POLICY STATEMENT AND REGULATIONS

Number: 100.8

VIDEO SURVEILLANCE OF CIVIC PROPERTY

POLICY OBJECTIVE

The District may use video surveillance systems to ensure the security of individuals, assets, and properties, and when such a system is operated in, on, or near facilities owned or occupied by the District of Summerland, the system must be operated in accordance with the guidelines for the use of the system outlined in this policy. This policy applies to any video surveillance system operated for or by the District of Summerland that collects personal information in any form but does not apply to video surveillance conducted by the Royal Canadian Mounted Police, and does not permit community safety cameras used to support the suppression of criminal activity and police investigation of high crime areas within the community (e.g. streets or public areas).

POLICY

Principles

1. As an owner of significant public assets that represent a large investment of public money, the District wishes to make use of video surveillance systems to better protect the security of its people, assets, and property.
2. The District 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.
3. Video surveillance systems will be installed only after other less intrusive security methods have been considered or attempted and have been deemed to be insufficient or unworkable, unless the urgency of the situation dictates otherwise. Video surveillance systems may be used in conjunction with other security efforts and initiatives.
4. Before implementing a surveillance system or expanding an existing video surveillance system, the reason for introducing or expanding the video surveillance system is to be provided in writing to the Chief Administrative Officer and the new system or expansion shall only be implemented upon approval of the Chief Administrative Officer.
5. The District has a right to investigate activity of a criminal nature on its property.
6. Video surveillance is not to be used to supervise staff performance or to verify staff attendance in the workplace.
7. Video surveillance must only be used in public places and will not take place in areas considered confidential or normally private (e.g. change rooms, washrooms)
8. All employee representatives will be notified in writing prior to implementation of any video surveillance system. Also, notices will be placed on appropriate District of Summerland employee notice boards.

Designated Responsibilities

1. The Chief Administrative Officer is responsible for the overall video surveillance program.
2. The Chief Administrative Officer, or their designate, is granted access to the equipment for the purpose of maintaining, backing up the software, and assisting with the extraction of portions of the data, and is responsible for protection of the video surveillance system records in accordance with the *Freedom of Information and Protection of Privacy Act.*

Video Surveillance Requirements and Use

1. Before introducing video surveillance in any District facility, the need for video surveillance must clearly meet the intent of this policy and the installation must conform to this policy and be approved by the Chief Administrative Officer. The Chief Administrative Officer, when considering a proposal, will consider the following:
    a. Incident report respecting vandalism, theft, property damage, and safety concerns.
    b. Safety or security measures in place or attempted before installing video surveillance.
    c. Safety or security problems that video surveillance is expected to resolve.
    d. Area and/or times of operation
    e. Expected impact on personal privacy
    f. How the video surveillance will benefit the District or is related to District 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.
2. Unless otherwise authorized by the Chief Administrative Officer, access to video surveillance information is limited to the following individuals:
    - Mayor
    - Chief Administrative Officer
    - Directors
    - Corporate Officer
    - District Solicitor
    - RCMP in relation to a law enforcement matter

    Other than the Mayor and the CAO, none of the persons on this list can access the surveillance information without authorization of the CAO or the Mayor.
3. The locations and times of all video taping, and access thereto, must be maintained in logs and kept current by the relevant department.
4. Video surveillance data or videotapes may not be publicly viewed or distributed in any fashion as provided by this policy and/or the Freedom of Information and Protection of Privacy Act. Video data must not be altered in any manner, with the exception of saving investigation material related to an incident or information required for law

enforcement purposes. Other than release to the RCMP, or use for District of Summerland 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.

5. Any other requests for access to incident specific information must be referred to the District's Corporate Officer.

Signage

1. At each facility where video surveillance takes place, signs not less than 30 cm X 30 cm in size must be prominently displayed at entrance to and egresses from the facilities.
2. The sign(s) must clearly state the following:

   "This area may be monitored by video surveillance cameras. Please direct inquiries to the Corporate Officer, District of Summerland, 250-494-6451 during regular office hours."

Retention and Destruction

1. The District will use a recording system that overwrites data on a continual basis.
2. Recorded video data will generally be retained for up to four weeks, depending on the system configuration, available memory, and the amount of available space within the District's storage facilities and the type of medium used. Recorded material will automatically be deleted and purged at the expiry of the above retention period.
3. 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(s) have 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.

Adopted: November 10, 2014