

	ELGIN POLICE DEPARTMENT 151 Douglas Avenue Elgin, Illinois 60120	
Effective Date: 12/21/16	STANDARD OPERATING PROCEDURE	Revised Date: 06/24/24
Chief of Police: 	City-Wide Camera System, 41.9	
Cross Reference: SOP 26.1 Disciplinary Procedures SOP 83.1 Physical Evidence Operations SOP 84.1 Property Evidence Control SOP 111.1 Discriminatory Profiling 625 ILCS 5/2-130		Policy Sections: 41.9.1 Overview of the City-Wide Camera System 41.9.2 License Plate Recognition System Procedures 41.9.3 The Video Management System 41.9.4 Authorized Use of the City-Wide Camera System 41.9.5 Prohibited Use of the City-Wide Camera System 41.9.6 Administration of Hot Lists 41.9.7 Storage and Retrieval of Images 41.9.8 Racial Profiling/Non-Discrimination 41.9.9 Quarterly Inspections/Audits 41.9.10 The Security Through Surveillance Program (STS) 41.9.11 Training Appendix A: Security Through Surveillance Registration Appendix B: COE Surveillance Camera Access Agreement

PURPOSE

The purpose of this policy is to establish procedures regarding the department's use and maintenance of a city-wide camera system.

POLICY STATEMENT

It is the policy of the department to utilize a city-wide camera system as method of enhancing public safety and to improve the department's ability to prevent and detect public safety emergencies, criminal conduct, and identify and apprehend subjects when needed. Various components of the City-Wide Camera System are accessible to authorized city employees for use in support of their respective work areas. The department's use of video camera technology will be conducted in a professional and ethical manner, in compliance with the Fourth Amendment and within accepted legal concepts regarding privacy laws, rules, and regulations, and shall not record or stream live audio. All information and recorded images will be used strictly for law enforcement purposes and will be preserved with utmost integrity and confidentiality consistent with department policy and legal rules governing the handling of evidence and criminal justice records.

DEFINITIONS

Alert: A visual and/or auditory notice that is triggered when a license plate reader system receives a potential "investigative hit" on a license plate.

Automated License Plate Reader (ALPR): An electronic device that is mounted on a law enforcement vehicle or positioned in a stationary location and that is capable of recording data on or taking a photograph of a vehicle or its license plate and comparing the collected data and photographs to existing law enforcement databases for investigative purposes, 625 ILCS 5/2-130.

Automated License Plate Reader System (ALPR): Serves as a component of the City-Wide Camera System that includes equipment consisting of License Plate Cameras, computers, and computer software used to collect and automatically recognize and interpret the characters on a vehicle's license plate. Digital images captured by the cameras are converted into data which is processed through the automated license plate reader system. ALPRs shall only be used for legitimate law enforcement purposes.

City-Wide Camera System: A comprehensive network of cameras deployed across various locations throughout the city. These cameras are utilized by multiple city departments to include law enforcement, Public Works, the Water Department, Parks & Recreation, and other city services to monitor and enhance public safety, crime prevention, and the overall efficiency of city operations.

Custom Hot List: An internally created list of license plates pertaining to stolen vehicles, stolen license plates, wanted person(s) and/or missing persons associated with a criminal offense(s), or a valid law enforcement investigation as described in this policy; the data generated by the custom hot list will be used to identify an investigative hit for a departmental investigation.

Hot List: A multi-agency created and shared list of license plate numbers pertaining to stolen vehicles, stolen license plates, wanted person(s) and/or missing persons from state and national databases; the data generated by the hot list will be used to identify an investigative hit as defined in this policy.

Investigative Hit: A read matched to a license plate that has been registered on the LEADS/NCIC list or a hot list, or a search of license plate reader system data which is an investigative lead or there is reasonable suspicion related to a law enforcement investigation.

IP Address: A numerical label assigned to an electronic device, such as a computer or printer, participating in a computer network that uses the internet protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing.

Law Enforcement Agency Data Systems (LEADS): A shared database for information records which are shared with other law enforcement agencies.

Legal Requirements: Legal requirements or legal rules refer to all applicable federal, state, and local laws and regulations, including the United States Constitution and the Illinois Constitution.

Legitimate Law Enforcement Purpose: Legitimate law enforcement purpose means any of the following:

- a. Traffic law enforcement.
- b. Regulating the use of parking facilities.
- c. For controlling access to secured areas that have clear boundaries, entry only through specific controlled points and limited access.
- d. The purpose of conducting criminal investigations upon an officer's determination that the vehicles or individuals associated with the license plate numbers are relevant and material to an ongoing investigation.
- e. The comparison of captured plate data with databases held by the Secretary of State, by Federal, State of Illinois, other state, and local law enforcement and with license plate numbers that have been manually entered into an ALPR system upon an officer's determination that the vehicles or individuals associated with the license plate numbers are relevant and material to an ongoing criminal or missing person investigation, for the purpose of identifying:
 1. Vehicles that are stolen, or in violation of any registration or inspection requirements.
 2. Persons who are missing or the subject of an arrest warrant, look-out order, traffic citation, or parking citation.
 3. Vehicles that are relevant and material to an ongoing criminal investigation.

License Plate Camera (LPC): A component of the City-Wide Camera System that generates a photographic/video image of a license plate.

National Crime Information Center (NCIC): A computerized index of criminal justice information which is available to federal, state, and local law enforcement agencies.

Pan-Tilt-Zoom Video Cameras (PTZ): A component of the City-Wide Camera System consisting of a pan-tilt-zoom video camera that is capable of remote directional and zoom control providing the ability to monitor large areas with a single security camera.

Read: The capture of digital images, license plates and vehicles with associated meta data such as date, time and GPS coordinates with vehicle images captured by the License Plate Recognition System (LPR).

Search: A manual inquiry into historical license plate reader data containing the dates, times, and locations of individually identifiable motor vehicles.

Security Through Surveillance (STS): A police department initiative that fosters partnerships with businesses and homeowners in effort to prevent and solve crimes through use of technology.

Stationary Cameras: A component of the City-Wide Camera System consisting of fixed position video cameras used for the purpose of monitoring a specific, unchanging location.

Video Management System (VMS): A component of the City-Wide Camera System where authorized city employees have access to video cameras situated at public locations, providing direct and live feed of the video recording. For the purposes of police department use, this is accessible within the Technical Investigations Unit and to officers through use of department issued cell phones and other electronic devices.

PROCEDURES

41.9.1 OVERVIEW OF THE CITY-WIDE CAMERA SYSTEM

- A. The City-Wide Camera System is utilized by authorized employees across various locations within the city. The Technical Investigations Unit is responsible for oversight of the police department's use of the camera system. However, all police department supervisors are responsible for monitoring subordinates to ensure the video camera technology is being utilized in accordance with this policy, training, and legal requirements.
- B. This interconnected camera system enables real-time monitoring and recording of activities taking place in public spaces, including city streets, city parks, and other key areas. The cameras capture video footage, which can be accessed and analyzed by authorized police department personnel for various purposes to include crime detection, investigation, and evidence collection.
- C. Components of the City-Wide Camera System, which encompasses the video management system, are as follows:
 - 1. License Plate Cameras (LPC)/Automated License Plate Recognition System (ALPR).
 - 2. Pan-Tilt-Zoom Video Cameras (PTZ).
 - 3. Stationary Cameras.

41.9.2 LICENSE PLATE RECOGNITION (LPR) SYSTEM PROCEDURES

- A. Only personnel who have received training in its use will be permitted to operate the department's automated license plate reader system. Refer to Section 41.9.11 for more information on training. Each use of the City-Wide Camera System, including any component of the system must be for a legitimate law enforcement purpose and reference a valid department case number or incident number such as the following example: 2024-00012345, Armed Robbery. Each use of the system will be logged.
- B. The information utilized to determine investigative hits are derived from hot lists and custom hot lists as explained in Section 41.9.6.
- C. Upon verification by the officer or the Emergency Communications Division, ALPR investigative hits will constitute reasonable suspicion or probable cause for a traffic stop. Verification includes confirming the status of the vehicle by visually confirming that the license plate matches the image

provided by the ALPR system against the information contained in LEADS.

1. The officer may also request confirmation through the Emergency Communications Division.
 2. Exigent circumstances may exist where the officer is unable to complete the verification process. In such cases, officers shall confirm the status of the associated vehicle as soon as practicable.
- D. Vehicle occupants may not be the subject associated with the license plate. Officers must develop a reasonable belief that the operator/occupant is the person of interest included in a hot list prior to initiating a traffic stop.
- E. In the event of an active law enforcement investigation in the City of Elgin or surrounding jurisdiction, and a full or partial license plate information or vehicle description is available, authorized users shall be allowed to search the LPR system for the suspect vehicle based on the information available to them. A valid department case number or incident number is required for each search. When an officer initiates a search, the system requires the officer to input the report/incident number and incident description.
- F. All entries of license plate information to a custom hot list, as defined in this policy, shall be documented on the corresponding general and/or supplemental report.
- G. All enforcement action taken in response to an investigative hit shall be documented in the corresponding general and/or supplemental report.
- H. Information gathered by the use of ALPR shall be considered confidential and shall not be released unless permitted by law.

41.9. THE VIDEO MANAGEMENT SYSTEM

- A. The Video Management System (VMS) is a component of the City-Wide Camera System and is comprised of images captured by License Plate Cameras (LPC), Automatic License Plate Recognition Systems (ALPR), Pan-Tilt-Zoom Cameras (PTZ) and Stationary Cameras, which are focused on pre-determined public areas. The VMS also has a multipurpose map allowing officers to aggregate different resources in one useable platform.
- B. The VMS is located in the Technical Investigations Unit and accessible to authorized department personnel and via department issued cell phones and other electronic devices.
- C. Through use of the VMS, the police department maintains control over the video cameras and has a direct, live feed of the video recording. The LPC, ALPR, PTZ and Stationary cameras are operational twenty-four hours a day, seven days a week, unless interrupted by power, network, or other mechanical failure or slowdown.
- D. Video cameras will be situated in a manner and location that will maximize the view of public areas for public safety purposes only.
- E. In any location where the view of a video camera would compromise a citizen's privacy expectation, the supervisor of the Technical Investigations Unit shall review the video camera's location to make a recommendation to re-locate the camera.
- F. Devices being used to access VMS footage will not be in a position that enables unauthorized public viewing or viewing by unauthorized personnel. The use of these devices will also adhere to applicable state and federal law.

41.9.4 AUTHORIZED USE OF THE CITY-WIDE CAMERA SYSTEM

- A. Any use of the City-Wide Camera System and/or the associated software is restricted to a legitimate law enforcement purpose. Information obtained from the City-Wide Camera System and/or the associated software shall not be obtained, stored, shared, or used for any other purpose.
- B. Any use of the City-Wide Camera System shall reference a valid case number or incident number. The system may be used for any legitimate law enforcement purpose.
- C. Information obtained from the City-Wide Camera System and/or associated software will only be disseminated to other law enforcement agencies for legitimate law enforcement purposes consistent with this policy. Information may also be disseminated to comply with a court-related request or subpoena, or pursuant to a valid Freedom of Information Act (FOIA) request. Unless authorized by law, such information shall not be sold, shared, or transferred to a third party.
- D. Misuse or abuse of the City-Wide Camera System and/or the associated software will result in discipline. Refer to Standard Operating Procedures 26.1 Disciplinary Procedures for information on the discipline process.

41.9.5 PROHIBITED USE OF THE CITY-WIDE CAMERA SYSTEM

- A. Prohibited uses of the City-Wide Camera System are as follows:
 - 1. For any purposes other than a valid and legitimate law enforcement purpose.
 - 2. To harass or intimidate any person or group.
 - 3. Solely on the basis of a protected characteristic. Protected characteristics that are an impermissible basis for LPR use include: a person's race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law. Refer to Section 41.9.8 for more information.
 - 4. To track vehicles for any reason other than for a legitimate law enforcement purpose.
 - 5. For the purpose or known infringement of a person's First Amendment rights such as collecting information about a person's lawful associations, lawful political and religious affiliations, or activities, etc.
 - 6. In any manner that would violate any applicable law, including local, state, and federal laws and the United States and Illinois Constitutions.
 - 7. To use an LPC or ALPR to record or observe information not related to a license plate in public view.
 - 8. For personal use or on behalf of another individual.
 - 9. For the purpose of or in conjunction with the use of facial recognition software and/or hardware.
 - 10. The department shall not sell, share, allow access to or transfer ALPR information to any state or local jurisdiction for the purpose of investigating or enforcing a law that:
 - 1. Denies or interferes with a person's right to choose or obtain reproductive health care services or any lawful healthcare services.
 - 2. Permits the detention or investigation of a person based on the person's immigration status.

11. Any ALPR user in this state, including any law enforcement agency, shall not share LPR information with an out-of-state law enforcement agency without first obtaining a written declaration from the out-of-state agency that it expressly affirms that ALPR information shall not be used in a manner that violates number 10 as listed above.
 1. If a written declaration of affirmation is not executed, the law enforcement agency shall not share the LPR information with the out-of-state law enforcement agency as stated in 625 ILCS 5/2-130.

41.9.6 ADMINISTRATION OF HOT LISTS

- A. The department will oversee access to the ALPR system. Each officer who is provided access will be given a unique User ID and password. The system will not have generic or guest User IDs. The department will, from time to time, audit the list and remove inactive users from the ALPR system.
- B. As defined in this policy, a hot list is an external list of data contained in state and national databases for law enforcement use.
 1. The content of a hot list is obtained via a secure file transfer from the State of Illinois.
 2. The hot list file is updated via an automated task several times daily. Should this task fail, an automated email will be sent to the Systems Technology Unit Sergeant of such failure.
 3. The hot list contains stolen vehicles, stolen license plates, wanted persons and missing persons from the State of Illinois.
 4. At the conclusion of each calendar year, the department shall prepare an annual report to the Chief of Police regarding the efficacy of the City-Wide Camera System, specifically identifying the cost of the LPR system and the usefulness and efficiency of the LPR system in leading to arrests and guilty pleas or verdicts. The report shall be made public within 30 days of submission to the Chief of Police. The report will also be made publicly available via the department's transparency hub located at:
<https://epdopendata-cityofelgin.hub.arcgis.com/>
- C. As defined in this policy, a custom hot list is an internally created list of license plates pertaining to stolen vehicles, stolen license plates, wanted person(s) and/or missing persons associated with a criminal offense(s) or a valid law enforcement investigation.
 1. License plates may be entered manually for inclusion on a custom hot list where reasonable suspicion exists that a vehicle is involved in an active law enforcement investigation.
 - a. Prior to manually entering vehicle information to a custom hot list, using the department authorized form, officers shall receive approval from a Sergeant or higher rank, or in their absence, their designee for the submission. [View the Approval to Create a Custom Hot List](#)
 - b. Partial license plate information will not be added to the custom hot list at any time or for any reason.
 - c. In the event of an emergency situation, where an entry to a custom hot list must be created without delay, an Emergency Communications Division supervisor will be authorized to immediately input the information into a custom hot list upon approval of a Sergeant or higher rank, or in their absence, their designee. If approval is given, the information will remain in the respective custom hot list according to the established guidelines.

2. The ALPR system automatically stops collecting data on license plates after ninety (90) days, unless the officer has obtained authorization for an extension by a Lieutenant or higher rank, or in their absence, their designee. Refer to Section 41.9.9 to view information on the Quarterly Inspection of the City-Wide Camera System.
3. Officers who determine that a license plate number should no longer be located on a custom hot list will be responsible for notifying the Sergeant assigned to the Technical Investigations Unit for removal of the information when it is no longer needed on a respective custom hot list.
4. Custom hot lists or their contents will not be shared or disseminated outside of this department without prior approval of the Chief of Police or designee.

41.9.7 STORAGE AND RETRIEVAL OF IMAGES

- A. Footage captured by the City-Wide Camera System will be automatically recorded on site at the Elgin Police Department. Video cameras may be recording continuously or on motion activation depending on the specific circumstances and storage considerations. The storage retention periods are specified below:
 1. Off-site city owned cameras, under the authority of the police department: 30 days
 2. Off-site city owned cameras, under the authority of an external city department, as determined by that department's policy
 3. Internal police department cameras 90 days
 4. Police Holding Facility: 90 days
 5. Property Evidence Room and area of the Prescription Medication Disposal Box: 90 days
- B. All LPR data will be stored on a secure server maintained by the LPR software vendor. Investigative hits may be imported into the department's approved records management system. Information will not be shared with outside entities except in accordance with the procedures set forth in this policy.
 1. "Reads" such as the capture of digital images, license plates and vehicles that are not associated with an ongoing investigation shall be maintained for a period of thirty (30) days.
 2. "Investigative Hits" such as a license plate that is connected to a hot list or law enforcement investigation shall be maintained for a period of thirty (30) days.
- C. Video footage that is not retained for evidentiary purposes or based upon public safety necessity or pursuant to a court order shall not be reproduced or distributed without the approval of the supervisor assigned to the Technical Investigations Unit.
- D. Video footage that has been exported to a recording a medium for evidentiary or public safety purposes shall be stored in a secure area and placed into evidence pursuant to the procedures outlined in Standard Operating Procedures 83.1 Physical Evidence Operations and 84.1 Property Evidence Control.
- E. All requests for city-wide camera video shall be directed to the Technical Investigations Unit or the Records Division.

41.9.8 RACIAL PROFILING/NON-DISCRIMINATION

- A. Persons in view of the video camera system will not be selected based solely on their race, ethnicity, or gender. This practice is consistent with Standard Operating Procedure 111.1, Discriminatory Profiling which affirms the department's commitment to unbiased, equitable treatment of all persons while enforcing the law and providing police services.
- B. Employees will make specific observations of individuals based on articulable reasonable suspicion

that the person may be or may have been involved in criminal activity or as a result of criminal activity within the area of the video camera's viewing parameters.

41.9.9 QUARTERLY INSPECTIONS/AUDITS

The Sergeant assigned to the Technical Investigations Unit, or designee, shall complete a documented quarterly inspection/audit using the authorized template. A copy of the inspection/audit shall be forwarded through the chain of command to the Commander for Investigations. The inspection shall include the following:

- A. Inspection of the Video Management System. Discrepancies, concerns, and areas requiring additional training or corrective action shall be included in the inspection.
- B. Quarterly Audit:
 - 1. Quarterly, the Sergeant assigned to the Technical Investigations Unit or their designee will audit the custom hot list to ensure the ALPR system is no longer collecting data on any license plate in the system over 90 days unless an extension was authorized as specified in Section 41.9.6.
 - 2. Quarterly, the Sergeant assigned to the Technical Investigations Unit or their designee will conduct a randomized audit of all LPR searches.
 - 3. Audit results shall be included in the annual report to the Chief of Police. Any suspected violations of this order discovered during an audit, or any other time, will be reviewed by the Chief of Police for a Professional Standards and/or disciplinary investigation.
- C. The Quarterly Inspection of the City-Wide Camera System is accessible via PowerDMS and is available through use of the following link: [View the Quarterly Inspection of the City-Wide Camera System](#)



41.9.10 THE SECURITY THROUGH SURVEILLANCE PROGRAM (STS)

- A. The Technical Investigations Unit oversees the Security Through Surveillance Program (STS) Program which is comprised of businesses, residents and public entities who voluntarily register their surveillance camera system with the police department and will follow the permissions established between the entities. If a crime occurs in the vicinity of a residence, business or public entity with a registered camera, the police department may contact the registrants and request a copy of their footage for evidence or investigative leads.
- B. Privately owned cameras can voluntarily be registered with the police department through the STS program electronically via the police department's website or using the Security Through Surveillance Registration Form; refer to Appendix A.
- C. Registrants of this program are responsible for purchasing the camera system(s) of their choice. The Technical Investigations Unit may offer a no cost specialized training program for those who wish to learn how to effectively utilize their surveillance cameras. Training may consist of camera selection, placement, footage storage options, and the type of assistance provided by the police department.
- D. Registrants of privately owned cameras advise the police department of the location of their cameras in the event these cameras may assist with investigations. If registrants wish to grant IP address access to privately owned cameras for live viewing over the internet or through the RIC, registrants must complete the city's Surveillance Camera Access Agreement; refer to Appendix B to view the agreement.

41.9.11 TRAINING

- A. The Sergeant assigned to the Technical Investigations Unit is responsible for ensuring all employees assigned to the unit are trained in the use of the VMS and all components thereof, including the LPR system and provided with specialized training to ensure the proper retrieval of footage from an array of video camera systems, capabilities of the video cameras, proper operation of video camera equipment. Training must include permissible uses of the VMS, including the LPC/ALPR system, the verification process for law enforcement alerts, security, and privacy protections on the use of the technology, responsibilities, and obligations under applicable federal, state, or local law and policy when using the VMS, mechanisms for reporting violations of ALPR policy, and the impact and sanctions for non-permitted uses and/or violations of this LPR policy. Training may also consist of reviewing department protocol, the First and Fourth Amendments, and consent to search issues.
- B. The Technical Investigations Unit is responsible for providing training on the ALPR System.
 - 1. All users of the ALPR system shall receive training prior to being given access to the ALPR system.
 - 2. All users of the ALPR system shall be LEADS certified consistent with their level of access to LEADS prior to being given access to the ALPR system.
 - 3. Training will include permissible uses of the ALPR system, the verification process for law enforcement alerts, security, and privacy protections on the use of the technology, responsibilities, and obligations under applicable federal, state, or local law and policy when using the ALPR system, and the impact and sanctions for non-permitted uses and/or violations of this ALPR policy.
- C. All training documents shall be forwarded to the Training Division for inclusion in the officer's training file.

APPENDIX A: SECURITY THROUGH SURVEILLANCE REGISTRATION FORM

	ELGIN POLICE DEPARTMENT <i>Security Through Surveillance</i>		
Business name	<input style="width: 250px;" type="text"/>	Business TX	<input style="width: 150px;" type="text"/>
Business address	<input style="width: 250px;" type="text"/>	Business fax	<input style="width: 150px;" type="text"/>
Business hours	Sun <input style="width: 80px;" type="text"/> Mon <input style="width: 80px;" type="text"/> Tues <input style="width: 80px;" type="text"/> Weds <input style="width: 80px;" type="text"/> Thus <input style="width: 80px;" type="text"/> Fri <input style="width: 80px;" type="text"/> Sat <input style="width: 80px;" type="text"/>		
Business contact number 1			
Contact's name	<input style="width: 250px;" type="text"/>	Title/position	<input style="width: 150px;" type="text"/>
Contact's TX	<input style="width: 100px;" type="text"/>	Alternate TX	<input style="width: 100px;" type="text"/>
E-mail address	<input style="width: 250px;" type="text"/>		
Alternative contact			
Contact's name	<input style="width: 250px;" type="text"/>	Title/position	<input style="width: 150px;" type="text"/>
Contact's TX	<input style="width: 100px;" type="text"/>	Alternate TX	<input style="width: 100px;" type="text"/>
E-mail address	<input style="width: 250px;" type="text"/>		
Camera Information, include the make, model, and number of cameras			
Length of time the video is stored	<input style="width: 150px;" type="text"/>		
Is there an IP access to the camera(s)?	<input type="checkbox"/> Yes <input type="checkbox"/> No If yes, list the IP address <input style="width: 150px;" type="text"/>		
Security company that installed the camera(s)	<input style="width: 250px;" type="text"/>		
TX	<input style="width: 150px;" type="text"/>		
151 Douglas Avenue Elgin, IL 60120 Phone: (847) 289-2500 Fax: (847) 289-2750 Effective 02/2/13			

APPENDIX B: CITY OF ELGIN SURVEILLANCE CAMERA ACCESS AGREEMENT

Page 1 only

SURVEILLANCE CAMERA ACCESS AGREEMENT

THIS AGREEMENT is hereby made and entered into this ____ day of _____, 20____, by and between the City of Elgin, an Illinois municipal corporation (hereinafter referred to as "City") and [INSERT LEGAL NAME OF PROPERTY OWNER, OCCUPANT OR OTHER PARTY IN CONTROL OF THE PREMISES], a(n) [INSERT LEGAL STATUS OF ENTITY AND ASSOCIATED STATE (e.g., a Delaware corporation, an Illinois not-for-profit corporation, etc.)] (hereinafter referred to as "Company").

WHEREAS, Company owns, occupies or operates a building located at [INSERT STREET ADDRESS OF BUSINESS], Elgin, Illinois (the "Premises"); and

WHEREAS, Company owns and/or controls a system of surveillance cameras (the "System") utilized for Company's own purposes, which enable visual monitoring of the Premises, and which may include both the interior and the exterior areas of the Premises; and

WHEREAS, Company desires to provide the City with access to real-time, visual image data collected by the System for law enforcement purposes; and

WHEREAS, the prevention, detection and prosecution of crime is in the public interest; and

WHEREAS, the City has determined that the ability to access and view the visual image data collected by the Company's System (the "Visual Image Data") will further the City's interest in preventing, detecting and prosecuting crime within the City of Elgin.

NOW, THEREFORE, in consideration of the mutual promises and covenants contained herein, the sufficiency of which is hereby mutually acknowledged, the parties hereto hereby agree as follows:

1. The above recitals are incorporated herein and made a part hereof as if fully recited herein.
2. Subject to the terms and conditions of this Agreement, Company hereby grants to City, its officers, representatives, agents and employees the right of real-time access to view the Visual Image Data via a remote Internet Protocol (IP) address, at no cost to the City, for the Term of this Agreement and any future extensions of this Agreement. The City shall also have the right to record or preserve the Visual Image Data for purposes consistent with the terms and provisions of this Agreement, in the City's sole discretion. The City's access to the Visual Image Data is intended for law enforcement purposes. City acknowledges and agrees that the Visual Image Data shall not be used for commercial or for-profit purposes of any kind.
3. Company shall provide City with such specifications regarding the System as are necessary for the City to access the Visual Image Data. In addition, Company shall disclose any material changes to Company's System that would affect City's ability to