



---

POLICY TITLE: Safety and Security Monitoring Policy  
POLICY #: R-002-007  
EFFECTIVE DATE: February 8, 2010  
ADOPTED BY COUNCIL ON: February 8, 2010  
RESOLUTION #: 40.02.10  
SUPERCEDES:

---

### **POLICY STATEMENT**

The Town of Sylvan Lake aims to provide a safe and secure environment for our staff and the general public in all Town owned facilities.

The Town of Sylvan Lake also recognizes the need to balance an individual's right to protection of privacy against the Town's duty to promote a safe environment for all citizens, and to protect Town property. The objective of security monitoring in Town owned buildings is to ensure the safety of the public and employees within the facility, as well as discourage those who may consider committing crimes.

### **PURPOSE**

The purpose of the Town of Sylvan Lake Safety and Security Monitoring Policy is to ensure that there are effective procedures in place to provide a safe environment for all staff and the general public; and to develop a security monitoring system policy that complies with the Freedom of Information and Protection of Privacy Act and ensure the consistency of monitoring measures.

### **DEFINITIONS**

**FOIP** means the Freedom of Information and Protection of Privacy Act, R.S.A. 2000, Chapter F-25

**Personal Information** is defined in Section 1 (1)(n) of FOIP as recorded information about an identifiable individual. It includes the individual's race, colour, national or ethnic origin; the individual's age or sex; the individual's inheritable characteristics; information about an individual's physical or mental disability; and any other identifiable characteristics listed in that Section.

**Reception Equipment** refers to the equipment or device used to receive or record the personal information collected through a surveillance system, including a video monitor.

**Record** is defined in Section 1 (1)(q) of FOIP as a record of information in any form and includes books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner, but does not include software or any mechanism that produces records.

**Storage Device** refers to a videotape, computer disk or drive, CD ROM or computer chip used to store the recorded visual images captured by a surveillance system.

**Security Monitoring System** refers to a mechanical or electronic system or device that enables continuous or periodic video recording, observing or monitoring of personal information about individuals in open, public spaces and public buildings.

**Town** means the municipal corporation of the Town of Sylvan Lake or where the context permits, the geographical area thereof.

## **GENERAL PRINCIPLES**

- A. Swipe card security access may be used to restrict public access from designated employee areas and employee entrances.
- B. All visitors to secured or restricted access areas in Town owned buildings will be required to sign in and out of a log book upon visiting.
- C. All meeting rooms, program rooms, storage rooms, janitorial rooms, etc. that are accessible from public areas are to remain locked when not in use.
- D. This Policy allows for the installation and use of security monitoring equipment in Town owned buildings only within the parameters and subject to the conditions established by the Policy.
- E. The use of security monitoring cameras is for public and employees safety (Section 33 of FOIP).
- F. All personal information will be the property of the Town of Sylvan Lake.
- G. The Government of Alberta, Guide to Using Surveillance Cameras in Public Areas, Revised 2004, and as further amended will be followed.

## **RESPONSIBILITIES**

- A. **Town Council** will approve the Policy and all subsequent amendments.
- B. **Chief Administrative Officer**, or designate, will be the custodian of the surveillance system program and ensure the Policy is complied with.

## **PROCEDURES**

The Chief Administrative Officer, or designate, will review and comply with this Policy in performing their duties and functions related to the operation of a security monitoring system.

Employees and/or contractors with access to a security monitoring system will swear an oath of confidentiality and sign written agreements regarding their duties under this Policy.

Employees who breach this Policy may be subject to disciplinary action.

If a contractor fails to comply with this Policy, it will be considered a breach of contract.

- 1 Recording equipment such as video cameras must be installed in identified public areas where monitoring is necessary and viable for detection or deterrence of activity.
  - 1.1 Recording equipment should not be positioned to monitor areas outside of a building or to monitor other buildings, unless necessary to protect external assets or to ensure personal safety.
  - 1.2 Cameras should not be directed to look through windows of offices.
  - 1.3 Equipment should not monitor areas where public and employees have a reasonable expectation of privacy (e.g. change rooms and adult washrooms). There may be situations where security monitoring equipment may need to be installed close to or at an entry to a children's washroom in a public building to monitor or deter potential criminal activity against children.
  - 1.4 The public must be notified using clearly written signs located in prominent areas and displayed at the perimeter of security monitoring areas, so the public has ample warning that security monitoring is or may be in operation before entering any area under surveillance.
- 2 Only authorized persons should have access to the systems controls and to its' reception equipment.
  - 2.1 Access to recorded information should be recorded in a log book and should include the date of the access, by whom, and for what purpose.
  - 2.2 Access to the storage devices and/or recorded information should only be granted because an incident has been reported or is suspected to have occurred.
  - 2.3 Request for access to recorded information by a non-designated individual must be requested in writing and authorization must be given in writing by the Chief Administrative Officer or designate.
- 3 Reception equipment must be located in a securely locked receptacle in a controlled access area, preferably off-site of the monitored area.
  - 3.1 Recorded information that reveals no incident or when no incident has been reported should be retained for 21 days.
  - 3.2 Recorded information that reveals an incident or may be required as part of an incident investigation should be retained for 365 days, or until law enforcement authorities or the courts advise otherwise.
- 4 A storage device release form stating who took the information or device, when, and under what authority, and if the information / device will be destroyed or returned after use must be completed before any storage device is disclosed to such authority.
- 5 Old storage devices must be securely disposed of by shredding, burning, or magnetically erasing the information.
- 6 The Chief Administrative Officer, or designate, shall review the use of security cameras in public places on a bi-yearly basis. The results of the review shall be properly documented, including a report to Council.

## **AUTHORIZED PERSONS**

Authorized persons for the purposes of this Policy refer to the Recreation, Parks & Culture Director, Recreation, Parks & Culture Manager, and the contracted security provider.



**Law Enforcement Disclosure**

Request for Disclosure under Section 40(1)(q) of the *Freedom of Information and Protection of Privacy Act*

In Accordance with section 40(1)(q) of the *Freedom of Information and Protection of Privacy Act*, the

\_\_\_\_\_ (Name of Public Body)

Requests disclosure of information pertaining to:

\_\_\_\_\_ (Name of Individual or Other Identifier)

\_\_\_\_\_ (General Description of Information Requested)

This information is required by this public body to assist in an investigation pursuant to:

\_\_\_\_\_ (Reference a Federal or Provincial Statute or Local Bylaw by Section or Description of Purpose)

**Requesting Official**

\_\_\_\_\_ Name

\_\_\_\_\_ Title

\_\_\_\_\_ Signature

\_\_\_\_\_ Badge Number (if applicable)

I, \_\_\_\_\_  consent to  refuse this disclosure of personal information.

**Authorized Disclosing Official**

\_\_\_\_\_ Name

\_\_\_\_\_ Title

\_\_\_\_\_ Signature

\_\_\_\_\_ Date

NOTE: This completed record may qualify for exemption to disclosure under section 20 of the *Freedom of Information and Protection of Privacy Act*.