REGIONAL DISTRICT OF OKANAGAN-SIMILKAMEEN
BOARD POLICY

POLICY: Video Surveillance Policy

AUTHORITY: Board Resolution dated June 15, 2017.

POLICY STATEMENT

The Regional District of Okanagan-Similkameen wishes to make use of video surveillance systems to better protect the security of its people, assets and property. The Regional District 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 systems will be installed only after other security methods have been considered or attempted and have been found to be insufficient or unworkable. Before implementing a new surveillance system or expanding an existing video surveillance system, the need for introducing or expanding the video surveillance is to be provided in writing and approval must be granted by the Board of Directors.

PURPOSE

To establish guidelines for the use of video surveillance technology consistent with the *Freedom of Information and Protection of Privacy Act*, in furtherance of the Regional District's activities to protect its property and the safety of those using it.

Use of video for purposes other than surveillance (ie. blurred images used for use volume or counting purposes only) and which does not impact personal privacy, is not contemplated in this policy, and would proceed under an alternate process.

DEFINITIONS

FIPPA Head means the person or persons named to this position by Regional District of Okanagan-Similkameen bylaw.

Open Public Space means the grounds of any real property, or portions of real property, owned or subject to a right of occupancy by the Regional District to which the public is invited or permitted to be on.

Personal Information means recorded information about an identifiable individual, other than contact information.

Privacy Impact Assessment (PIA) means an assessment that is conducted to determine if an enactment, system, project or program meets the requirements of the *Freedom of Information and Protection of Privacy Act*.

Regional District means Regional District of Okanagan-Similkameen.

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

PRIVACY CONSIDERATIONS

Video surveillance systems that record images of individuals collect personal information and therefore are subject to the *Freedom of Information and Protection of Privacy Act*.

Video surveillance systems are to be clearly visible and marked by signage. This signage will state the following:

"This area is monitored by video surveillance to protect persons and property. For further information please contact the Regional District of Okanagan-Similkameen Freedom of Information & Protection of Privacy Head, 101 Martin Street, Penticton BC or 250-492-0237."

Video surveillance systems may be restricted to times when incidents are most likely to occur.

RESPONSIBILITIES

The FIPPA Head is responsible for:

- Ensuring the establishment of procedures for the use of video surveillance equipment, including the random audit of such procedures.
- Confirming signage is posted in accordance with the policy.
- Documenting the reason for implementation of a video surveillance system at the designated area.
- Maintaining a record of the location of the video camera equipment.
- Maintaining a list of personnel who are authorized to access and operate the system.
- Maintaining a record of the times when video surveillance will be in effect.
- Retaining and/or destroying any recorded information in accordance with this policy.

The Manager of Information Services or designate 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. Equipment specifications and standards are to follow corporate policy.

Regional District staff, contractors and/or consultants are responsible to review and comply with the policy in performing their duties and functions related to the operation of video surveillance systems. No employee, consultant or contractor shall knowingly or deliberately breach the policy.

PROCEDURES

Installation and Placement

- Video surveillance will not be installed in locations where confidential or private activities or functions which are normally carried out may be viewed.

- Cameras will not be directed to look through windows of buildings.

- Installation of video recording equipment should be restricted to areas identified as high crime areas, public nuisance areas or where Regional District or other property has been stolen or damaged in the past.

- Covert surveillance. ie. hidden cameras without signage, is not contemplated under this policy.

Video Surveillance Access, Use, and Disclosure

- Within the Regional District, access to video surveillance information is limited to the following individuals:
  - FIPPA Head or designate
  - Chief Administrative Officer

- Images recorded by a video surveillance system will be stored in a locked facility as determined by the FIPPA Head. Physical and computer-related security will be in place at all times to prevent unauthorized access to the recording equipment and images.

- Use of video surveillance information is to be for the purposes of investigation of an incident.

- Information Services staff may have access to surveillance systems for the purposes of system installation, maintenance, trouble-shooting, repair or upgrade. They will not access images recorded in the system unless that is necessary for these system purposes.

- Images may be disclosed to police or another law enforcement agency for the purposes of a law enforcement investigation or proceedings. The Regional District also may use and disclose images for its own investigations and proceedings. Images will otherwise be disclosed only to comply with a subpoena, warrant or order issued by a court, person or body in Canada with jurisdiction to compel disclosure.

- Any requests for access to incident-specific information must be referred to the FIPPA Head.

- Before introducing new video surveillance systems in any Regional District facilities, parks, or public spaces, the need for video surveillance will clearly meet the criteria of this Policy and the installation will conform to this Policy and be approved by the Board of Directors. When considering the proposal, staff will provide a report to the Board outlining the following:
    a. Incident reports respecting vandalism, theft, property damage, and safety concerns.
    b. Safety or security measures currently in place or attempted before installing video surveillance.
    c. Safety or security problems that video surveillance is expected to resolve.
    d. Areas and times of operation.
    e. Expected impact on personal privacy.
    f. How the video surveillance will benefit the Regional District or is related to Regional District business.
    g. How the benefits are expected to outweigh any privacy rights as a result of video surveillance.

- A privacy impact assessment will be conducted for each proposed surveillance system and for expansion of an existing system. This will be done before the report to the Board of Directors is prepared.

RESPONDING TO UNAUTHORIZED ACCESS, USE OR DISCLOSURE

If the Regional District has reason to believe that unauthorized access to, use or disclosure of video surveillance system images or data has or may have occurred, it will promptly investigate the matter and take reasonable steps to remedy the matter, including by retrieving any images or data and stopping the unauthorized access, use or disclosure. The Regional District also will assess whether any affected individuals should be notified and will notify them in appropriate cases where it is possible to do so. The Regional District will also assess, and implement, measures to prevent unauthorized access, use or disclosure in future.

RETENTION AND DESTRUCTION

Images and other data recorded by a video surveillance system will be retained for 30 days after recording. Images and data relating to an incident reported to or identified by the Regional District will be retained until the completion of all related investigations and proceedings are completed.

When recorded information which contains personal information about an individual reveals an incident and the Regional District uses this information to make a decision that directly affects the individual, the information will be retained for one (1) year after the decision has been made.

Images and other data that are to be disposed of will be destroyed in a secure and permanent manner.