TITLE: VIDEO SURVEILLANCE OF MUNICIPAL PROPERTY

Approved by Council Date: September 26, 2023

Revised by Council Date:

PURPOSE OF POLICY

The purpose of this policy is to establish guidelines for the use of video surveillance to enhance the security and safety of persons, properties, things, and activities that are in, on, or near facilities owned or occupied by the MD and used for public civic purposes.

POLICY STATEMENT

1. This Policy applies to any video surveillance system operated by or for the MD that collects personal information in any form. It does not apply to video surveillance systems that do not collect personal information about identifiable individuals. This Policy does not apply to video surveillance conducted by the Royal Canadian Mounted Police ("RCMP"), who are subject to the Freedom of Information and Privacy Act, to covert video surveillance.

DEFINITIONS

2. For the purpose of this policy, the following definitions shall apply:

    a) "MD" shall mean and refer to the Municipal District of Pincher Creek No. 9
    b) "Employer" shall mean and refer to the Municipal District of Pincher Creek No. 9
    c) "Employee" shall mean any employee of the Municipal District of Pincher Creek No. 9
    d) "FOIP " shall mean Freedom of Information and Privacy

SCOPE

3. As an owner of significant public assets that represent a large investment of public money, the MD wishes to make use of video surveillance systems to better protect the security of its people, assets and property.

4. The MD acknowledges that the use of video surveillance may, in some circumstances, represent an intrusion into personal privacy and does not wish to impair personal privacy any more than is warranted to provide necessary and reasonable protection of its property against vandalism, theft, damage and destruction. Video surveillance recordings can be used by the MD for the investigation and as evidence in any civil proceedings.

5. Video surveillance systems will be installed only after other less intrusive security methods have been considered or attempted and have been found to be insufficient or unworkable.

6. Before implementing a surveillance system or expanding an existing video surveillance system, the reason for introducing or expanding the video surveillance is to be clearly articulated in writing and approval for the introduction or expansion of video surveillance must be granted by Council.

DESIGNATED RESPONSIBILITIES:

7. The Chief Administrative Officer is responsible for the overall video surveillance program. This responsibility may be designated to the Director of Finance as designate.

8. The IT Specialist is responsible for ensuring the establishment of procedures for the use of video surveillance equipment, including the random audit of such procedures, in accordance with this policy.

9. The IT Specialist is responsible for the life cycle management of authorized video surveillance systems including, but not limited to, specifications, installation, maintenance, replacement, disposal, and related requirements, including signage. Equipment specifications and standards are to follow corporate policy.

10. MD employees and service providers shall review and comply with the policy in performing their duties and functions related to the operation of video surveillance systems. MD officers and employees may be subject to discipline if they knowingly or deliberately breach the policy.

11. Employees who have read and acknowledge this policy shall sign off on Appendix "A" - Video & Audio Recordings – Acknowledgement Form.

12. Service providers having access to video surveillance information must be bonded and sign a confidentiality agreement limiting access to, copying and disclosure of personal information and requiring compliance with this Policy. Breach of the confidentiality agreement may lead to penalties up to and including contract termination.

VIDEO SURVEILLANCE REQUIREMENTS AND USE

13. Video surveillance will not be used to supervise staff performance or to verify staff attendance in the workplace.

14. Before introducing video surveillance in any MD owned facility the need for video surveillance must clearly meet the criteria of this Policy and the installation must conform to this Policy and be approved by Council in consultation with the FOIP Officer.

15. When considering the proposal, Council will consider the following:

    a) Incident reports respecting vandalism, theft, property damage, and safety concerns.
    b) Safety or security measures in place currently or attempted before installing video surveillance.
    c) Safety or security problems that video surveillance is expected to resolve.
    d) Areas and/or times of operation.
    e) Expected impact on personal privacy.
    f) How the video surveillance will benefit the MD or is related to MD business.
    g) How the benefits are expected to outweigh any privacy rights as a result of video surveillance.
    h) How it will protect the security and safety of persons.
    i) The MD has the right to investigate activity of a criminal nature on its property.

16. Video surveillance must only be in public places and must be practically minimized. Surveillance will not take place in areas considered confidential or normally private, e.g. change rooms, washrooms.

17. Where there is a risk to people, property, or things in areas normally used to conduct MD business, the Chief Administrative Officer may authorize video surveillance to investigate individuals for matters affecting the substantial interest of the MD and inform Council immediately of the matter.

DAILY USE, ACCESS, AND SECURITY

18. Access to video surveillance information is limited to the following individuals:
    - Chief Administrative Officer
    - Director of Finance
    - IT Specialist
    - FOIP Officer
    - MD Solicitor
    - RCMP in relation to a law enforcement matter
    - An Agent appointed by the Municipal District of Pincher Creek No. 9.
    - A reference to a person in this section includes his or her deputy, where applicable.

19. Use of video surveillance information is to be for the purposes of investigation of an incident in any public place. IT Specialist will access the equipment only for the purpose of maintaining, backing up the software, and assisting with the extraction of the portions of the data. MD staff may be authorized to view, retrieve and access video surveillance in the course of their duties.

20. Physical and computer related security must be in place at all times to properly secure access to the recording equipment and video data. Detailed logs that record all instances of access to and use of the recording equipment and video material must be maintained at all times by the relevant department.

21. Records of video surveillance systems that collect personal information must be protected in accordance with the Freedom of Information and Protection of Privacy Act.

22. The locations and times of all video material must be maintained in logs and kept current by the relevant department. Generally, the video surveillance equipment or screen must be located so that the public is not able to see any video reproduction. An exception to this may occur when the video screen is mounted in a public place with the intention of communicating information to the general public by live video feed.

23. Video surveillance data or videotapes may not be publicly viewed or distributed in any fashion as provided by this policy and/the FOIP Act. Video data must not be altered in any manner, with the exception of saving investigation material related to an incident on public places or information required for law enforcement purposes. Other than release to the RCMP, or use for MD purposes in accordance with this Policy, video surveillance data will only be released on the authority of a warrant to seize the recorded data for evidence or other court order.

24. Any other requests for access to incident specific information must be referred to the MD FOIP Officer and will only be disclosed in accordance with the FOIP Act.

RETENTION AND DESTRUCTION

25. The MD will use a recording system that overwrites data on a continual basis.

26. Retention of the recorded video data is determined by the amount of available space within the MD storage facilities and the type of medium used to store such data.

27. Recorded video data will generally be retained for between two and four weeks depending on the system configuration and available memory. Recorded material will automatically be deleted and purged at the expiry of the above retention period.

28. Recorded data that has been saved to another medium, for investigation purposes, will be retained for at least one year after being used, so that the affected individual has a reasonable opportunity to obtain access to that personal information. Such recorded data is to be destroyed after one year or after the affected individual has had access to the data, unless otherwise required for legal, administrative or other proceedings.

29. Old storage devices must be securely disposed of based on medial format by shredding, burning or magnetic erasure.

SIGNAGE

30. It is a requirement of the FOIP Act that individuals be notified when the MD collects their personal information. Accordingly, at each facility where video surveillance takes place, signs must be prominently displayed at entrances to and egresses from the facilities.

31. The sign must clearly state by symbols the placement of video surveillance cameras or the following:

"This area may be monitored by video surveillance cameras. Please direct inquiries to the Municipal District of Pincher Creek No. 9. " and will include the name of the Chief Administrative Officer and phone contact number, as well as the business hours they can be contacted. A pictogram of a video camera must also be shown on the sign.

TRAINING

32. When applicable and appropriate, the policy and guidelines will be incorporated into training and orientation programs of the corporation. Training programs addressing staff involvement with the use and monitoring of video surveillance equipment under the policy and under the FOIP Act shall be conducted as required.

Richard D. Lemire
Reeve

Roland Milligan
Chief Administrative Officer

Appendix A
Video & Audio Recordings – Acknowledgement Form

The MD uses a security camera system capable of recording both video and audio for monitoring the Administration building and Public Works building/yard.

The video and audio recordings are used to ensure the safety and security of the MD's facilities, and staff.

All video and audio recordings are kept for a maximum of 30 days.

Authorized access to video and audio recordings, as determined by the Chief Administrative Officer and The Director of Finance, only occurs when a significant security or safety incident has happened.

The video and audio recording devices are protected from unauthorized access by a secure swipe code, and all access is documented.

As described above, I _____ understand the MD uses a security camera system capable of recording video and audio. My signature below indicates my understanding and acknowledgment.

_____ _____

Employee Name CAO

_____ _____

Employee Signature Date