CITY OF CORNER BROOK

Policy Statement

Policy Title	*Video Surveillance*	**Index:**	*Communication*
Section:	*Computers*	**Policy Number:**	*12-02-01*
Authority	*Council*	**Adopted Date:**	*June 22, 2026*
Effective Date:	*June 22, 2026*	**Revision Date:**	
Policy Owner:	City Clerk		

1. POLICY STATEMENT

The City of Corner brook is committed to the protection of public safety, crime prevention and asset security in conjunction with the protection of privacy and personal information.

2. PURPOSE

To establish guidelines and procedures for the governance, collection, notification, use, disclosure, security and retention of information collected through video surveillance systems installed by the City of Corner Brook. Video surveillance systems may be installed in areas that cover City owned property, buildings and infrastructure for the purpose of security and investigatory methods, as well as security by means of deterrence.

3. DEFINITIONS

ATIPPA – the *Access to Information and Protection of Privacy Act, 2015 Ch. A-1.2* as amended, also referred to as "the Act"

ATIPP Co-ordinator – the individual designated in accordance with ATIPPA

ATIPP Head – the person designated by Council as the head of the public body for the purpose of ATIPPA

CCTV –means any video security technology (video cameras; still frame cameras; digital cameras; and time-lapse cameras) that enables continuous or periodic recording (videotape, photographs or digital images), viewing or monitoring of a public area but does not include Covert Surveillance.

Covert Surveillance – refers to any video or surveillance activity that is conducted without the knowledge of the individual(s) being monitored, where recording equipment is intentionally concealed, disguised or otherwise not readily observable. Covert Surveillance is used where the collection of information (including personal information) is necessary for any legal investigative purpose including but not limited to law enforcement and investigation of by-law or regulatory violations.

Computer Services Department – refers to the department responsible for the administration of technology, software and digital infrastructure

Personal Information – as defined by the *Access to Information and Protection of Privacy Act, 2015 SNL2015 Ch. A-1.2* as amended.

User Account – an account designed for user access to the CCTV surveillance systems that are explicitly managed by the Computer Services Department or other applicable department and is assigned to the specific individual that is granted access through virtue of this policy.

Record – as defined in the *Access to Information and Protection of Privacy Act, 2015 Ch. A-1.2* as amended and any similar successor legislation.

4. APPLICABILITY

Responsibility

The City Manager shall be responsible for implementation, administration and evaluation of the City's video security Policy and procedures.

The ATIPP Coordinator shall be responsible for ensuring that information obtained through CCTV surveillance is administered in accordance with this policy and the Act. The ATIPP Coordinator shall also be responsible for receiving and reviewing all requests for information including information recorded through CCTV that is requested either informally or formally through an Access to Information Request under the Act. The City Manager may designate an alternate ATIPP Coordinator and/or other staff persons from time to time the City Manager deems necessary or expedient for the purpose of administering this policy.

The Computer Services Manager shall arrange inspection, monitoring, maintenance, and alteration as required of each City owned and operated site that is equipped with a CCTV surveillance system to ensure that they comply with this policy, as well as any site-specific policies that are in place. In particular, the Computer Services Manager shall ensure that any staff with authorized access to the monitoring equipment and recorded information shall be trained in its use in accordance with their duties under this Policy and any other applicable policies, bylaws and/or legislation. The Computer Services Manager is responsible for maintaining user access and accounts. The Computer Services Manager may delegate duties to other employees from the Computer Services Department from time to time as the Computer Services Manager deems necessary or expedient for the purposes of administering this policy.

The City is not liable for any inability to retrieve recorded data including but not limited to, due to failure of technical equipment, inadequate or delayed requests that go beyond the City's usual scope and/or timeline for retention.

Use

Video surveillance systems shall only be installed where it is deemed by the City to be necessary or expedient for investigation, law enforcement and/or security purposes. CCTV surveillance systems may not record audio but may be equipped with visual recording capabilities for investigatory purposes. Access to information collected via video surveillance will only be accessed and operated by authorized personnel and will be limited to staff who require access to perform their duties.

Video surveillance systems and/or recorded footage shall not be used for performance monitoring, evaluation, or disciplinary action pertaining to City employees save and except for the following circumstances:

a. The actions of the City employee is or may be considered a criminal offence; or
b. The video surveillance forms part of an investigation of the employees conduct where the City Manager has pre-authorized such investigation

Process

New Camera Installation

Prior to the installation of any new CCTV surveillance system, a review must be conducted that analyzes the following:

- What is the purpose of adding new video surveillance system in an area?
- Are there any other methods that can be used to achieve that purpose?
- Are there any privacy concerns with installing a video surveillance system in an area that outweigh the purpose of installing them in an area?
- Will the information that may be collected through the video surveillance system be useful for the purpose of which the system was installed?

To request the installation of a new video surveillance system in a specific area, the request form (Schedule A – Option 1: New Camera Installation) must be completed and submitted to the immediate supervisor of that department for review and approval. The request will be reviewed by the ATIPP Co-ordinator and the Computer Services Manager to evaluate. If approved the Computer Services Manager and the ATIPP Coordinator shall provide the appropriate parameters, use and access that ensure compliance with this policy and the Access to Information and Protection of Privacy Act.

User Account Access

If a staff member is requesting user access to the CCTV surveillance software, they must complete the request form (Schedule A – Option 2: User Account Access). The request form shall include information that states the purpose of the access, the type of access needed and why (live or recorded or both) and any other methods that were considered to accomplish this purpose.

This form shall be submitted to the immediate supervisor of that department for review and approval. The request will be reviewed by the ATIPP Co-ordinator and the Computer Services Manager to evaluate. If approved the Computer Services Manager and the ATIPP Coordinator shall provide the appropriate parameters, use and access the ensure compliance with this policy and the Access to Information and Protection of Privacy Act.

Recorded Footage Access

Any request for CCTV information, either informally or formally in accordance with the Act must be made to the ATIPP Co-ordinator. No CCTV information is to be released to the public or staff without consulting with the ATIPP Co-ordinator. Upon receiving a request for information that may be recorded through the CCTV surveillance system, the ATIPP Co-ordinator shall request the Computer Services Manager to extract the information based on the narrowest parameters possible that can potentially contain the information requested. The Computer Services Manager is to then provide this information to the ATIPP Co-ordinator to review and determine if it can be released to the individual(s) who has requested it and if any information contained in the records would need to be withheld in accordance with the Act.

Requests from Law Enforcement Personnel and/or Agencies - The City may disclose recorded CCTV footage to law enforcement personnel. Requests for CCTV footage from law enforcement personnel should be made directly to the ATIPP Co-ordinator. The ATIPP Co-ordinator shall review the request for compliance with the Act, confirm the lawful authority of the agency or person requesting the footage and ensure disclosure is limited to what is strictly necessary.

Requests for CCTV video surveillance for the purpose of civil litigation, investigation and/or prosecution of alleged offences, internal and/or external investigations of workplace incidents, occupational health and safety (OHS) matters or other security concerns shall follow the same process as stated above and should be made directly to the ATIPP Coordinator. These requests may be, but are not limited to, the purpose of gathering documentation for civil litigation to which the City is or intends to be a party, investigating alleged violations of municipal, provincial, or federal laws, investigating a reported workplace accident, injury or potential incident , responding to a health or safety concern involving staff or the public, investigating alleged workplace misconduct including harassment, violence or policy violation or investigating cause of damage, loss, security breaches or operation disruptions. Requests shall not be made for personal reasons not aligned with a use as outlined in this policy. Access to any recorded footage obtained for this purpose shall only be granted to designated officials whose duties reasonably require such access including the City Manager, City Solicitor, City Insurer, Municipal Enforcement Officers, Human Resources Manager, Occupational Health and Safety representatives, authorized police representatives or another representative otherwise authorized by the City Manager.

The ATIPP Co-ordinator shall record any requests for disclosure, along with whether the request was approved and if footage was released.

Live Streamed Cameras

Live cameras installed by the City are intended for tourism promotion. These cameras stream real-time images of public outdoor areas and are accessible to the public through the City's official website. These cameras capture information in public areas and clear signage shall be posted in all locations where live-stream cameras are installed to inform the public that a live video feed is in operation and available online.

Any requests for the installation of cameras for live-only access shall follow the same approval process for CCTVs outlined in this policy. Requests must demonstrate the purpose for installation which must be in line with this policy and the Act.

Any location with live streamed camera shall include on the posted sign notification that it is a live streamed camera area including information on where the streaming can be found.

Collection

The information that is collected through use of CCTV includes recorded video of images only. The CCTV utilized should be for video images only and should contain no capability of audio information or should have any auditory capability disabled - therefore no audio information is to be collected and subsequently recorded or stored from CCTVs.

Information that is collected should serve the purpose for the system only and therefore the installation and use of CCTV systems should be done with the least amount of invasion of privacy as possible.

The installation of CCTV surveillance systems shall be prohibited in areas where both the public and employees have a higher expectation of privacy, such as change rooms, washrooms, and neighbouring residential properties.

For further clarity nothing herein prevents the City from recording audio and video in Covert Surveillance. The City may conduct Covert Surveillance using video and audio surveillance when appropriate in a law enforcement function and/or to conduct a legal investigation on a civil matter.

Notifications

The City shall ensure that the public is notified about the presence of CCTV surveillance equipment by prominently posting signs in the vicinity of areas under surveillance. Signs shall be of a consistent size and format and include notification that video surveillance is in use and provide the title, address and telephone number of contact person who can answer questions about the system and privacy.

For further clarity, the use of Covert Surveillance shall be exempt from this section of the policy.

Access and Auditing

The City shall ensure that CCTV video monitors are accessed only by authorized staff or an authorized service provider and are not located in a position that enables public viewing or viewing by staff whose duties do not reasonably require access. Access to video monitors or areas where information collected from the video surveillance systems exist shall be secured to prevent unauthorized access.

The Computer Services department shall host all user access and accounts and be responsible for administering those accounts as required. The CCTV surveillance software shall have the ability to provide an audit report which may generate a history of access for each user. This audit report shall be run every 6 months or when deemed necessary to review with the ATIPP co-ordinator and ensure compliance with this policy. This review should also include quality check to confirm there are no technology issues or vulnerabilities with the equipment and the program, that there are no changes with information that can be obtained by the camera, as well as making sure there are no physical alterations to positioning and capture of approved subject matter. In addition, the Computer Services department may review audit history upon complaint of inappropriate access, misuse of the video surveillance equipment and/or software or a breach of this policy

Any authorized personnel whose level of access changes or who are no longer employed with the City of Corner Brook, should be removed from the list of users with access as soon as that change becomes effective.

Disclosure

A breach of this policy by any City employee may also constitute a breach of the Access to Information and Protection of Privacy Act and may result in disciplinary action up to and including termination of employment for just cause. Additionally, the employee may, in accordance with the ATIPP Act, be found guilty of an offence and may be subject to a fine and/or jail time as a person who has wilfully collected, used or disclosed personal information in contravention of the Act.

Upon a notification of a privacy breach in accordance with this policy the City Manager and the ATIPP Co-ordinator shall be immediately notified and attempts made to contain the breach and limit further disclosure of information if reasonably practicable. The City Manager and/or ATIPP coordinator may also report the privacy breach to the Office of the Privacy Commissioner.

Security

<u>Equipment</u>

All procurement, maintenance and installation of equipment for CCTV surveillance shall be arranged by the Computer Services department, and new equipment should be purchased in keeping with the

existing equipment, unless otherwise approved by Computer Services due to needs or change of technological specifications. No purchase or installment of CCTV surveillance equipment, including but not limited to cameras shall be conducted without receiving approval in accordance with this policy.

All records of CCTV surveillance that are exported and stored in accordance with this Policy shall be clearly labelled with the date(s) and location(s) where the video recording took place and shall be stored in a location where access is restricted to only those who require it or are granted access by the ATIPP Coordinator and/or the Computer Services Manager.

Retention

Data from CCTV surveillance will be stored and maintained for at least 14 days in a manner that preserves the integrity of the recorded information to ensure its viability if the collected information requires disclosure or review. The time of storage depends on the type of camera, the amount of information collected and the storage space of the system. If there is a request for a video or is an indication that a request may come, the system should be searched to determine whether the requested footage is still available.

In the circumstance that there could be information collected through CCTV surveillance that is required for legal and/or investigatory purposes, including but not limited to law enforcement purposes, the information shall be stored in a location where access is limited to only authorized personnel who require access. The video file shall be stored in a password protected and/or encrypted folder on the system and/or any applicable devices.

Exported video surveillance records shall be retained for a minimum of 10 years and will be reviewed for selective retention after that time. Retention after this will be based on whether it was disclosed, whether the use was for law enforcement, workplace investigation or other legal reason. Any Authorized Personnel may direct that the recording(s) be retained beyond the date of retention for either another specified period or permanently retention depending on its administrative and archival value. Additional or permanent retention will be considered when used in relation to a criminal, safety, and/or security investigation or if it is being used, or may be used, as evidence in a criminal, civil, or administrative proceeding. Recordings related to an event of historical significance may also be considered for permanent retention when deemed so by authorized personal.

Contact Information

This policy must be consistent with the ATIPP Act, the Charter of Rights and Freedoms, as well as City policies and other applicable legislation, rules and laws. The video security system as well as the Policy will be subject to regular review.

6. POLICY REVIEW

This policy shall be reviewed on a regular basis to ensure that it conforms with all legal obligations under legislation and applicable case law, as well as any potential changes to industry standards and technological requirements.

7. SCHEDULE(S) (Optional)

8. AMENDMENT(S) (Mandatory)

Date of Council Decision	Report / Bylaw	Description

9. REVIEW(S) (Mandatory)

Date of Policy Owner's Review	Description

10. Reference: Regular Meeting June 22, 2026

IN WITNESS WHEREOF this policy is sealed with the Common Seal of the City of Corner Brook.

[redacted]

Mayor

[redacted]

City Clerk

[redacted]

CORNER BROOK

Schedule A - Video Surveillance Request Form

This form is used to request:

1. Installation of a new camera on City property

2. User access to the video surveillance system

Any request for recorded footage must be made directly to the City Clerk and will be reviewed in accordance with the Video Surveillance Policy and the Access to Information and Protection of Privacy Act (ATIPPA, 2015).

A. Applicant Information

Applicant Name:

_____

Department:

_____

Contact Information (phone/email):

_____

B. Type of Request

[ ] Installation of New Camera

[ ] Request for User Access to System

C. Purpose of Request

Describe the purpose of the camera installation or system access:

_____

_____

D. Other Methods Considered

Describe any alternative approaches attempted and results:

_____

_____

CORNER BROOK

E. Installation Requests Only

What information will the camera capture?

_____

_____

Identify any potential privacy concerns (homes, daycare, etc.):

_____

_____

F. Access Requests Only

[ ] Live Footage Only

[ ] Live & Recorded Footage

State the purpose for access:

_____

_____

Could another method achieve the same purpose?

_____

Signature

Signature: _____