Board Policy No. 411

Tempo Platform Camera Use Policy

ADOPTED: 9/9/2020	**SUBJECT CATEGORY:** SECTION 400-OPERATIONS
RECENT AMENDMENT: N/A	**SUBSECTION:** BUS RAPID TRANSIT
SEE ALSO: N/A	**CONTROL DEPARTMENT:** GENERAL COUNSEL'S OFFICE

I. PURPOSE

The Tempo Platform Cameras ("Cameras") are intended to improve the safety and protection of AC Transit passengers and employees while on or approaching Tempo platforms, in addition to protecting District property on platforms, including but not limited to Ticket Vending Machines (TVMs), Communications Interface Cabinets (CIC), and Electrical Interface Cabinets (EIC). The implementation of Tempo platform cameras will serve the following key purposes:

- Reassure the public and employees of being able to safely access and wait on Tempo platforms, which will result in greater ridership on the Tempo line.
- Provide evidential support to prosecute offenders for criminal offenses against passengers, employees and District property.
- Provide the District, public and employees a means of redress against property crimes, such as theft or vandalism.

II. PERSONS AFFECTED

Members of the public, District employees, and law enforcement/public safety personnel.

III. DEFINITIONS

"Camera Data Management" means the procedures and processes performed by the Camera IT System Administrator and Camera Application Administrator to ensure that video offloaded from the Camera System follows Tempo Platform Camera Use Policy.

"Law Enforcement/Public Safety Agencies" means law enforcement agencies including Alameda County Sheriff's Office, local police agencies to include Oakland and San Leandro police departments, and other emergency service providers as needed.

"Tempo Platform Facilities" include, but are not limited to, any real property (platforms, canopies, structures), equipment (cameras, TVMs, CICs and EICs), systems, or other interest owned, leased, funded, and/or operated by AC Transit as part of the Tempo Bus Rapid Transit System.

"Tempo Platform Cameras" mean the fixed unit cameras installed on the platform canopy or platform pole. There are four cameras per platform. The fixed unit cameras have a digital zoom feature, but cannot be remotely controlled to move left/right or up/down, and do not have sound capability.

IV. POLICY

A. Roles

"Camera Application Administrator" shall be responsible for (1) reviewing and responding to requests for access to Camera data; (2) ensuring that Camera data only be used for the authorized purposes described in this Policy; and (3) maintaining a record of access to Camera data including documentation of authorized use. This role shall be performed by Protective Services or the General Counsel's Office.

"Camera IT System Administrator" shall be responsible for administering and configuring the camera system hardware and software. The administrator creates, assigns, monitors, and audits security user policies and permissions. The administrator assures proper system operation, validates adherence to security policies and procedures, and installs software updates and patches.

B. Authorized Use

The Cameras shall be used only to advance the purposes identified in this section and Section I above. Use of the Cameras will take place 24 hours a day, 7 days per week, and 365 days per year on all Tempo platforms. The cameras are not intended for use in areas such as off District property or outside the public right-of-way. The Cameras shall not be used to harass, intimidate, or discriminate against any individual or group.

For purposes of this Use Policy, District purposes include use for District criminal investigations and to address criminal activity to protect against harm to persons and property. It shall be permissible for data collected from the cameras to be used for the following public safety and District investigation purposes:

- To assist in identifying and preventing crimes against persons and property;
- To locate missing children, adults, and/or elderly individuals, including in response to Amber Alerts and Silver Alerts;
- To assist in identifying, apprehending, and prosecuting criminal offenders;
- To assist in gathering evidence for internal personnel, civil, and criminal investigations and court actions in accordance with the law;
- To help Law Enforcement and Public Safety Personnel respond to emergency events;
- To assist in investigating and resolving staff and customer complaints and/or issues;
- To comply with statutory disclosure requirements;
- To assist in locating victims, witnesses, suspects, and others associated with a law enforcement investigation;
- To assist in contact tracing as mandated by District protocol or by local health officials; and
- To protect Tempo Facilities.

Administrative functions of Camera data used for criminal enforcement purposes will be managed by AC Transit. Any data obtained from Cameras shall be used and handled pursuant to this use policy.

AC Transit may permit authorized law enforcement agencies to review Camera Data to investigate criminal activity, complaints by customers and employees, and may provide law enforcement agencies with Camera Data when legally required to do so. All other uses not referenced in this document shall be prohibited. Specifically, the District will not share information with U.S. Immigration & Customs Enforcement (ICE) or any agency conducting immigration enforcement or removal operations. Camera technology shall not be used for personal or non-law enforcement purposes and all uses shall adhere to this use policy.

B. Data Collection

Data collected by Camera systems will be limited to still and video images and associated metadata (date, time, location, etc.) within the fixed field of view of the Cameras, including Tempo platforms and the public right-of-way. Data collected will be stored for a maximum of 30 calendar days, except when requested by subpoena, court order, an ongoing investigation, or other lawful request. The District shall not collect or use facial recognition or other biometric data collection software without express approval by the Board of Directors.

C. Data Access Restrictions

Access to Camera Data shall be restricted to the following personnel:

- All persons authorized by the General Manager or his/her designee on a right/need to know basis.
- District personnel involved in the operation, installation and maintenance of the Camera system.
- General Counsel's Office per court order or subpoena or during an investigation.
- Public access as determined under state law.
- Law enforcement personnel pursuant to subpoena in an ongoing law enforcement- initiated investigation.

D. Data Protection

AC Transit's IT Department shall implement security controls necessary to prevent unauthorized access to camera files and metadata, including, but not limited to: authentication, monitoring, auditing, and encryption. IT procedures are designed and intended to prevent corruption of data, data breaches, or unauthorized access to District video camera systems and to provide data protection.

E. Data Retention

Data from the Tempo video camera system will be collected, retained and stored in accordance

with this policy. Data captured from the camera system shall be stored on a secure data storage system for thirty (30) days, at which time it will be overwritten, unless the data is subject to subpoena, court order, statute, or an ongoing investigation, inquiry, or litigation.

F. Public Access

The District shall grant public access to data collected from the Cameras in accordance with applicable law, or as required by court order. Camera Data Management will be administered by District personnel and the General Counsel's office to ensure the security of information and compliance with applicable privacy laws.

Such data will not otherwise be disclosed/released by the District without the consent of the General Counsel's Office. Access to Camera data shall be administered and recorded by the Camera Application Administrator. At a minimum, data access records shall include the following:

- The date and time the information is accessed.
- The data elements used to query the Camera system.
- The username of the person who accesses the information.
- The purpose for accessing the information.

Camera data shall only be used for the authorized purposes described in this Policy, and indicate the authorized use as set forth above.

District employees shall not release any information, including capabilities regarding the District's Camera systems to the public without prior authorization from the General Counsel's Office.

G. Third Party Data Sharing

The District shall maintain robust security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect Camera information from unauthorized access, destruction, use, modification, or disclosure.

The District will retain all ownership rights to the data collected. Third party recipients of Camera data shall not share such data unless permitted by the District in writing and in accordance with this policy, and shall forward any subpoena requests for the data to the District.

H. Auditing and Oversight

The Camera IT System Administrator shall oversee the Camera system and data retention to ensure compliance with this policy. The District will perform periodic audits through its internal auditor to ensure that no misuse of the system or parts of the system occurs. Results of the

audit will be provided to the General Manager and General Counsel.

A log shall be maintained that records access to Camera data as set forth above. The log shall be available for presentation for all required audits, and the District shall prepare an annual report identifying the types of data requests received and responded to, and the intended use of requested data.

V. AUTHORITY

A. Board Authority

The Board of Directors shall periodically review this Policy and approve any amendments as necessary.

B. General Manager's Authority

The General Manager has authority to authorize Camera data access by District personnel and establish internal procedures necessary to carry out the directives of this Policy.

VI. ATTACHMENTS

None.