POLICY		**CAT-SUB-####**	
CCTV (Closed-Circuit Television) Video Surveillance Policy		**Category** MUN - Municipal Services	**Sub-category** FAC - Facility
Approval Type COUNCIL	**Department/Division** Infrastructure Services	**Author and Position** Director, Facilities Management	
Date Approved Click here to enter a date.	**Last Reviewed/Amended** Click here to enter a date.	**Next Review Date** Click here to enter a date.	

Related Policies or Procedures

- *The Municipal Freedom of Information and Protection of Privacy Act*
- *Municipal Act, 2001*
- *2011-121 Records Retention By-law*
- *Access & Privacy Policy*
- *Record Creation Guidelines*
- *Authorized Destruction Procedures*
- *Information Management Policy*
- *The Information and Privacy Commission of Ontario (the IPC) "Guidelines for Video Surveillance Cameras in Public Places", October 2015*
- *CCTV Systems Operational Procedure*

---

1. Policy Purpose

The purpose of this policy is to establish clear and consistent guidelines for the deployment and use of CCTV (Closed-Circuit Television) Video Surveillance Systems across City of Kitchener facilities. CCTV systems are implemented to enhance the safety and security of municipal properties by protecting the physical site, individuals who access and or work within these spaces, and safeguard the assets contained within them. The City is committed to using video surveillance in a responsible and transparent manner, and solely for the purpose of promoting public safety and protecting municipal assets—while upholding the privacy rights of all individuals.

This policy outlines the standards and procedures governing the installation, operation, recording, and management of video surveillance equipment to ensure that all surveillance activities align with applicable legislative and regulatory requirements, including the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*, and the *Information and Privacy Commissioner of Ontario (IPC)*.

This policy defines the responsibilities and requirements related to:

- Installation of video surveillance systems
- Day-to-day operation and oversight
- Use and handling of recorded information
- Custody, control, and authorized access to surveillance records

2. Policy Scope

This policy applies to all CCTV (Closed-Circuit Television) Video Surveillance Systems installed within City of Kitchener facilities and governs their use by City employees, visitors, and tenants. It establishes the framework for the responsible management of surveillance technology to ensure safety, security, and compliance with applicable legislation. This policy does not apply to:

- audio recording of Council or Committee meetings,
- installation and operation of surveillance equipment by third parties, and
- CCTV equipment installations for the purposes of construction site monitoring.

Application

☒ Employees *(Indicate below which categories apply: All employees, Permanent full-time, Temporary full-time, Continuous part-time, Casual, Probationary, Student, Management, Non-union)*

- All Employees

☐ Unions *(Indicate below which categories apply: All Unions, CUPE 68 Civic, CUPE 68 Mechanics, CUPE 791, IATSE, IBEW, KPFFA)*

- Click or tap here to enter text.

☐ Council

☐ Specified Positions*:* Click or tap here to enter text.

☒ Other: Local Boards and Advisory Committees

3. Policy Content

3.1 Video Surveillance Systems

Equipment

All video surveillance equipment used across City of Kitchener facilities shall centrally monitored at the Kitchener City Hall at the Corporate Security Operation Centre (200 King St. W), or in secure designated areas within individual facilities equipped with surveillance systems.

Video surveillance operates continuously 24 hours a day, 7 days a week—across all applicable locations.

Security Protocols: Reception equipment shall be housed in strictly controlled access areas. Access to these areas and the equipment is limited to authorized personnel only, including the Corporate Security Management and staff, and other authorized individuals. Video monitors shall be positioned to prevent public viewing at all times, ensuring the confidentiality and integrity of surveillance footage.

Requests for Installing Video Surveillance Equipment

All requests to install video surveillance equipment shall be submitted to the Manager of Corporate Security for review. Each request must be based on substantiated concerns such as documented criminal activity, elevated safety risks, or a demonstrated need for crime prevention, to ensure that surveillance is deployed strategically and in alignment with the City's public safety priorities.

A Privacy Impact Assessment (PIA) is required for every CCTV surveillance camera request in accordance with the city's Access and Privacy Policy. A PIA evaluates potential privacy implications, verifies that camera placement respects individual privacy, and confirms that appropriate public signage is posted at the surveillance site, ensuring transparency, accountability, and adherence to privacy standards in all surveillance initiatives.

3.2 Installation and Operation of Video Surveillance Equipment – General Guidelines

1. Camera Placement

Camera placement shall be assessed on a case-by-case basis to determine the effects the equipment may have on personal privacy. The City shall take all reasonable steps to mitigate any adverse effects. No camera will be placed such that it views into an area where individuals have a high expectation of privacy, such as washrooms, change rooms or private buildings.

2. Signage

The City must ensure that the public is notified of the legal authority for the collection of personal information in all its City owned and/or leased facilities and properties where video surveillance is present. Signage shall be installed in a clearly visible location at all Facilities which are subject to surveillance.
Facilities Management shall be responsible for the procurement, installation, and associated costs of all interior and exterior surveillance notification signage, including ensuring signage is properly placed on public entrance doors and around the perimeter of applicable locations. Signage must comply with approved standards for language, imagery, and sizing to maintain consistency and visibility in accordance with IPC guidance.

3. Approval

Locations for CCTV systems and cameras, and all signage require the approval of the Director of Facilities Management. Legislated Services shall be responsible for determining suitable location(s) where mandatory public notice signage will be installed, ensuring that the public has reasonable and adequate warning that surveillance is or may be in operation prior to entering any area that is within the video surveillance viewing area in accordance with the following notification requirements under MFIPPA;

- the legal authority for the collection,
- the reason for the collection,
- how the information will be used,
- contact for more information.

3.3 Use of Requested Information

The information collected through video surveillance must only be used for the following types of incidents:

- to assess the effectiveness of safety and security measures taken at a particular City facility,
- to investigate an incident involving the safety or security of people, and City facilities or assets,
- to provide law enforcement agencies with evidence related to an incident under police investigation,
- to provide evidence as required to protect the City's legal rights,
- to respond to a FOI (freedom of information) Requests under MFIPPA,
- to investigate an incident or allegation of serious employee misconduct,
- to review and analyse an incident resulting in an insurance claim filed against the city.

Access to video surveillance footage shall be limited to authorized personnel. Reviews of recorded footage are permitted only under circumstances involving a reported or observed incident, or for the purpose of investigating potential criminal activity.

Real-time monitoring is restricted to City of Kitchener Corporate Security personnel and a limited number of designated individuals. In cases involving an incident or allegation of serious employee misconduct, authorization from the Director of Human Resources is required prior to any review.

Authorized Corporate Security staff must maintain system login credentials and access logs related to surveillance footage.

3.4 Access, and Disclosure of Records

A) Formal Access Requests (FOI)

Requests for access to surveillance images and video footage shall be directed to the Access and Privacy Specialist at accessandprivacy@kitchener.ca.

Access requests must include sufficient detail to support processing and shall meet the following requirements:

- Be submitted in writing and/or on the prescribed form,
- Include the required application fee,
- Specify the date, time, and description of the event,
- Identify the relevant video surveillance location.

Upon receipt of an access request, the Access and Privacy Specialist shall coordinate with the Manager of Corporate Security and authorized security personnel to retrieve the relevant surveillance footage. The footage will be transferred to the Access and Privacy Specialist using a secure drive or stored within a secure digital folder to ensure data protection.

B) Law Enforcement Investigation Requests

Law enforcement investigation requests shall be processed directly by the Corporate Security team and must include sufficient detail to support processing and shall meet the following requirements:

- be submitted in writing and/or on the prescribed request form,
- Include the relevant incident or investigation number,
- Provide the officer's badge number,
- Specify the date, time, and a brief description of the event,
- Identify the applicable video surveillance location.

Corporate Security staff shall retrieve the relevant footage and ensure secure transfer to the requesting agency.

All hard drives and other storage devices not actively in use must be stored in a locked receptacle located within a controlled-access area. Access to these devices is restricted to authorized personnel only. A detailed log of all access and usage of recorded material must be maintained by the Corporate Security to support a complete audit trail.

Where access to information requests are granted, in accordance with this policy and applicable legislation, any images containing identifiable individuals shall be redacted, severed or obscured to protect personal privacy. A qualified external service provider may be retained to carry out the redaction.

3.5 Data Retention and Disposal

<u>Retention</u>

General Retention Period

- Video surveillance footage that has not been accessed for law enforcement or public safety purposes shall be retained for 30 calendar days.

Retention for Law Enforcement or Public Safety Use

- If footage is accessed for law enforcement or public safety purposes, it shall be retained for:
  - one year from its last use, or
  - until all related legal proceedings and appeals have been fully resolved.

- Such footage must be stored electronically on the corporate IT network.

<u>Disposal</u>

Automatic Overwrite of Not Accessed NVR Recordings

Video surveillance footage stored on the hard drive that has not been accessed for access requests, law enforcement, or public safety purposes must be automatically overwritten on

or before the end of the 30-day retention period.

Erasure must be conducted in a manner that ensures personal information cannot be reconstructed or retrieved.

Footage that is saved or downloaded for investigative or operational purposes shall be classified as an official City record. Prior to destruction, the City's Authorized Destruction Form shall be completed in accordance with records management procedures and applicable legislation.

3.6 Footage Accessed for Law Enforcement or Public Safety Purposes

Footage disclosed to a law enforcement agency by Corporate Security staff shall be managed in accordance with established internal procedures. All transfers of surveillance material must be documented and handled securely.

Footage saved to a secure drive folder for law enforcement or public safety purposes must be retained only as long as necessary and must be deleted under one of the following conditions:

- on or before the end of the applicable retention period, as defined by City policy and legislative requirements; or
- once all related proceedings, investigations, and appeals have been fully concluded.

Digital copies (e.g., CDs, flash drives) released to external authorities are considered to be in custody of the receiving organization. The external agency is responsible for ensuring secure storage and appropriate destruction of the material in accordance with their own policies and legal obligations.

3.7 Use of Corporate Security Flash Drives

In circumstances where CD copying is unavailable, Corporate Security flash drives may be used to transfer surveillance footage. The following procedures shall be followed to ensure secure handling and compliance with retention standards:

- flash drives shall be securely wiped immediately following successful transfer and return,
- transferred footage shall be saved to a designated secure drive for the duration of the applicable retention period,
- any digital copies retained by Corporate Security staff (e.g., CDs, flash drives) must be securely disposed of within the retention period using approved destruction methods, including:
  - shredding
  - incineration
  - magnetic erasure
  - physical destruction.

4. Annual Audit and Evaluation

An Annual Post-Installation Review must be conducted by the Manager/ Supervisor of Corporate Security using the designated form and reviewed by the Access and Privacy Specialist to evaluate the effectiveness, necessity, and procedural integrity of the surveillance program.

The annual evaluation shall confirm the following:

- *Justification of Surveillance Use*

Surveillance operations remain necessary and appropriate; consideration will be given to whether usage should be modified, restricted, or discontinued.

- *Logging of Requests*

All access and disclosure requests related to surveillance footage have been properly documented and monitored.

- *Signage Compliance*

All surveillance signage is correctly placed, securely mounted, and clearly visible to the public.

- *Review of Camera Placement*

Camera locations have been reviewed to account for changes in the surrounding area, ensuring they do not inadvertently capture spaces where individuals may have a heightened expectation of privacy.

If any camera is deemed high risk, Corporate Security and the Access and Privacy Specialist must be notified to support timely adjustments to camera placement and maintain compliance with privacy standards.

- *Security of Requested Footage*

Surveillance images subject to access or disclosure requests are securely stored and protected against unauthorized access or alteration.

- *Proper Disposal of Unrequested Footage*

Surveillance images not subject to a request, are destroyed in accordance with the city's Records Retention and Information Management Policy and Procedure, ensuring that personal information cannot be reconstructed or retrieved.

5. Roles and Responsibilities

To ensure the effective and compliant operation of video surveillance systems, the following roles and responsibilities are established:

Manager/Supervisor of Corporate Security

The Manager/Supervisor of Corporate Security is accountable for:

- developing and maintaining procedures for the installation, operation, and use of video surveillance systems in City facilities,
- managing the custody, control, access, and retention of all Recordings and Accessed Recordings,
- reviewing and approving proposed changes to existing systems and evaluating new system proposals for compliance with this policy, applicable City by-laws, and legislation,
- establishing and overseeing training programs related to system operation and privacy responsibilities,
- maintaining up-to-date lists of designated system operators and Authorized Employees,
- authorizing the disclosure of Accessed Recordings, and
- annual Post-Installation Review of CCTV video surveillance systems.

Security Services Staff and Authorized Employees

Corporate Security staff and designated authorized employees are responsible for the following:

- completing mandatory training on system operation, privacy protection, and confidentiality requirements,
- creating, storing, and disclosing accessed recordings in full compliance with this policy and applicable legislation, and
- ensuring surveillance systems are managed internally, with access credentials configured on a per-user basis to maintain accountability and restrict unauthorized access.

Employees

Employees involved in the installation, operation, or handling of surveillance systems and recordings are responsible for:

- Reviewing and adhering to this policy and participating in required training.
- Avoiding unauthorized access, use, alteration, destruction, or erasure of recordings.
- Safeguarding personal privacy in compliance with the MFIPPA.
- Promptly reporting any unauthorized access or disclosure of recording

6. Compliance

Failure to comply with this policy, including any unauthorized access to or disclosure of recordings or accessed recordings, is cause for disciplinary action up to and including termination of employment.

7. Results of Review

☐ No Edits Required
☐ Housekeeping Edits
☐ Substantial Edits
☐ Repeal/Replace

8. Policy History

Administrative and Housekeeping Changes

Date	Nature of Change
yyyy-mm-dd	Departmental re-organization/Titling changes/ Standing Committee restructuring.

Substantial Changes

Date	Council/CLT Directive
2025-11-25	As Per Council/CLT Directive.

Appendix "A" – List of Definitions

Incident: refers to incidents that may include but are not limited to allegations or inappropriate behaviour which would be in violation of any City procedures relating to employee or public conduct**.**

Personal Information: is defined in Section 2 of MFIPPA, as recorded information about an identifiable individual, which includes, but is not limited to, information relating to an individual's race, colour, national or ethnic origin, sex and age. If a video surveillance system displays these characteristics of an identifiable individual, or the activities in which he or she is engaged, its contents will be considered "personal information" in accordance with MFIPPA**.**

MFIPPA: Municipal Freedom of Information and Protection of Privacy Act means legislation that governs access to and the privacy of municipal records.

Facility: any building, structure, property, or parcel of land that is owned, leased, operated, or otherwise occupied by the City. This includes, but is not limited to, administrative offices, community centers, public works yards, recreational venues, parks, marinas, golf courses, cemeteries, and any other municipal sites or infrastructure used to deliver City services or programs.

Accessed Recording: means information accessed from a Video Surveillance System by an Authorized Employee.

Authorized Employee: means any employee authorized by the Manager, Security Risk to create an Accessed Recording.

Record: is defined in Section 2 of MFIPPA, as any record of information, however recorded, whether in print form, on film, by electronic means or otherwise, and includes: a photograph, a film, a microfilm, a videotape, a machine-readable record, and any record that is capable of being produced from a machine-readable record.

Storage Device: means a videotape, computer disk or drive, CD ROM, computer chip or other device used to store the recorded data, or visual, audio or other images captured by a video surveillance system.

Video Surveillance System: refers to any system or device that enables continuous or periodic video or audio recording, observing or monitoring, and includes the storage device used to store the recorded visual images