City of Pitt Meadows
THE Natural PLACE

COUNCIL POLICY C042

02 - Buildings, Facilities & Properties

Video Surveillance

Effective Date: September 4, 2012
Last Revised: April 15, 2025

1. Purpose

The purpose of this policy is to authorize and set standards for the implementation and use of video surveillance systems in City facilities and spaces.

2. Scope

This policy applies to all City Staff and all video surveillance systems owned and managed by the City.

3. Exclusions

This policy is not applicable to, nor intended to interfere with, the surveillance needs and responsibilities of the RCMP or other law enforcement agencies.

4. Definitions

In this policy,

(1) **City** means the City of Pitt Meadows.

(2) **Collected data** means any video, audio, images, or other personal information captured and recorded through a video surveillance system.

(3) **FIPPA (the "Act")** means the Freedom of Information and Protection of Privacy Act.

(4) **Privacy Impact Assessment ("PIA")** means a written assessment that is conducted by the City to determine if a proposed program, activity or system meets the privacy protection requirements established by FIPPA, and which identifies steps to mitigate privacy risks and ensure compliance.

(5) **Privacy Head** means the person appointed by Council, pursuant to FIPPA, to oversee the Privacy Program of the City.

(6) Video surveillance means a mechanical, electronic or digital surveillance system or device that enables continuous or periodic video recording, observing or monitoring of individuals, assets and/or property.

5. Policy Statements

5.1. Video Surveillance

(1) The City may implement video surveillance for the purposes of safety, security, and law enforcement, including the deterrence of, and intervention in, unlawful activities.

(2) The City recognizes the intrusive nature of video surveillance and will only use such systems if:

a) there is evidence of crime, public safety concerns, or other compelling circumstances that support the necessity of surveillance in a City facility or space;

b) the surveillance is authorized by FIPPA; and

c) it is determined that other, less privacy-invasive options would not be effective or feasible.

(3) Access to, and disclosure of, collected data will be done in compliance with FIPPA, this Policy, and the City's Privacy Management Program, with all necessary procedures established by the Privacy Head.

5.2. Consultation and Assessment

(1) Before implementing a new video surveillance camera or system, City staff will:

a) consult with the IT Department regarding the technical feasibility of implementing a surveillance system in the specified location;

b) consult with the Privacy Head regarding the scope, responsibilities, and privacy risks associated with the proposal;

c) ensure compliance with section 5.1(2) of this Policy; and

d) complete a PIA, using the form prescribed by the Privacy Head.

(2) A PIA for a new video surveillance system will include:

a) an assessment of how the system might affect the privacy of individuals and steps for mitigating privacy risks;

b) details of the physical and technical security measures, including access controls, that will be implemented to ensure the protection of the surveillance system and collected data;

c) recommendations from the Privacy Head to ensure the collection, use, disclosure, and security of any personal information is compliant with the Act; and

d) any other information deemed necessary by the Privacy Head.

(3) The Privacy Head must review and approve the PIA, confirming compliance with FIPPA and the City's Privacy Program, before a new video surveillance system is implemented.

5.3. Notification of Surveillance

(1) The City will provide notice to the public of a video surveillance system by prominently displaying signs in or at the perimeter of the surveillance area.

(2) The notification of surveillance must be approved by the Privacy Head and meet the notification requirements established by FIPPA.

5.4. System Calibration

(1) Video surveillance systems will be situated and calibrated so that they collect the minimum amount of personal information required to achieve the purposes identified for that system.

5.5. Security, Access, and Disclosure

(1) Only authorized individuals who require the information in order to do their jobs will have access to video surveillance systems, software, and collected data.

(2) Physical and electronic security measures will be implemented to ensure the safety, security, and controlled access of video surveillance systems, software, and collected data.

(3) Collected data will only be accessed when there is documented evidence of a crime, imminent risk to public safety, or other compelling circumstance that warrants access.

(4) Requests for access and disclosure of collected data will be managed in accordance with the Privacy Program as prescribed by the Privacy Head.

5.6. Records Management

(1) Collected data will be retained for a period of no longer than 60 days and destroyed at the end of this retention period, unless legislation prescribes otherwise.

6. Related Policies

Other related policies include:

(1) Freedom of Information & Protection of Privacy Bylaw No. 2877, 2021

(2) Privacy Program Policy A043