DRAFT - SAN MATEO COUNTY
AIRPORTS OPERATIONS AND SECURITY SYSTEMS
PRIVACY POLICY

PURPOSE:

The San Mateo County Airports Operations and Security Systems Privacy Policy (Policy) outlines the purpose of using automated airport operations and security systems at the San Mateo County Airports (Airports). It also outlines how information collected through the use of these systems will be used, disclosed, stored and destroyed.

The San Carlos Airport has installed automated aircraft identification and security systems that capture images of aircraft as they pass by. These systems digitally record video and/or still images, 24 hours a day, 7 days a week. This information is processed and stored in an automated fashion, on servers and storage devices owned and operated by the County. Cameras are openly installed at various locations at the Airport that are defined as being restricted or protected, in both public and non-public areas of the facility, where neither airport employees nor the public have any reasonable expectation of privacy. All records acquired by these systems are the property of San Mateo County.

The purpose of these data collection and imaging systems is to provide data to support airport operations and security. Examples of use of the data include: responding to customer complaints and questions, incident review, public education, billing of fees, providing security, and law enforcement. In connection with such uses, personally identifiable information will not be disclosed unless it is absolutely required to address an airport operations or security issue.

SYSTEM MANAGEMENT

The Airport Manager shall be responsible for ensuring employees comply with the requirements of this Policy and the San Mateo County's Information Technology Security Policy. The Airport Manager is also responsible and accountable for managing the data collected and ensuring the privacy and civil liberties protection and other provisions of this Policy are carried out, including ensuring that all data collected, disclosed, stored and destroyed is in accordance with local, State, and Federal laws and guidelines. It remains, however, the personal responsibility of all authorized personnel with access to collected data to take reasonable measures to protect the privacy and civil liberties of individuals, as well as the security and confidentiality of the data.

Use of Airports operations and security systems data is restricted to the purposes outlined in this Policy. The Airport Manager, the Director of Public Works, or their designees shall authorize access to these systems by: 1) County employees in good standing responsible for, or assisting with, Airport operations and security; or 2) third-party vendors responsible for, or assisting with, Airport operations and security. Airport employees shall not use or allow others to use the equipment or database records for any unauthorized purpose.

SAFETY AND ACCOUNTABILITY

San Mateo County Airports will observe the following safeguards regarding access to and use of stored data:

1. All data resulting from the Airport's operations and security systems shall be accessible only through a unique password-protected account. The County will utilize firewalls and other reasonable physical, technological, administrative, procedural, and security measures to mitigate the risk of unauthorized access to the system. Use of and access to the system shall be in compliance with the County's information technology policies and procedures and this Policy.

2. Authorized users are permitted to access data for legitimate Airport business purposes only. All authorized users shall be trained in the technical, legal and ethical use of airport operations and security data.

3. All designated County employees shall receive a copy of this Policy and provide written acknowledgement that they have read and understand the County's Policy prior to being granted access. All authorized third-party vendors will be provided a copy and agree to the terms of this Policy prior to systems' access.

4. The Airport Manager or his/her designee will, no less frequently than every twelve (12) months, conduct an audit sampling of system utilization, access, employee training, and/or signed Policy documents, etc., to verify access and use is in accordance with this Policy. The first audit sampling described above shall be conducted within six (6) months of system implementation. The results of that sampling will be provided in a report to the Board of Supervisors.

5. In the event the Airport engages an outside vendor for billing purposes and to process payment card transactions, the vendor shall comply with the Payment

Card Industry Data Security Standards (“PCI DSS”) and all applicable data collection safeguards as described herein.

DATA RETENTION

The Airport will retain camera/video recordings resulting from the use of these systems for a period of no more than one (1) year. Once the retention period has expired, the record will be purged entirely from all active and backup systems. In certain situations, data may be kept longer if necessary for safety, security, law enforcement, or as required by law. In such cases, the justification of such action and intended use shall be documented and retained, as allowed by law and as provided for in the County’s document retention guidelines.

RECORDS REQUESTS

External requests for data collected will be processed in accordance with the California Public Records Act (CPRA) and Freedom of Information Act (FOIA). The Airport will make every effort to protect personally identifiable information as allowed by law. All requests under CPRA or FOIA will be reviewed by the County’s legal Counsel for approval. All responses to such requests will be limited to the maximum extent permitted by law. The Airport Manager will maintain a log of all external records requests that are not a result of normal Airports operations, maintenance, or administration of the system. The log will include, at minimum; the date, content, and identification of the person or persons to whom a record was provided or denied. Records may be shared with law enforcement agencies for official law enforcement purposes or as otherwise required by law.

DATA ACCURACY AND APPEALS

The Airport will take reasonable measures to ensure the accuracy of all data collected by authorized agents for third party billing purposes. Any errors or discrepancies in data collected should be communicated back to the third party vendor to be marked, corrected, or deleted in accordance with the type of error in question. If an aircraft operator disagrees with the determination of the claim, they have a right to submit a written request for appeal for billing matters within thirty (30) days of the date of the decision being appealed. Written requests for appeal will be reviewed and adjudicated by the Director of Public Works or his/her designee.

POLICY REVISIONS

The Policy will be reviewed and updated as necessary to ensure consistency with changing local, State, and Federal laws, and guidelines, and changes in data sources, technology, operations, and other relevant considerations. Airport staff will provide a report to the Board of Supervisors regarding implementation of this Policy within six (6) months of its effective date. The most current version of the San Mateo County Airports Operations and Security Systems Privacy Policy can be found on the Airport's webpage at: http://publicworks.smcgov.org/airports.