	ADMINISTRATIVE ORDER	Approved By: City Manager	No. Effective Date: 19 May 2026 Updated Date: N/A
Subject: PHYSICAL SECURITY SYSTEM – CCTV, ACCESS CONTROL & VIDEO RETRIEVAL POLICY			

INTRODUCTION

The City of Highland Park ("City/City's") implemented a comprehensive physical security system to enhance the safety of employees, residents, and visitors; protect City facilities and assets; and support operational needs. This system includes, but is not limited to, closed-circuit television (CCTV) cameras, secure door access controls, card/fob credentialing, presence monitoring, cloud-based management software, and associated data storage.

This policy establishes the standards under which the system will be used and administered. While the system is intended to strengthen security and support City functions, improper or unauthorized use may undermine privacy expectations, compromise investigatory processes, expose the City to legal liability, and erode public trust. To minimize such risks, the policy defines the appropriate uses, restrictions, responsibilities, and retention requirements associated with the physical security system.

DEFINITIONS

1. **"Physical Security System" ("System")**
   The integrated set of CCTV cameras, access control devices, badge readers, cloud-based management software, logs, and associated data storage owned or operated by the City.
2. **"Video Records / CCTV Footage"**
   Any still image, recording, video clip, or archived data generated by the System.
3. **"Access Logs"**
   Digital records documenting entry attempts, door activity, credential use, system alerts, or administrative actions.
4. **"System Administrator"**
   The City Manager and any designee authorized by the City Manager to act on their behalf.

5. **“Authorized User”**
   Individuals approved to access, retrieve, review, or administer portions of the System, including the City IT Manager, Facilities Supervisor, Deputy Director of Public Works, and Director of Public Works or other personnel designated in writing by the City Manager.
6. **“User”**
   Any City employee, elected or appointed official, contractor, volunteer, or individual authorized to access a City facility that is equipped with System components.
7. **“Public Record”**
   Any video record or access log that meets the definition of a public record under the Illinois Freedom of Information Act (FOIA) or the Illinois Local Records Act.

MANAGEMENT AND ADMINISTRATION

The Physical Security System is maintained and administered by the Information Technology division in coordination with the Public Works Facilities Section. The City retains the right to monitor, record, review, and retrieve System data at any time for legitimate governmental purposes, consistent with this Administrative Order.

Unauthorized access, misuse, or tampering with the System or its components may result in disciplinary action up to and including termination.

There should be **no presumption of privacy** in areas monitored by cameras or controlled by access systems. Cameras will not be placed in locations where employees or the public have a reasonable expectation of privacy (e.g., restrooms, locker rooms).

NO PRESUMPTION OF PRIVACY; RIGHT TO MONITOR

The City reserves the right but not the duty to access, review, retrieve, preserve, and disclose System data at any time and without prior notice to any User, including in the following circumstances:

- Suspected violation of any City policy or Administrative Order;
- Suspected criminal activity or threat to safety;
- Compliance with a lawful request, subpoena, FOIA request, or court order;
- Employee unavailability (e.g., illness, separation, leave);
- When otherwise in the City’s best interest.

Video Records and Access Logs may be disclosed to law enforcement, the City’s Legal Counsel, Human Resources, or other authorized individuals as necessary for City business.

PERMITTED USES OF THE SYSTEM

The System is to be used primarily for:

1. **Security and Public Safety**
    - Deterring and investigating unauthorized access, theft, vandalism, or threats to persons or property.
    - Supporting Police Department criminal investigations.
2. **Facility and Operational Management**
    - Monitoring infrastructure failures, access issues, maintenance needs, and after-hours building activity.
3. **Verification and Incident Response**
    - Confirming events related to workplace injuries and accidents, safety hazards, or emergencies.
4. **Human Resources Investigations**
    - Only with prior consultation and authorization from Human Resources for allegations involving misconduct, tardiness patterns affecting operations, or workplace policy violations.

Prohibited Uses
The System shall not be used for:

- Routine monitoring of employee productivity or performance;
- Personal purposes;
- Surveillance unrelated to legitimate City business;
- Any discriminatory, harassing, retaliatory, or otherwise inappropriate purpose.

Privacy and Operational Limitations

1. Cameras will not be used in private areas, including restrooms or locker rooms.
2. Live monitoring is not permitted except during emergencies, active incidents, or by Public Safety personnel performing official duties.
3. Live monitoring is permitted in specifically authorized locations in the City (City Hall, Water Plant, Fire Stations, Police Department/Dispatch)
4. Facial recognition, behavioral analytics, or similar advanced features may not be activated without written authorization from the City Manager and review by Legal.
5. Access credentials (cards, fobs, digital keys) are City property and must be returned upon separation.

VIDEO RETRIEVAL AND REVIEW PROTOCOLS

A. Criminal or Suspected Criminal Activity

- Employees or residents alleging a crime **must file a police report**.
- The Police Department will determine whether video retrieval is necessary.
- Video will be retrieved **only at the direction of the Police Department** for law enforcement investigations.
- The City Facilities Supervisor, IT Manager, or staff member (at the direction of the City Manager) are authorized to retrieve video.

B. Human Resources and Personnel Matters

- Requests must be initiated with Human Resources.
- HR will evaluate whether the circumstances justify video review.
- Upon HR approval, authorized personnel (IT Manager, Facilities Supervisor, or Director of Public Works) may retrieve the footage.

C. Operational or Facility Management Requests

Examples include malfunctioning doors, misplaced keys/fobs, or after-hours access questions.
Requests must be submitted to the Facilities Supervisor and must include:

- Purpose of the request;
- Date/time range;
- Location(s) involved.

D. Verification and Incident Response

Requests related to workplace injuries, accidents, safety hazards, or emergencies may be initiated by a Department Director.

Requests must be submitted to the Facilities Supervisor and must include:

- Purpose of the request;
- Date/time range;
- Location(s) involved;
- A brief description of the incident or safety concern.

Upon receipt, the Facilities Supervisor may coordinate with the IT Manager to retrieve the relevant footage. If the incident involves or may give rise to a personnel matter, HR must be notified prior to retrieval and the request will be processed under Section B.

Footage retrieved under this section may be shared with the affected employee's Department Director, Human Resources, and/or Legal Counsel as appropriate to the circumstances.

FOIA COMPLIANCE

Video Records and Access Logs may be subject to the Illinois Freedom of Information Act.
However, exemptions may apply, including but not limited to:

- Records relating to building security systems;
- Ongoing police investigations;
- Private or personal information;
- Juvenile information;
- Infrastructure vulnerability data;
- Images where disclosure would create a safety or privacy risk.

Procedure for FOIA Requests

- All FOIA requests must be processed by the City's FOIA Officer.
- IT, Facilities, and department staff **shall not release footage directly** to requestors.
- The FOIA Officer will coordinate with Legal, IT, and relevant departments to determine whether a record is exempt, must be redacted, or may be released.

DATA RETENTION

In accordance with the City's adopted retention practices:

- **Police Department:** Video retained for 90 days
- **All Other City Facilities:** Video retained for 30 days

Retention may be extended **only** when:

- A Police, Legal, or HR investigation requires preservation;
- A litigation hold is issued;
- A FOIA request, subpoena, or court order requires retention beyond standard schedules.

SYSTEM INTEGRITY AND AUDIT REQUIREMENTS

The City will maintain records of:

- Video retrieval requests;
- Requestor identity;
- Purpose of retrieval;
- Timeframes and locations accessed;

- Recipients of retrieved video.

Records are maintained in the Verkada (command.verakda.com) Online Portal

RESPONSIBILITIES

Information Technology Division

- Administer system software and storage online service;

Facilities Section

- Oversee installation, maintenance, and positioning of cameras and access devices.
- Manage user permissions.
- Maintain security, logs, retention, and infrastructure.

Police Department

- Lead and authorize all criminal investigations requiring video retrieval.

Human Resources

- Review and approve any video request related to personnel matters.

Department Directors

- Ensure staff awareness of policy.
- Report incidents in a timely manner.
- Coordinate with HR or Police when appropriate.

REPORTING MISUSE

Employees are responsible for reporting violations of this policy to their immediate supervisor, Human Resources, or the City Manager's Office.

DISCIPLINARY ACTION

Failure to comply with this policy may result in disciplinary action up to and including termination. Misuse may also result in legal consequences where applicable.

INTERPRETATION

Questions regarding interpretation of this Administrative Order shall be submitted to the City Manager's Office.