be directed toward the scene upon arrival at the authorized location.

1303.8 DATA RETENTION

UAS footage should be purged by BPD within 5 ~~60~~ days if it does not contain any data of evidentiary value. If the data has evidentiary value, it should be uploaded into BPD's evidence database and kept pursuant to the established retention guidelines set forth in policy 804-Records Maintenance and Release.

1303.9 PUBLIC ACCESS

Unauthorized use, duplication, and/or distribution of UAS camera footage is prohibited. Personnel shall not make copies of any UAS camera footage for their personal use and are prohibited from using a recording device such as a personal camera or any secondary video camera to capture UAS camera footage.

All UAS camera footage is property of the Berkeley Police Department and shall not be copied, released or disseminated in any form or manner outside the parameters of established policy, procedure, or laws.

The Custodian of Records, or their designee, will be responsible for handling requests for UAS camera footage.

1303.10 THIRD PARTY DATA SHARING

Pursuant to the Records Maintenance and Release policy, data collected from the UAS may only be shared with other law enforcement agencies on a case-by-case basis in connection with an active investigation, or in response to a lawful judicial warrant or court order in compliance with state and local law.

1303.11 TRAINING

The Program Coordinator will coordinate training of PICs and Visual Observers. The training course and materials will be approved through the training staff. An approved department instructor will oversee all training. Each training session will be documented and forwarded to the Policy and Training Bureau Sergeant.

1303.12 AUDITING AND OVERSIGHT

Division Captains or their designee shall ensure compliance with this Surveillance Use Policy.

The Office of Strategic Planning and Accountability shall conduct monthly ~~biennial~~ audits of UAS use. A report of these audits shall be published semiannually and should be sent to the Police Accountability Board.

Intentional violation of this policy may serve as grounds for disciplinary action pursuant to the Policy 1010, Personnel Complaints policy.

1303.13 MAINTENANCE

All UAS maintenance shall be conducted by the owner/operator of the device consistent with the manufacturer's specifications and as needed based on UAS usage.

Unmanned Aerial System (UAS) Operations

611 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the use of an unmanned aerial system (UAS) and for the storage, retrieval and dissemination of images and data captured by the UAS. Department personnel shall adhere to requirements for Unmanned Aerial Systems covered in this policy as well as the corresponding Surveillance Use Policy 1303.

611.1 DEFINITIONS

Drone as First Responder (DFR) - A mode of operation where a UAS is deployed immediately in response to a call for service or other emergency. This mode of operation provides real-time aerial situational awareness to dispatchers, analysts and responding officers, assisting in the assessment of incidents, the coordination of resources, and the potential de-escalation or clearance of calls without the need for immediate physical police presence.

Federal Aviation Administration (FAA) – An entity of the federal government that regulates all aspects of civil aviation.

Pilot in Command (PIC) –Trained officer who is the sole person responsible for the operation of the UAS.

Unmanned Aerial System (UAS) - An unmanned aircraft of any type that is capable of sustaining directed flight, whether preprogrammed or remotely controlled (commonly referred to as an unmanned aerial vehicle (UAV)), and all of the supporting or attached systems designed for gathering information through imaging, recording or any other means.

Visual Observer –Trained officer who may act as a spotter for PIC to assist in navigating the UAS and avoidance of hazards.

611.2 POLICY

Unmanned aerial systems may be utilized for the purpose of enhancing the department's mission to safeguard our diverse community by enabling remote visual assessment and real-time situational awareness in the situations specified in this policy. Any use of a UAS will also be in strict accordance with BMC 13.114 Sanctuary City Ordinance, constitutional and privacy rights, and FAA regulations.

All uses of the UAS shall be reported in compliance with the Berkeley Municipal Code (BMC) 2.99 Surveillance Technology Ordinance, and BMC 2.100 Police Equipment Ordinance.

Additionally, the Department shall publish data regarding specific requests, flight paths, and deployments on the Department's transparency portal. Flight logs and incident types for DFR operations should be published as soon as practicable, typically within one hour of docking.

611.3 PRIVACY

The Department acknowledges that UAS operations involve inherent privacy considerations, specifically the risk of inadvertently capturing footage of private areas (e.g., backyards or through windows) or uninvolved community members. To address this, the Department prioritizes civil liberties by restricting recording to authorized missions and strictly adhering to the restrictions on random surveillance outlined in Section 611.6 (Prohibited Use).

To safeguard these rights, UAS operations shall adhere to the following restrictions:

1) Absent a warrant or exigent circumstances, operators and observers shall adhere to FAA regulations and shall not intentionally record or transmit images of any location where a person would have a reasonable expectation of privacy (e.g., residence, yard, enclosure).

2) Operators and observers shall take reasonable precautions to avoid inadvertently recording or transmitting images of uninvolved community members or areas where there is a reasonable expectation of privacy. Cameras shall be diverted away from private spaces when not actively engaged in a permitted use.

3) For DFR operations, cameras shall be programmed to orient toward the horizon (preventing ground recording) while in transit to a call for service and shall only be directed toward the scene upon arrival at the authorized location.

611.4 PROGRAM COORDINATOR

The Police Chief will appoint a program coordinator who will be responsible for the management of the UAS program. The program coordinator will ensure that policies and procedures conform to current laws, regulations, and best practices.

611.5 PERMITTED USE

Authorized operators shall only ~~may~~ deploy the UAS in the following circumstances, subsequent to supervisory approval for all deployments with the sole exception of Drone as First Responder (DFR) deployments:

1) To provide real-time situational awareness during high-risk or critical incidents, such as barricaded suspects, hostage situations, active shooters, the apprehension of armed and dangerous suspects, the pre-planning and service of a warrant allowing officers to create time and distance to formulate de-escalation strategies, facilitate safe tactical planning, and reduce the need for immediate physical engagement.

2) To assist in locating lost, missing, or injured persons during search and rescue operations.

3) To rapidly respond to calls for service to verify the nature of the incident, potentially determining that a law enforcement response is unnecessary for unfounded reports or low-priority incidents, thereby acting as a resource multiplier and keeping patrol officers available for other calls.

4) To locate fleeing suspects to effectively contain perimeters and reduce the need for dangerous ground-based foot pursuits.

5) To track fleeing vehicles from a safe distance, allowing patrol units to de-escalate or terminate dangerous ground pursuits while maintaining visual contact.

6) To clear interior buildings or confined spaces remotely to prevent potentially violent encounters between officers and hidden suspects.

7) To assist the Fire Department with fire mitigation and suppression, hazardous materials releases, or disaster response and recovery.

8) To remotely inspect potential explosive devices or hazardous objects.

9) To document complex crime scenes, accident scenes, or areas where an aerial perspective is critical for the investigation.

10) To respond to active criminal activity at mass gatherings or special events.

11) To mitigate hazards caused by other UAS interfering with emergency operations.

12) For pilot certification training and maintenance of proficiency.

13) To address other unforeseen exigent circumstances where there is an imminent threat to public safety, provided the deployment is consistent with the general privacy and safety principles of this policy.

611.6 PROHIBITED USE

1) The UAS shall not be used:

   a) To conduct random or arbitrary surveillance activities. This prohibition includes, but is not limited to, first amendment assemblies in accordance with Policy 428 First Amendment Assemblies.

   b) To target a person based solely on actual or perceived characteristics, such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, or disability.

   c) To harass, intimidate, or discriminate against any individual or group.

2) Furthermore, the UAS shall not be equipped with:

   a) Facial recognition software

b) Biometric analysis capabilities

c) Weapons of any kind, including lethal or non-lethal munitions.

611.7 TRAINING

The Program Coordinator will coordinate training of PICs and Visual Observers. The training course and materials will be approved through the training staff. An approved department instructor will oversee all training. Each training session will be documented and forwarded to the Policy and Training Bureau Sergeant.

611.8 RETENTION REQUIREMENTS

UAS footage should be purged by BPD within 5 ~~60~~ days if it doesn't contain any data of evidentiary value. If the data has evidentiary value, it should be uploaded into BPD's evidence database and kept pursuant to the established retention guidelines set forth in policy 804-Records Maintenance and Release.

611.9 RELEASE OF RECORDINGS

1) Unauthorized use, duplication, and/or distribution of UAS camera footage is prohibited. Personnel shall not make copies of any UAS camera footage for their personal use and are prohibited from using a recording device such as a personal camera or any secondary video camera to capture UAS camera footage.

2) All UAS camera footage is property of the Berkeley Police Department and shall not be copied, released or disseminated in any form or manner outside the parameters of established policy, procedure, or laws.

3) The Custodian of Records, or their designee, will be responsible for handling requests for UAS camera footage.

External Fixed Video Surveillance Cameras

351.1 PURPOSE AND SCOPE

This policy provides guidance for the placement and monitoring of City of Berkeley external fixed video surveillance cameras by the Berkeley Police Department (BPD).

This policy only applies to fixed, overt, marked external video surveillance systems utilized by the BPD. It does not apply to mobile audio/video systems, covert audio/video systems or any other image-capturing devices used by the Department, as authorized by the City Council for use by other City Departments. BPD Personnel shall adhere to the requirements for External Fixed Video Surveillance Cameras covered in this policy as well as the corresponding Surveillance Use Policy -1304.

351.2 POLICY

The Berkeley Police Department utilizes a video surveillance system to enhance its anti-crime strategy, to effectively allocate and deploy personnel, and to enhance safety and security in public areas. As specified by this policy, cameras may be placed in strategic locations throughout the City to record, deter, and solve crimes, to help the City safeguard against potential threats to the public, and to help manage emergency response situations during natural and human-made disasters, among other uses specified in Section 351.3.1.

Video surveillance in public areas will be conducted in a legal and ethical manner while recognizing and protecting constitutional standards of privacy.

351.3 OPERATIONAL GUIDELINES

Only City Council-approved video surveillance equipment shall be utilized. BPD members authorized to review video surveillance may only record and review public areas and public activities where no reasonable expectation of privacy exists and pursuant to Section 351.3.1. The City Manager shall obtain Council approval of any proposed additional locations for the placement and use of video surveillance technology.

351.3.1 PLACEMENT REVIEW AND MONITORING

Camera placement will only occur in locations approved by the City Council and will be guided by this policy and the underlying purpose or strategy associated with the overall video surveillance plan. As appropriate, the Chief of Police should confer with other affected City departments when evaluating camera placement. Environmental factors, including lighting, location of buildings, presence of vegetation or other obstructions, should also be evaluated when determining placement.

Camera placement includes existing cameras such as those located at San Pablo Park, the Berkeley Marina, and cameras placed in Council identified and approved intersections throughout the City, and potential future camera locations as approved by City Council.

Current City Council approved location

- 6th Street at University Avenue
- San Pablo Avenue at University Avenue
- 7th Street at Dwight Way
- San Pablo Avenue at Dwight Way
- 7th Street at Ashby Avenue
- San Pablo Avenue at Ashby Avenue
- Sacramento Street at Ashby Avenue
- College Avenue at Ashby Avenue
- Claremont Avenue at Ashby Avenue
- 62nd Street at King Street

The cameras shall only record video images and not sound. Recorded images pursuant to Section 351.5 may be accessed, reviewed, and used for specific criminal or BPD administrative investigations and video surveillance may be accessed and reviewed by authorized BPD personnel for the following purposes:

(a) To support specific and active criminal investigations.

(b) To support serious traffic-related investigations.

(c) To support police misconduct investigations,

(d) To respond to and review critical incidents or natural disasters.

Unauthorized recording, viewing, reproduction, dissemination, or retention of video footage is prohibited.

351.3.2 FIXED CAMERA MARKINGS

All public areas monitored by video surveillance equipment shall be marked in a conspicuous manner with unobstructed signs to inform the public that the area is under police surveillance.

351.3.3 INTEGRATION WITH OTHER TECHNOLOGY

The Department may integrate technologies not otherwise prohibited with the video surveillance system, provided that such use does not conflict with this policy or expand internal or external access beyond what is allowed by policy. For example, integration may occur on a shared access platform where video data and automated license plate reader data are viewable in the same system.

351.4 VIDEO SUPERVISION

Access to video surveillance camera data shall be limited to Berkeley Police Department (BPD) personnel utilizing the camera database for uses authorized above, with technical assistance from Public Works Department and Department of Information Technology personnel. Information may be shared in accordance with Sections 351.6 or 1304.9 below. BPD members seeking access to the camera system shall obtain the approval of the Investigations Division Captain, or their designee.

Supervisors should monitor video surveillance access and usage to ensure BPD members are complying with this policy, other applicable department policy, and applicable laws. Supervisors should ensure such use and access is appropriately documented.

351.4.1 VIDEO LOG

No one without authorization will be allowed to login and view the recordings. Those who are authorized and login should automatically trigger the audit trail function to ensure compliance with the guidelines and policy.

351.4.2 PROHIBITED ACTIVITY

Video surveillance systems will not intentionally be used to invade the privacy of individuals or observe areas where a reasonable expectation of privacy exists.

Video surveillance systems shall not be used in an unequal or discriminatory manner and shall not target protected individual characteristics including, but not limited to race, ethnicity, national origin, religion, disability, gender or sexual orientation.

Video surveillance equipment shall not be used to harass, intimidate or discriminate against any individual or group.

Video surveillance systems and recordings are subject to the Berkeley Police Department's Immigration Law Policy, and hence may not be shared with federal immigration enforcement officials, unless required by federal law.

Video recordings shall not be disclosed to law enforcement agencies from other states if the purpose of the request is to support the enforcement of laws that restrict or criminalize reproductive rights or rights regarding the provision or receipt of gender-affirming care.

351.5 STORAGE AND RETENTION OF MEDIA

Video surveillance recordings are not government records pursuant to California Government Code 34090 in and of themselves. Except as otherwise permitted in this section, video surveillance recordings shall be purged within one hundred and eighty (180) days of recording. Recordings of incidents involving use of force by a police officer or involving, detentions, arrests, or recordings relevant to a formal or informal complaint against a sworn police officer shall be retained for a minimum of two years and one month. Recordings relating to court cases and complaints against BPD sworn officers that are being adjudicated will be manually deleted at the same time other evidence associated with the case is purged in line with the Department's Evidence Retention policy. Any recordings related to a police misconduct investigation shall be maintained until such matter is fully adjudicated, at which time it shall be deleted in line with the Department's ER~~R~~vidence Retention policy, and any applicable orders from the court.

Any recordings needed as evidence in a criminal or police misconduct proceeding shall be copied to a suitable medium and booked into evidence in accordance with current evidence procedures.

351.5.1 EVIDENTIARY INTEGRITY

All media downloaded and retained pursuant to this Policy shall be treated in the same manner as other evidence. Media shall be accessed, maintained, stored and retrieved in a manner that ensures its integrity as evidence, including strict adherence to chain of custody requirements.

Electronic trails, including encryption, digital masking of innocent or uninvolved individuals to preserve anonymity, authenticity certificates and date and time stamping, shall be used as appropriate to preserve individual rights and to ensure the authenticity and maintenance of a secure evidentiary chain of custody.

351.6 RELEASE OF VIDEO IMAGES

Data collected and used in a police report shall be made available to the public in accordance with department policy and applicable state or federal law, also referenced in Policy 1304.8.

Requests for recorded video images from the public or the media shall be processed in the same manner as requests for department public records pursuant to Policy 804, Records Maintenance and Release.

Requests for recorded video from other law enforcement agencies shall be referred to the Investigations Division Captain, or their designee for release in accordance with this policy and must be related to a specific active criminal investigation.

Requests for recorded video from the Office of Director of Police Accountability and Police Accountability Board shall be referred to the Investigations Division Captain, or their designee, for release in accordance with Charter Article XVIII, Section 25, Subdivision (20)(a).

Recorded video images that are the subject of a court order or subpoena shall be processed in accordance with the established department subpoena process.

The Chief of Police will report any request from federal immigration authorities, vendor, or any non-local agency to access data for federal immigration enforcement purposes within 10 days of receiving the request.

In the event a Federal Agency is given BPD-owned data stored with Flock, the Berkeley Police Chief or designee will notify the City Manager, City Attorney, and City Council within 72 hours of the discovery of the incident.

351.7 VIDEO SURVEILLANCE AUDIT

The video surveillance software generates a site log each time the system is accessed. The site log is broken down by server, device, user or general access. The site log is kept on the server for two years and is exportable for reporting. System audits will be conducted by the Office of Strategic Planning and Accountability (OSPA) on a regular basis, at least monthly ~~biennial~~. A report of these audits shall be published semiannually, and should be sent to the Police Accountability Board. As part of the audit, OSPA will confirm that BPD doesn't enter any direct data sharing agreements or give direct access to outside agencies. A log of any instance of when surveillance footage has been shared, including date, time, reasons for search, and any recipient agencies.

BPD will enforce against prohibited uses of the cameras pursuant to Policy 1010, Personnel Complaints, or other applicable law or policy. The City Manager shall enforce against any prohibited use of cameras and/or access to data by other City of Berkeley personnel.

The audit shall be documented in the form of an internal department memorandum to the Chief of Police. The memorandum shall include any data errors found so that such errors can be corrected. After review by the Chief of Police, the memorandum and any associated

documentation shall be published on the City of Berkeley website in an appropriate location, and retained within the Office of Strategic Planning and Accountability.

351.8 TRAINING

All department members authorized to operate or access video surveillance systems shall receive appropriate training. Training should include guidance on the use of cameras, associated software, and review of relevant policies and procedures, including this policy, as well as review of relevant City of Berkeley laws and regulations. Training should also address state and federal law related to the use of video surveillance equipment and privacy. All relevant recordings that are utilized will be collected pursuant to Policy 802, Property and Evidence, and retained pursuant to Policy 804, Records and Maintenance.

351.9 MAINTENANCE

It shall be the responsibility of the Public Works Director to facilitate and coordinate any updates and required maintenance, with access limited to that detailed in the City Manager's promulgated policies.

Surveillance Use Policy-External Fixed Video Surveillance Cameras

1304.1 PURPOSE

This policy provides guidance for the use of City of Berkeley external fixed video surveillance cameras by the Berkeley Police Department (BPD).

This policy only applies to fixed, overt, marked external video surveillance systems utilized by BPD. It does not apply to mobile audio/video systems, covert audio/video systems or any other image-capturing devices used by the Department. Department personnel shall adhere to the requirements for External Fixed Video Surveillance Cameras covered in this policy as well as the corresponding Use Policy-351.

This Surveillance Use Policy is legally-enforceable pursuant to BMC 2.99.

1304.2 AUTHORIZED USE

Only BPD members who receive training on this policy, who are then granted access by an administrator may access the data from the video surveillance cameras. This data may only be accessed to further a legitimate law enforcement purpose, as listed in this Policy. Members must follow the necessary logging mechanisms, such as case number and case type when querying the database.

The cameras shall only record video images and not sound. Recorded images pursuant to Section 351.5 may be accessed, reviewed, and used for specific criminal or BPD administrative investigations and video surveillance may be accessed and reviewed by authorized BPD personnel for the following purposes:

(a) To support specific and active criminal investigations.

(b) To support serious traffic-related investigations.

(c) To support police misconduct investigations, and

(d) To respond to and review critical incidents or natural disasters.

Unauthorized recording, viewing, reproduction, dissemination, or retention of video footage is prohibited.

The following are prohibited uses of the video surveillance system:

(a) Unauthorized recording, viewing, reproduction, dissemination, or retention of video footage is prohibited.

(b) Video surveillance systems will not intentionally be used to invade the privacy of individuals or observe areas where a reasonable expectation of privacy exists.

(c) Video surveillance systems shall not be used in an unequal or discriminatory manner and shall not target protected individual characteristics including, but not limited to race, ethnicity, national origin, religion, disability, gender or sexual orientation.

(d) Video surveillance equipment shall not be used to harass, intimidate or discriminate against any individual or group.

(e) Video surveillance systems and recordings are subject to the Berkeley Police Department's Immigration Law Policy, and hence may not be shared with federal immigration enforcement officials, unless required by federal law.

(f) Video recordings shall not be disclosed to law enforcement agencies from other states if the purpose of the request is to support the enforcement of laws that restrict or criminalize reproductive rights or rights regarding the provision or receipt of gender-affirming care.

1304.3 DATA COLLECTION

The cameras will film and store video on City of Berkeley encrypted servers. License plate and facial recognition data hardware is not installed on the cameras and may not be installed or used unless approved by the City council. Audio is a standard feature of the camera, but is deactivated by the system administrator and may not be activated or used unless approved by the City Council. Surveillance camera data shall be wholly owned by the City of Berkeley.

1304.4 DATA ACCESS

Access to video surveillance cameras data shall be limited to BPD personnel utilizing the camera database for uses described above and pursuant to Use Policy 351, with technical assistance from Public Works Department and Department of Information Technology personnel. Information may be shared in accordance with 1304.9 below. BPD members seeking access to the video surveillance system shall obtain the approval of the Investigations Division Captain, or their designee.

Supervisors should monitor camera access and usage to ensure BPD members are complying with this policy, other applicable department policy, and applicable laws. Supervisors should ensure such use and access is appropriately documented.

1304.5 DATA PROTECTION

All data transferred from the cameras and the servers shall be encrypted. Access to the data must be obtained through the Public Works Department according to this policy and published regulations that limit access and use of data by Public Works and other City Departments and personnel. All system access including system log-in, access duration, and data access points is accessible and reportable and shall be documented by the Public Works Department's authorized administrator. All relevant recordings that are utilized will be collected pursuant to Policy 802, Property and Evidence, and retained pursuant to Policy 804 Records and Maintenance.

1304.6 CIVIL LIBERTIES AND RIGHTS PROTECTION

The Berkeley Police Department is dedicated to the most efficient utilization of its resources and services in its public safety endeavors. The Berkeley Police Department recognizes the need to protect its ownership and control over shared information and to protect the privacy and civil liberties of the public, in accordance with federal and state law. Provisions of this policy, including

1304.4 Data Access, 1304.5 Data Protection, 1304.7 Data Retention, 1304.8 Public Accessand 1304.9 Third Party Data Sharing serve to protect against any unauthorized use of video surveillance camera data. License plate and facial recognition data hardware is not installed on the cameras. Audio is a standard feature of the camera, but is deactivated by the system administrator. These procedures ensure the data is not used in a way that would violate or infringe upon anyone's civil rights and/or liberties, including but not limited to potentially disparate or adverse impacts on any communities or groups.

1304.7 DATA RETENTION

Video surveillance recordings are not government records pursuant to California Government Code 34090 in and of themselves. Except as otherwise permitted in this section, video surveillance recordings shall be purged within one hundred and eighty (180) days of recording. Recordings of incidents involving use of force by a police officer or involving detentions, arrests, or recordings relevant to a formal or informal complaint against a police officer shall be retained for a minimum of two years and one month. Recordings relating to court cases and complaints against BPD sworn officers that are being adjudicated will be manually deleted at the same time other evidence associated with the case is purged in line with the Department's evidence retention policy. Any recordings related to BPD administrative proceedings pursuant to this section shall be maintained until such matter is fully adjudicated, at which time it shall be deleted in line with the Department's evidence retention policy, and any applicable orders from the court. All data will automatically delete after the aforementioned retention period by the System Administrator from Public Works.

Any recordings needed as evidence in a criminal or police misconduct proceeding shall be copied to a suitable medium and booked into evidence in accordance with current evidence procedures.

This policy reaffirms the City Manager’s authority, which may be delegated to the Berkeley Police Chief, to pause or end the deployment of the subject equipment at any time and for any cause. The City Council shall be, within 48 hours, notified of any such decision to pause or end its deployment.

1304.8 PUBLIC ACCESS

Data collected and used in a police report shall be made available to the public in accordance with department policy and applicable state or federal law.

Requests for recorded video images from the public or the media shall be processed in the same manner as requests for department public records pursuant to Policy 804.

Recorded video images that are the subject of a court order or subpoena shall be processed in accordance with the established department subpoena process.

1304.9 THIRD-PARTY DATA-SHARING

Requests for recorded video from other law enforcement agencies shall be referred to the Investigations Division Captain, or their designee for release in accordance with this policy, and must be related to a specific active criminal investigation. Data collected from the video surveillance system may be shared with the following:

(a) The District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence;
(b) Other law enforcement personnel as part of an active criminal investigation;
(c) Recorded video images that are the subject of a court order or subpoena shall be processed in accordance with the established department subpoena process

Requests for recorded video from the Office of Director of Police Accountability and Police Accountability Board shall be referred to the Investigations Division Captain, or their designee, for release in accordance with Charter Article XVIII, Section 125, Subdivision (20)(a). The Chief of Police will report any request from federal immigration authorities, vendor, or any non-local agency to access data for federal immigration enforcement purposes within 10 days of receiving the request.

In the event a Federal Agency is given BPD-owned data stored with Flock, the Berkeley Police Chief or designee will notify the City Manager, City Attorney, and City Council within 72 hours of the discovery of the incident.

1304.10 TRAINING

All BPD members authorized to operate or access video surveillance systems shall receive appropriate training. Training should include guidance on the use of cameras, associated software, and review of relevant policies and procedures, including this policy as well as review of relevant City of Berkeley laws and regulations.

Training should also address state and federal law related to the use of video surveillance equipment and privacy. All relevant recordings that are utilized will be collected pursuant to Policy 802 Property and Evidence, and retained pursuant to Policy 804 Records Maintenance.

1304.11 AUDITING AND OVERSIGHT

The video surveillance software generates a site log each time the system is accessed. The site log is broken down by server, device, user or general access. The site log is kept on the server for two years and is exportable for reporting. External fixed video surveillance camera system audits will be conducted by the Office of Strategic Planning and Accountability (OSPA) on a regular basis, at least monthly ~~biennial~~. A report of these audits will be published semiannually and sent to the Police Accountability Board. As part of the audit, OSPA will confirm that BPD doesn't enter any direct data sharing agreements or give direct access to outside agencies. A log of any instance of when surveillance video and/or audio data has been shared, including date, time, reasons for search, and any recipient agencies.

BPD will enforce against prohibited uses of this policy pursuant to Policy 1010, Personnel Complaints or other applicable law or policy. The City Manager shall enforce against any prohibited use of the cameras and/or access to data by other City of Berkeley personnel.

The audit shall be documented in the form of an internal department memorandum to the Chief of Police. The memorandum shall include any data errors found so that such errors can be corrected. After review by the Chief of Police, the memorandum and any associated documentation shall be placed into the annual report filed with the City Council pursuant to BMC Section 2.99.020 2. d., published on the City of Berkeley website in an appropriate location, and retained within the Professional Standards Bureau.

1304.12 ACCOUNTABILITY

All saved data will be safeguarded and protected by both procedural and technological means. The Berkeley Police Department will observe the following safeguards regarding access to and use of stored data:

(a) Non-law enforcement requests for access to stored external fixed video surveillance camera data shall be processed according to the Records Maintenance and Release Policy in accordance with applicable law.

(b) All external fixed video surveillance camera data downloaded to any workstation or server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.

(c) Berkeley Police Department members approved to access external fixed video surveillance camera data under these guidelines are permitted to access the data for legitimate California law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

(d) Aggregated external fixed video surveillance camera data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the consent of the Chief of Police or City Manager.

(e) Measures will be taken to ensure the accuracy of external fixed video surveillance camera information. Errors discovered in external fixed video surveillance camera data collected by external fixed video surveillance camera units shall be marked, corrected or deleted in accordance with the type and severity of the error in question.

(f) Such external fixed video surveillance camera data may be released to other authorized and verified law enforcement officials and agencies for legitimate California law enforcement purposes.

(g) Every external fixed video surveillance camera browsing inquiry must be documented by either the associated Berkeley Police case number or incident number, and/or a reason for the inquiry. For security or data breaches, see the Records Release and Maintenance Policy.

1304.13 MAINTENANCE

It shall be the responsibility of the Public Works Department to facilitate and coordinate any updates and required maintenance with access limited to that detailed in the City Manager's promulgated policies.