



CITY PROCEDURE

Process for Video Surveillance

Procedure Title	Process for Video Surveillance		
Procedure Number	507-9	Approved Date	2026-07-16
Department	Legislative and Legal Services	Last Amended	
City Manager Signature	"S. Bourke" (signed)	Last Reviewed	
		Signature Date	2026-10-09

1. Purpose

- 1.1. The purpose of this procedure is to establish operational requirements for the implementation, use and management of video surveillance systems in accordance with Provincial Privacy Legislation and City policy.

2. Definitions

The definitions in [Policy 507 Privacy Management](#) apply to this procedure. In addition, in this procedure:

- 2.1. **"Access Request"** means a request under section 7 of the ATIA for access to a Record, including a Record containing the applicant's own Personal Information.
- 2.2. **"Authorized User"** means an Employee or Contracted Service Provider who has been granted approved access to a video surveillance system or recordings to perform assigned duties.
- 2.3. **"Covert Surveillance"** means the secretive continuous or periodic observation of person(s), vehicle(s), place(s) or object(s) to obtain information concerning the activities(s) of individuals.
- 2.4. **"Disclosure"** means to release, transmit, reveal, expose, show, provide copies of, verbally state the contents of or give Personal Information by any other means to someone. It includes oral transmission or information by telephone, or in person; provision of Personal Information on paper, by facsimile or in any other format; and electronic transmission through electronic mail, data transfer or the internet.
- 2.5. **"Destroy"** means the permanent destruction of all copies of a Record so that they cannot reasonably be reconstructed or retrieved (such as by shredding, pulping or secure digital deletion).
- 2.6. **"Facility Security"** means the City's Corporate Facility Management Department, responsible for stewardship, maintenance and security of the City's vertical infrastructure.
- 2.7. **"GIS and ITS"** means the City's GIS and ITS Department, responsible for maintaining and safeguarding the City's information technology systems.



CITY PROCEDURE

Process for Video Surveillance

- 2.8. **"Live Viewing"** means the real-time observation of video surveillance footage as it is being recorded.
- 2.9. **"Need-to-Know"** means access that is limited to individuals who require the information to perform assigned duties, and only to the minimum extent necessary.
- 2.10. **"Privacy Coordinator"** means the position responsible for operational administration, carrying out the powers, duties and functions related to Provincial Privacy Legislation that are delegated to the Privacy Coordinator by the City Manager.
- 2.11. **"Third Party"** means any person, group of persons or organization, but does not include: (a) the City; (b) the person making the request; or (c) a person on whose behalf the request is made.

3. Procedure & Guidelines

3.1. Authorization and Implementation

- 3.1.1. Employees must not install, modify or expand a video surveillance system without the approval of Facility Security under this section.
- 3.1.2. Facility Security, in consultation with the Privacy Coordinator, GIS and ITS, must review requests from departments to determine whether video surveillance is required based on operational need.
- 3.1.3. Video Surveillance must only be approved where:
 - a. A specific safety, security or operational need is identified;
 - b. Less intrusive alternatives are not effective; and
 - c. The proposed surveillance is proportionate to the identified purpose.
- 3.1.4. A Privacy Impact Assessment must be completed and approved under the Privacy Impact Assessment Procedure 507-3, where required under that procedure, before implementation.
- 3.1.5. Covert Surveillance may be conducted only where:
 - a. It is permitted by law;
 - b. Overt video surveillance would defeat the purpose; and
 - c. Prior written approval has been obtained from the City Manager.
- 3.1.6. Covert Surveillance must be limited to a specific purpose and defined time period and is subject to a Privacy Impact Assessment.

3.2. Installation and Collection

- 3.2.1. Facility Security must install and configure video surveillance only where necessary to achieve the approved purpose and in a manner proportionate to that purpose.



CITY PROCEDURE

Process for Video Surveillance

- 3.2.2.** Surveillance must be limited to locations with a demonstrated need, including:
 - a.** Entry and exit points;
 - b.** High-risk or high-traffic areas;
 - c.** Restricted or hazardous areas; or
 - d.** Locations with documented incidents.
- 3.2.3.** Video Surveillance must not be used where there is a high expectation of privacy, including washrooms and change rooms.
- 3.2.4.** Cameras must be configured to:
 - a.** Focus only on intended surveillance areas; and
 - b.** Minimize capture of adjacent properties or private spaces.
- 3.2.5.** Facility Security must maintain an inventory of approved video surveillance systems, including camera locations, and a list of Employees and Authorized Users with access. Where supported by technology, system audit logs will be employed and audited from time to time.

3.3. Notification

- 3.3.1.** Facility Security must ensure notice of video surveillance is provided through signage at entry points and in monitored areas.
- 3.3.2.** Signage must include:
 - a.** Notice of surveillance;
 - b.** Purpose of collection;
 - c.** Legal authority;
 - d.** Contact information for inquiries; and
 - e.** Where recordings may be input into an Automated System to generate content or make decisions, recommendations or predictions, a statement of that use
- 3.3.3.** Signage must be clear, visible and accessible.

3.4. Access and Use

- 3.4.1.** Access to video surveillance systems and recordings must be role based and limited to a Need-to-Know basis.
- 3.4.2.** Access must differentiate between:
 - a.** Live Viewing;
 - b.** Recorded playback with specified time limitations;
 - c.** Exporting; and
 - d.** Disclosing recordings.
- 3.4.3.** Recorded playback and exports require the approval of Facility Security and must be logged.



CITY PROCEDURE

Process for Video Surveillance

- 3.4.4.** Employees and Authorized Users must review recordings only where required for:
 - a.** Incident investigation; or
 - b.** Safety or security purposes.
- 3.4.5.** Employees and Authorized Users must not access video surveillance systems or recordings for purposes unrelated to their duties.
- 3.4.6.** Facility Security must review access at least annually and remove it when no longer required due to role change, transfer, contract completion or termination of employment.
- 3.4.7.** Employees must not permit a Third Party to view recordings without the prior approval of the Privacy Coordinator, and viewing may be permitted only where authorized under Provincial Privacy Legislation or another enactment.
- 3.4.8.** In an emergency, viewing by or Disclosure to a law enforcement agency or other appropriate person or body may occur without prior referral where the City Manager, or a person to whom that power has been delegated in writing under POPA, believes on reasonable grounds that it will avert or minimize (a) a risk of harm to the health or safety of a minor, or (b) an imminent danger to the health or safety of any person. The Employee must limit what is shown or Disclosed to what is necessary in the circumstances, notify the Privacy Coordinator and the Privacy Officer, and document the viewing or Disclosure as soon as practicable afterward.

3.5. Disclosure

- 3.5.1.** Internal access for operational purposes is not considered a Disclosure.
- 3.5.2.** The authority to Disclose recordings is governed by the Collection, Use and Disclosure Procedure 507-1. Employees must refer requests for Disclosure to the Privacy Coordinator in accordance with that procedure.
- 3.5.3.** The Privacy Coordinator must ensure all Disclosures are documented in an auditable log including:
 - a.** Date and time;
 - b.** Recipient;
 - c.** Purpose; and
 - d.** Legal authority.
- 3.5.4.** The Privacy Coordinator must establish standard access and Disclosure forms, and requests must be made on them.
- 3.5.5.** Recordings must be transmitted only by methods approved for information of that classification level, in accordance with the Safeguarding Personal Information Procedure 507-5.



CITY PROCEDURE

Process for Video Surveillance

- 3.5.6.** Disclosure to law enforcement, Regulatory Bodies or other public bodies must be made in accordance with section 4.9 of the Collection, Use and Disclosure Procedure 507-1.

3.6. Redaction

- 3.6.1.** Redaction techniques must be applied where required for a Disclosure or in response to an Access Request.
- 3.6.2.** Redaction methods may include:
- a.** Blurring or masking individuals; and
 - b.** Removing audio.

3.7. Retention

- 3.7.1.** Routine recordings that have not been accessed or used must be retained in accordance with the City's approved records retention schedule.
- 3.7.2.** Where a recording has been Used to make a decision that directly affects an individual, including a decision made using an Automated System, it must be retained for at least one year after the Use, so the individual has a reasonable opportunity to obtain access to it, unless a shorter period has been agreed to in writing in accordance with section 6(b) of POPA.
- 3.7.3.** Recordings must be securely Destroyed once retention requirements have been met, and must not be Destroyed while subject to a legal hold, an outstanding access or correction request, or the retention requirement in section 3.7.2.

3.8. Security

- 3.8.1.** Video surveillance systems and recordings must be protected by reasonable security arrangements, appropriate and proportional to their security classification under the Safeguarding Personal Information Procedure 507-5, including:
- a.** Secure storage;
 - b.** Encryption;
 - c.** Access controls; and
 - d.** Audit logs.
- 3.8.2.** Employees and Authorized Users must not take screenshots, photographs or informal copies of recordings unless authorized by the Privacy Coordinator.
- 3.8.3.** Monitoring equipment must be stored in secure locations not accessible to the public.
- 3.8.4.** Where system functionality allows, audit logs must record:
- a.** User access;
 - b.** Exports; and
 - c.** System changes.



CITY PROCEDURE

Process for Video Surveillance

- 3.8.5. Authorized Users may be granted access only where required for approved purposes and must be:
- a. Authorized;
 - b. Limited in scope; and
 - c. Removed when no longer required.

3.9. Incident Response

- 3.9.1. Employees and Authorized Users must report any suspected or confirmed Privacy Incident involving video surveillance to the Privacy Coordinator without unreasonable delay and follow the Privacy Incident Response and Notification Procedure 507-6.

4. Roles and Responsibilities

- 4.1. The City Manager must review and approve this procedure and any amendments.
- 4.2. Employees and Authorized Users must comply with this procedure.
- 4.3. The Privacy Coordinator administers Disclosure referrals under Procedure 507-1 and provides guidance on privacy requirements.
- 4.4. GIS and ITS must maintain and secure technical safeguards for video surveillance systems, and Facility Services must consult GIS and ITS before implementing a system or technical change.

5. Attachments

- 5.1. [Request for Personal Information Form](#)
- 5.2. [Regulatory Bodies Disclosure Form](#)

6. Version History

Action	Date	Description
New Procedure	2026-07-16	