VIDEO SURVEILLANCE POLICY

1.0 PURPOSE

Video surveillance, when utilized with other security measures, is an effective means of ensuring the security and safety of the Town of St. Marys facilities, the individuals who use them, and the assets housed within them. However, the need to ensure security and safety must be balanced with an individual's right to privacy.

The Town recognizes that video surveillance technology has a potential for infringing upon an individual's right to privacy. The Town's objective is to balance individuals' right to privacy with the need to enhance the safety of Town employees, clients/patrons, visitors and property.

Although a video surveillance system may be required for legitimate operational purposes, it must be used in accordance with the *Municipal Freedom of Information and Protection of Privacy Act* ("MFIPPA"), as well as the Ontario Human Rights Code and the Canadian Charter of Rights and Freedoms.

The use of hidden surveillance systems to capture images of individuals without their knowledge is what is referred to as "covert surveillance". This policy is in place to establish guidelines for video surveillance systems that are not covert in nature.

This Policy establishes guidelines for the use of video surveillance systems within and around Town owned and leased buildings and properties.

2.0 LEGISLATED REQUIREMENTS

This Policy reflects the provisions of the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), Ontario Human Rights Code and the Canadian Charter of Rights and Freedoms.

3.0 DEFINITIONS

Personal Information is defined in Section 2 of MFIPPA as recorded information about an identifiable individual, which includes, but is not limited to, information relating to an individual's race, colour, national or ethnic origin, sex and age. If a video surveillance system captures and/or displays these characteristics of an identifiable individual or the activities in which he or she is engaged, its contents will be considered "personal information" under the Act.

Receiving Equipment refers to the equipment or device used to receive or record the personal information collected through a video surveillance system, including a camera or video monitor or any other video, audio, physical or other mechanical, electronic or digital device.

Record, also defined in Section 2 of MFIPPA, means any record of information, however recorded, whether in printed form, on film, by electronic means or otherwise, and includes: a photograph, a file, a microfilm, a videotape, a machine-readable record, and any record that is capable of being produced from a machine-readable record under the control of the Town of St. Marys.

Storage Device refers to a server, videotape, computer disk or drive, CD ROM, DVD, computer chip or other device used to store the recorded data or visual, audio or other images captured by a video surveillance system.

Town refers to The Corporation of the Town of St. Marys

Video Surveillance System refers to a video, physical or other mechanical, electronic or digital surveillance system or device that enables continuous or periodic video recording, observing, or monitoring of personal information about individuals. In this policy, the term "video surveillance system" may refer to any component associated with capturing and/or recording the image of an individual.

4.0 PUBLIC CONSULTATION

The Town acknowledges the importance of public consultation when new or additional video surveillance systems are considered for municipally owned buildings and property. The extent of public consultation may vary depending on the extent of public access.

When new or additional video surveillance systems are being considered for municipally owned or operated buildings to which the public are invited, such as a library, recreation facilities, or Town Hall, as well as for open public spaces such as streets or parks, notice shall be provided at the site and on the Town's website with an opportunity for public feedback.

When new or additional systems are contemplated inside municipal buildings or staff parking lots where there may be a high risk to staff or clients/patrons, consultation shall not be required.

5.0 PROCEDURE

5.1 Privacy Assessment

Prior to the installation, or significant changes to, video surveillance equipment, departments must ensure that the use is justified on the basis of significant safety concerns, or for crime prevention. Effects that the video surveillance system may have on personal privacy must be minimized. The Clerks Department will be consulted during the privacy assessment.

5.2 Installation and Placement

Video surveillance equipment shall be installed in strictly controlled access areas that have been identified as requiring video surveillance and should never include areas where the public and employees have a reasonable expectation of privacy such as washrooms and change rooms. Adjustment of monitor position must be restricted to ensure that only designated areas are being monitored. The Clerk, or designate, with have final authorization for all installation and placement of video surveillance cameras.

5.3 Notification Requirements

The public must be notified of the existence of video surveillance equipment by clearly written signs prominently displayed at the entrances, exterior walls, and interior of buildings and/or perimeter of the video surveillance areas. Signage must satisfy the notification requirements under section 29(2) of Municipal Freedom of Information and Protection of Privacy Act and contain the following information:

- The legal authority for the collection;
- The principal purpose(s) for which the personal information is intended to be used; and
- The title, business address and business telephone number of someone who can answer questions about the collection.

5.4 Access to video surveillance footage

Circumstances which warrant viewing the information obtained through video monitoring are limited to incident and accident reports that occur at recreational facilities and other town properties, requests from a law enforcement agency and Municipal Freedom of Information requests.

Access to video surveillance systems and information obtained through video monitoring is strictly limited to the Information Technology Department and the Facilities Supervisor. The ability to approve copying recorded surveillance images is limited to the Clerk, or designate, and subject to obtaining the required authorization as set out in sections 2 through 4 below.

1. Surveillance images that have not been accessed for any purpose shall be automatically erased by the system according to the Records Retention – Video Surveillance Schedule. Surveillance images that have been accessed will be subject to a separate retention period in accordance with the Records Retention Schedule.
2. Requests for copies of recorded surveillance images shall be logged in the Video Surveillance Footage Request system and must include sufficient detail to address the following:
    - Contact Information, department, staff name, phone extension, e-mail address and date of request

- Date, time, description of event and camera location
- Type of Request:
    - Incident or Accident requests
    - Law Enforcement Investigation
    - Municipal Freedom of Information Request

3. Requests for copies of recorded surveillance images are authorized by the Clerk, or designate, prior to release.
4. Third party service providers and Law Enforcement officers granted access to records created as a result of video surveillance must agree that any records dealt with or created pursuant to the video surveillance program remain under the Town of St. Marys' control and are subject to the provisions of the Municipal Freedom of Information and Protection of *Privacy Act*.

5.5 Collection and Disposal

Personal Information collected by the Town pursuant to this Policy will be recorded and will only be used for the purposes set out herein, or as may otherwise be permitted or required by law. For example personal Information may be disclosed to the police or other law enforcement agencies in Canada to aid an investigation. In the event of a reported or observed incident, the review of recorded information may be used to assist in the investigation of the incident.

Disclosure of storage devices should be made to authorities only upon the presentation by the authorities of a warrant or court order for the same and upon completion of a form setting out the name of the individual(s) who took the storage device, under what legal authority, the date and whether the storage device will be returned or destroyed after its use by the authorities.

Storage devices containing personal information may be shared with third party service providers who have a need to access such information and only upon them entering into an agreement to keep such information confidential and handle the personal Information in accordance with the terms of this Policy and applicable law.

Upon receipt of a request and supply of video surveillance a second copy will be made of the information provided and stored in a secure place by the Clerk, or designate.

Storage devices (videos) that are not in use must be dated, labelled and stored securely. Access to the storage devices (videos) should only be by authorized personnel. Logs must be kept of all instances of access to, and use of, recorded material. The personal information recorded by video surveillance is subject to the Municipal Freedom of Information and

Protection of Privacy Act. Circumstances which warrant review of the information are limited to an incident that has been reported or to investigate a potential crime.

5.6 Records Retention

The retention periods for video surveillance images are governed by the receiving equipment, and are for thirty days. Requests from law enforcement agencies, a department manager, or MFIPPA request will be for the same duration as FOI request as governed by the Town of St. Marys Records Retention By-law.

6.0 DESIGNATED RESPONSIBILITIES

1. The Clerk, or designate, is responsible for ensuring that the implementation and administration of any video surveillance system is in accordance with this procedure and the Video Surveillance Policy. This includes:

- Documenting the reason for implementation of a video surveillance system for each designated area;
- Maintaining a record of the locations of the video surveillance equipment;
- Maintaining a list of personnel who are authorized to access and operate the system(s);
- Maintaining a record of the times when video surveillance will be in effect;
- Posting Notice of Collection(s); and
- Assigning a person responsible for the day to day operation of the system in accordance with the policy, procedures and directions that may be issued.

All requests must be submitted to the Clerk, or designate, for approval prior to purchasing and installing any video surveillance device.

2. The Information Technology Department, in conjunction with the Clerk, or designate, provide leadership, management and control over video surveillance application systems in order to ensure corporate strategies are supported, standardized, consistent and reliability.

3. The Clerk, or designate, is responsible for administering the requirements of Municipal Freedom of Information and Protection of Privacy Act and maintaining the following:

- a record of the locations of all video surveillance monitors;
- the location of postings of all Notices of Collection;
- a list of personnel who are authorized to access and operate the systems;
- a record of times when the video surveillance will be in effect); and
- control over the access and release of personal information recorded by the system. Maintain a log of all releases to law enforcement or FOI requests.

4. The video needs assessment will be assessed by the Clerk, or designate, to ensure compliance with the principles of Municipal Freedom of Information and Protection of Privacy Act and other relevant legislation.

5. Where the Town has a contract with a service provider, the contract shall provide that failure by the service provider to comply with the policy or the provisions of the Municipal Freedom of Information and Protection of Privacy Act and other relevant legislation is considered a breach of contract leading to penalties up to and including contract termination.

7.0 SIGN STANDARDS

Signage must satisfy the notification requirements under section 29(2) of Municipal Freedom of Information and Protection of Privacy Act and contain the following information:

- The legal authority for the collection;
- The principal purpose(s) for which the personal information is intended to be used; and
- The title, business address and business telephone number of someone who can answer questions about the collection.

The size of the sign shall fit the individual situation.

8.0 BREACH OF POLICY

Employees are responsible for compliance with this policy and shall be aware that any employee who breaches this policy may be subject to discipline up to and including dismissal.