PRESIDIO TRUST

**INTERNAL POLICY**

**Title:** Technologically Assisted Physical Surveillance Policy

**Owner:** Department of Public Safety

**Effective Date:** April 23, 2024

## PURPOSE, SCOPE & APPLICABILITY

Purpose:

The Technologically Assisted Physical Surveillance (TAPS) Policy ("Policy") defines the manner in which the Security Camera System, both fixed and mobile, and automated License Plate Reader (LPR) technology will be used to support park operations and deter crime. We understand that the use of TAPS systems can make some visitors feel unwelcome, reinforcing a misperception that the Presidio is a private place instead of a public, national park site. However, this policy establishes limits on the use of TAPS systems to balance these competing interests.

Scope:

This Policy aims to ensure that the deployment of TAPS complies with applicable privacy rights, including the Privacy Act and Constitutional protections, aligns with organizational safeguards, and contributes to the overall security and efficiency of park operations. This Policy encompasses the entire lifecycle of TAPS, from planning and implementation to data storage and access.

Applicability:

This Policy applies to all Trust personnel that use or plan to use TAPS, including security systems and LPR technology. All users of TAPS must be approved in advance by the Trust CEO.

All individuals, including employees, consultants, volunteers, and vendors acting on behalf of Presidio Trust, are required to comply with this Policy. All Security Camera Systems installed or operated by third parties in Area B of the Presidio are required to comply with this policy. This Policy does not apply to the operations of the U.S. Park Police (USPP) or other law enforcement surveillance unrelated to the Trust and unrelated to the LPR technology noted below.

## POLICY STATEMENTS

1. TAPS shall be conducted or approved by the Trust solely for the purpose of obtaining information to monitor and improve park planning efforts, construction projects, resource management activities, park operations, or to facilitate for the USPP the detection, investigation, prevention and deterrence of terrorist attacks and criminal activity in areas with a documented history of criminal activity or where there is a reasonable expectation that criminal conduct might occur.
    a. TAPS devices shall be installed and programmed to protect privacy rights and, to the maximum extent possible, protect privacy interests.

b. Unauthorized recording, viewing, reproduction, dissemination, or retention is prohibited.

    i. The Trust use of security camera systems, both fixed and mobile, is allowed for non-law enforcement purposes only. Law enforcement personnel may request access consistent with paragraph 5 below.

    ii. The USPP is authorized in accordance with the Trust Act, Public Law 104-333, Section 104(i), and the 1998 Memorandum of Agreement between the Trust and the National Park Service (NPS), to use surveillance, including LPR and subscription-based criminal data-base services, consistent with USPP authorities, when conducting law enforcement activities within Area B.

2. Surveillance Limitations

    a. No individual or group shall be subjected to surveillance based on characteristics such as race, ethnicity, color, ancestry, national origin, religious or philosophical beliefs, political affiliation, or views, physical or mental disability, medical condition, marital status, sexual orientation, age, gender, gender identity, genetic and/or biometric data, or trade union membership. Additionally, no location shall be subjected to surveillance due to the characteristics of the individuals who may frequent that location.

    b. TAPS devices, including both Security Camera System, both fixed and mobile, and license plate reader technology, will only be deployed in and record and/or monitor public areas and public activities where there is no reasonable expectation of privacy. Notably, surveillance devices shall not be installed in restrooms or other private spaces.

    c. Surveillance devices shall only record video images and not sound.

    d. Use of TAPS systems shall not be used to curtail, directly or indirectly, the free exercise of First Amendment freedoms and related values.

    e. Surveillance activities shall be conducted in accordance with the Privacy Act, the E-Government Act, and the Federal Records Information Management Act, including but not limited to the publication of applicable Privacy Impact Statements (PIAs), Adapted PIAs, Privacy Threshold Analyses (PTAs) and System of Records Notices (SORNs), as required.

3. TAPS Deployment and Location Approvals:

    a. The authority to approve TAPS systems locations is with the Board of Directors, as delegated to the CEO.

    b. In instances where surveillance is implemented to deter crime, the surveilled area must be limited to a reasonable distance from the location or building where the crime occurred or where the alleged criminal perpetrator is expected.

    c. Security Camera Systems that are fixed shall be installed consistent with the requirements of the National Environmental Policy Act and the National Historic Preservation Act and the Presidio Trust's federal regulations, planning policies, and guidelines implementing these federal laws.

    d. Security Camera Systems that are mobile shall be installed as a deterrent in areas with a documented history of criminal activity or where there is a reasonable expectation that criminal conduct might occur.

e. LPR cameras shall be installed consistent with the requirements of the National Environmental Policy Act and the National Historic Preservation Act and the Presidio Trust's federal regulations, planning policies, and guidelines implementing these federal laws.

LPRs are to be positioned in a manner to capture the license plate area of the vehicle and will not collect images of any persons (including the driver or pedestrian(s)).

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

4. Access to and Use of Surveillance Information:

a. The Trust shall not sell, share, or transfer surveillance information, except upon request by a law enforcement agency and as permitted by law. LPR data is accessed only by authorized USPP or other law enforcement agencies.

b. Surveillance information may be reviewed and monitored for the following purposes only:

i. To respond to and review critical incidents or natural disasters.

i. When requested by a law enforcement agency and permitted by law, authorized Trust personnel may access non-LPR surveillance information in response to a specific and active criminal investigation.

ii. Authorized Trust personnel may access non-LPR surveillance information in support of administrative investigations.

iii. Access to LPR data is allowed to further law enforcement purposes only and is restricted to credentialed USPP and Park Rangers. USPP will identify staff to act as account administrator(s) for the purposes of managing the creation of LPR access accounts, oversight of those accounts, and performing minor administrative tasks.

iv. Trust employees are not authorized to access LPR data. The Trust Director of the Department of Public Safety will provide program administrative oversight of the LPR system only for purposes of finance, contract review, and contract performance metrics.

c. System Access Report: A System Access Report including system log-in, queries, purpose of queries, access duration, and data access points for all security camera systems shall be produced annually by the system administrator. This System Access Report shall be part of any annual review of the security camera systems.

5. Surveillance and LPR data will be retained for 30 days. Any retained surveillance or LPR data will be destroyed when transmitted to an LE agency or a request for retention has been completed. LPR data retained by law enforcement personnel will be in accordance with USPP and/or specific law enforcement agency data retention policy.

6. The Department of Public Safety will conduct an annual review of TAPS systems, in consultation with the USPP related to LPR, to assess the scope and effectiveness of the program.

*This Policy supplements applicable federal law and regulations which shall control in the event of any direct conflict. A violation of this Policy or any procedures promulgated under the authority of this Policy*

*does not create any right or benefit, substantive or procedural, enforceable at law by any person against the United States, its agencies, its directors, officers or employees, or any other person.*

**DEFINITIONS**

Access – Refers to the cards, passcodes, and keys provided to unlock a security mechanism.,

Fixed or Mobile Video Surveillance – Use of a camera as a means of viewing or recording activities or conditions other than those occurring within the sight or immediate vicinity of a law enforcement official or agent thereof who is aware of such use.

License Plate Reader (LPR) Technology – means a searchable computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms to read and convert images of registration plates and the characters they contain into computer-readable data. Captured data may include a whole or partial license plate number, vehicle make, model, and color, as well as the date, time, and location when the image was collected.

Physical Surveillance – Observation or detection of activities, conditions, locations, or objects.

Private Activity – An activity, condition, or location is private when the area where it occurs or exists, and other relevant considerations afford it a constitutionally protected reasonable expectation of privacy. A *place* is private if physical entry therein would be an intrusion upon a constitutionally protected reasonable expectation of privacy.

Technologically-Assisted Physical Surveillance – includes the utilization of License Plate Reader (LPR) technology and fixed or mobile video surveillance and may include any one of five different types of technology: video surveillance; tracking devices; illumination devices; telescopic devices; and detection devices (e.g., devices capable of detecting concealed items).

**RELATED REFERENCES**

Privacy Act of 1974. https://www.justice.gov/Overview_2020/dl?inline

The Trust Act, Omnibus Parks Public Lands Act of 1996, Public Law 104-333. (11/12/1996). https://www.congress.gov/104/plaws/publ333/PLAW-104publ333.pdf

National Institute of Standards and Technology. NIST 800-53 rev. 5.1 - Security and Privacy Controls for Information Systems and Organizations (12/10/2020). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Trust Adapted Privacy Impact Assessment - FlockSafety Automated License Plate Recognition (ALPR)

USPP Privacy Threshold Analysis- FlockSafety Automated License Plate Recognition (ALPR) at Golden Gate NRC (02/17/2023).

**REVISION HISTORY**

Original Document Approved- June 24, 2019
Approved on April 23, 2024 by the Executive Team.