Citywide Public Safety Surveillance System Policy

I. Background

In order to help ensure public safety and security and to detect, deter, and prevent potential criminal and terrorist activities, the City of New Orleans (City) has established a Citywide Public Safety Surveillance System (System). The System not only supplies critical supplemental assistance to the City's police officers' ongoing security and public safety efforts, but also enhances the collaborative nature of those efforts by leveraging the resources of the private sector and other City agencies. The System is an important part of the City's integrated approach to providing protection for those who work in, live in, and visit New Orleans.

The Office of Homeland Security and Emergency Preparedness as the operating entity establishes policies and procedures to limit the authorized use of the System and to provide for limited access to and proper handling of data.

II. Policy

A. Statement of Purpose

The System is a public safety and counterterrorism tool designed to:

- Facilitate the observation of suspected felonious criminal activity in public areas
- Deter criminal activity
- Reduce public safety response times to critical and life threatening incidents
- Create a common technology to support the integration of new security equipment and technologies
- Monitor critical infrastructure and key resources for pre-operational activity by terrorist organizations or their agents
- Aid in the detection of preparations to conduct terrorist attacks
- Provide a degree of common domain awareness for citywide public safety
- Provide valuable evidence for enforcement of laws and ordinances

B. Access

Access to the System for City employees and contractors shall be granted only for the purposes outlined in this policy and by written authorization from the Director of Homeland Security and Emergency Preparedness. Users will be provided a unique username and password that is not to be shared. Employees of other local, state and federal law enforcement agencies or those requesting access should send a written request from the respective agency head or delegate requesting access, detailing the purpose and need for access. Access to the System is limited to the purposes and uses set forth in this policy.

C. Operation

The System will be operated 24 hours a day, seven days a week, in a professional manner and only in furtherance of legitimate public safety purposes.

As with all City operations, no person shall be targeted or monitored by the System solely because of actual or perceived race, color, religion or creed, age, national origin,

alienage, citizenship status, gender (including gender identity), sexual orientation, disability, marital status, partnership status, military status, or political affiliation or beliefs.

The System shall be used only to monitor public areas and public activities where no legally protected reasonable expectation of privacy exists.

Facial recognition technology is not utilized by the System.

All City-owned cameras that are part of the System shall have accompanying signage or decals, and the City will recommend that signage accompany any privately-owned cameras viewable in the System.

All City-owned cameras that are part of the System shall not be capable of transmitting or recording audio.

The System shall utilize software-based alerting to prompt users to review cameras in close proximity to 911 calls for service. Footage shall only be archived pursuant to the Data Storage guidelines and Data Usage guidelines as set forth in this policy.

Daily, supervisors should review the New Orleans Police Department (NOPD) Major Offense Log and review for video data that may require archiving.

D. Data Storage

All data gathered through the use of the System shall be retained and destroyed in accordance with the applicable State approved record retention schedule, or as otherwise required by law. Pre-archival footage shall be retained for a maximum of 30 days.

Requests to archive footage from the System shall only be allowed on Evidence.com or its subsequent successor platform. Archived footage is stored by NOPD Item number or Public Integrity Bureau Control Number on Evidence.com or its subsequent platform.

In the event that archiving footage on Evidence.com or its subsequent successor platform is not possible, as may be the case for ongoing Public Integrity Bureau investigations or similar internal investigations, the City Attorney shall be consulted for the appropriate course of action to ensure compliance with applicable laws and regulations.

E. Data Usage

Data from the System may be only used by the City of New Orleans in furtherance of the purposes set out in the Statement of Purpose (II.A). In limited circumstances, data from the System may also be used in furtherance of legitimate law enforcement and public safety purposes beyond the scope of those purposes set out in the Statement of Purpose (II.A). Such use is subject to certain restrictions:

- **Incidental Use**: occurs when data from the System is used in furtherance of a purpose set out in the Statement of Purpose (II.A), and the user incidentally notices something useful for a legitimate law enforcement or public safety purpose beyond the scope of those purposes set out in the Statement of Purpose (II.A). For Incidental Use, no additional approval is required.
- **Secondary Use**: occurs when data from the System is intentionally used for a

legitimate law enforcement or public safety purpose beyond the scope of those purposes set out in the Statement of Purpose (II.A). Any decision to make Secondary Use of data from the System must be approved and documented in writing by the Director of Homeland Security and Emergency Preparedness and City Attorney, or their designees approved in writing. Such examples include using video to provide information related to traffic studies, or any civil matter. Any individual seeking to make Secondary Use of data from the System must demonstrate that the data will further a law enforcement or public safety purpose.

F. Data Sharing and Requests

Data shall only be used for law enforcement or public safety purposes; except as required by law, subpoena, or other court process, such data shall not be otherwise disclosed by the City.

G. Safeguarding and Protecting Stored Data

The City shall take all appropriate technological, physical, administrative, procedural, and personnel measures to protect the confidentiality and integrity of all sensitive data, whether in transit or in storage.

Accordingly, the City shall observe the following safeguards regarding access to and use of data:

- Physical access to any area displaying or housing data on the System, is limited to City personnel, authorized contractors, and authorized invited guests. Physical security protections must include locked facilities requiring access cards for entry with an audit trail, and cameras monitoring the equipment and entrances and exits to areas with workstations accessing the System.
- Prior to accessing the System, all users must be authorized by the Director of Homeland Security and Emergency Preparedness. All users shall be briefed on the policies and shall be required to sign an agreement acknowledging these policies.
- Direct access to the System databases or servers is limited to authorized City personnel; the system will use differentiated access and users will only have permissions to access cameras, recording or viewing as their position requires.
- All City personnel with access to the System and databases or servers must complete annual security training, based, in part, on a curriculum covering the proper use and handling of sensitive information.
- The City shall employ data security technologies to protect the integrity of its data from hacking and other risks.
- Access to the System will only occur at designated workstations within the Real Time Crime Center facility. These workstations shall employ data and hardware security features, including preventing use of USB or removable storage devices.
- Audit trails or an equivalent technique shall be used to create an immutable audit log of where and when data is accessed.

H. Accountability
Any violation of these policies may result in immediate revocation of access to the system. Disciplinary action, including suspension and termination of City employees, may be taken as appropriate for violations of the policy.

Nothing in this policy is intended to create any private rights, privileges, benefits or causes of action in law or equity. Rather, these are designed to ensure that the System is properly used based on legally appropriate and relevant law enforcement and public safety considerations and information.

I. Exemptions
Nothing contained herein shall be construed to require the disclosure of records exempted pursuant to La. R.S. 44:3, which exempts from disclosure law enforcement records pertaining to pending or anticipated criminal litigation, criminal intelligence, or threat or vulnerability information relating to terrorist-related activity.

Acknowledgement of Receipt of Policy

I, _____, have received and read the Citywide Public Safety Surveillance Policy. I understand that if I violate this Policy, appropriate administrative and/or disciplinary action may be taken against me.

_____ _____

Date User Signature

_____ _____

Date Director of Homeland Security and Emergency Preparedness or designee