Municipality of the District of Lunenburg
POLICY

Title: Video Surveillance	
MODL Policy No. 089	
Effective Date: November 24, 2020	Amended Date:

1. **Purpose:**

   1.1. The purpose of this Policy is to assist the Municipality in deciding whether collection of Personal Information by means of surveillance cameras is both lawful and justifiable, to assist the Municipality in understanding how privacy protection measures can be built into the use of a Video Surveillance System, and to ensure clarity for the public and employees of the Municipality with respect to the purposes for which a Video Surveillance System may be used. This Policy is also meant to:

   1.1.1. Ensure that any Video Surveillance System complies with the Municipal Government Act and the *Freedom of Information and Protection of Privacy Act*, as applicable.

   1.1.2. Ensure consistency of corporate surveillance undertaken by and within the Municipality.

   1.1.3. Outline the responsible and acceptable use of a Video Surveillance System as it is used for recording, monitoring and storing video on all properties owned or occupied by the Municipality of the District of Lunenburg (the "Municipality") and its affiliates for the express purposes of enhancing safety and security, preventing and deterring crime, identifying suspects, and gathering evidence.

2. **Scope:**

   2.1. This Policy applies to the Video Surveillance System and video records administered by the Municipality; it does not apply to video recordings gathered in other circumstances (e.g., recordings of Council Meetings).

   2.2. For the purpose of this Policy, the Municipality's environment includes all streets, public places, land and buildings that are owned or leased by the Municipality.

3. **Definitions:**

   3.1. **Authorized Personnel –** means personnel authorized by the Chief Administrative Officer to operate surveillance equipment and access live or recorded material.

   3.2. **CCTV –** means Closed Circuit TV, referring to the self-contained Video Surveillance System described in this Policy.

   3.3. **Chief Administrative Officer –** means the Chief Administrative Officer of the Municipality of the District of Lunenburg.

   3.4. **Clerk –** means the Clerk of the Municipality of the District of Lunenburg.

3.5. **Covert Surveillance -** refers to the secretive continuous or periodic observation of person, vehicles, and places or objects to obtain information concerning the activities of individuals.

3.6. **Director –** means director or department head of the Municipality of the District of Lunenburg.

3.7. **FOIPOP -** means the *Freedom of Information and Protection of Privacy Act*, SNS 1993, c. 5.

3.8. **MGA –** means *Municipal Government Act of Nova Scotia,* SNS 1998, c 18.

3.9. **Overt Surveillance -** refers to the non-secretive continuous or periodic observation of persons, vehicles, places or objects to obtain information concerning the activities of individuals.

3.10. **Personal Information –** means recorded information about an identifiable individual including the individual's name, address or telephone number, the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations, the individual's age, sex, sexual orientation, marital status or family status, an identifying number, symbol or other particular assigned to the individual, the individual's fingerprints, blood type or inheritable characteristics, information about the individual's health-care history, including a physical or mental disability, information about the individual's educational, financial, criminal or employment history, anyone else's opinions about the individual, and the individual's personal views or opinions, except if they are about someone else.

3.11. **Privacy Impact Assessment (PIA) -** is a process that can be applied to any public body for the purpose of determining the level of protection and security afforded to personal information that is collected, used or disclosed in a new modified information system. The security of information refers to the technical, physical and procedural measures taken to protect personal information from the time it is collected until a public body disposes of it.

3.12. **Reception Equipment -** refers to the equipment or device used to receive or record Personal Information collected through a surveillance system, including a video monitor.

3.13. **Record -** a record of information in any form and includes books, 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.

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

3.15. **Surveillance Equipment –** means any closed circuit television (CCTV) cameras and any other video/image monitoring and recording equipment systems used to monitor and record public, and restricted areas of property owned or leased by the Municipality.

3.16. **Municipality –** means the Municipality of the District of Lunenburg, and as referred to in this Policy shall include all departments and offices which make up the Municipality's administration, as well as any agency of the Municipality which has agreed to be bound by this Policy.

3.17. **Video Surveillance 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, public buildings or public transportation, and includes all recorded records collected by same.

4. **Policy Statement:**

4.1. Subject to this Policy, the Chief Administrative Officer has the sole authority to oversee and coordinate the use of any Video Surveillance System on Municipality Property.

4.2. The Municipality recognizes the need to balance an individual's right to protection of privacy against the Municipality's duty to promote a safe environment for all citizens, and to protect municipal property.

4.3. Any Video Surveillance System implemented under this Policy will be designed and operated in a manner that minimizes privacy intrusion and that is reasonably necessary to achieve the lawful goals of the Municipality.

4.4. The Municipality shall only use a Video Surveillance System for the following purposes:

4.4.1. to record unlawful acts and breaches of Municipality security;

4.4.2. to ensure public health and safety;

4.4.3. to prevent or deter unlawful acts and breaches of Municipality security; and

4.4.4. to aid law enforcement investigations.

4.5. Personal Information obtained by the Municipality through its Video Surveillance System will be used for security, health and safety and law enforcement purposes only. For greater clarity, a Video Surveillance System will not be used by the Municipality to monitor or evaluate Municipality employees, except as specifically authorized pursuant to Section 6.5.

4.6. All Personal Information obtained through the Video Surveillance System is confidential and will only be viewed or released as per Sections 6.6 & 6.7 of this Policy.

4.7. Authorized Personnel involved in the use of the Video Surveillance System will be appropriately trained and supervised in the responsible use of the Video Surveillance System.

4.8. All existing uses of a Video Surveillance System will be brought into compliance with this Policy within twelve months of the approval of this Policy.

5. **Responsibilities:**

5.1. **Municipal Council is responsible for:**

5.1.1. Approval of this Policy and any subsequent amendments.

5.2. **Chief Administrative Officer is responsible for:**

5.2.1. Overseeing and coordinating the use of any Video Surveillance System on Municipality Property.

5.2.2. Overseeing consistent adherence to this Policy.

5.2.3. The approval of the installation of Surveillance Equipment, including video cameras, on all Municipality owned and leased properties.

5.2.4. Monitoring the effectiveness of the Policy, and recommending changes to the Policy where considered appropriate.

5.3. **Authorized Personnel are responsible for:**

5.3.1. Establishing and maintaining an internal reporting network relating to control mechanisms

and advising the Chief Administrative Officer;

5.3.2. Budgeting for the cost of the Video Surveillance System requirements;

5.3.3. Ensuring Privacy Impact Assessments are conducted on new surveillance initiatives and on significant upgrades to existing surveillance systems;

5.3.4. Informing the Chief Administrative Officer of:

5.3.4.1. Proposed changes to authorized video surveillance which may affect the security of the Municipality;

5.3.4.2. Proposed changes in internal reporting network relating to proposed installation of new Surveillance Equipment that may be affected by this Policy.

5.3.4.3. Any new legislation pertaining to the use of video surveillance that must be incorporated into this Policy.

5.3.5. Reviewing all proposed changes to existing any Video Surveillance System and newly proposed systems to ensure that they meet all the requirements of this Policy.

5.4. **Employees are responsible for:**

5.4.1. Reviewing and complying with this Policy in performing their duties and functions related to the operation of a Video Surveillance System;

5.4.2. Attending training relating to this Policy, where available.

6. **Procedures:**

6.1. **Privacy Risk Assessment:**

6.1.1. The following steps/factors must be considered before a Video Surveillance System is implemented:

6.1.1.1. A Privacy Risk Assessment shall be conducted on the effects that a proposed Video Surveillance System may have on personal privacy and the ways in which any adverse or disproportionate effects can be mitigated;

6.1.1.2. A Security Threat Assessment (Schedule 1) shall be completed;

6.1.1.3. The use of the Video Surveillance System must be justified on the basis of verifiable, specific reports of incidents of crime or significant safety concerns;

6.1.1.4. A Video Surveillance System should only be considered after other measures of deterrence or detection have been considered and rejected as not workable;

6.1.1.5. The proposed design and operation of the Video Surveillance System should minimize privacy intrusion.

6.2. **Public Consultation:**

6.2.1. The Municipality acknowledges the importance of public consultation when a new or additional Video Surveillance System is considered for in public areas of Municipality-owned buildings and properties. The extent of public consultation may vary depending on the extent of public access to the building or property in question.

6.2.2. When a new or additional Video Surveillance System is being considered for open public spaces such as streets or parks, the Municipality shall consult with relevant stakeholders and the public to determine the necessity and acceptability. When a new or additional Video Surveillance System is being considered for Municipality owned or operated building to which the public are invited, such as a library, art gallery, or Municipal Office, notice shall be provided at the site with an opportunity for public feedback. When a new or additional Video Surveillance System is contemplated inside municipal buildings or parking lots where there may be a high security risk to staff or clients (or their property), consultation shall not be required.

6.3. **Design and Installation and Acceptable Use of Surveillance Equipment:**

6.3.1. Video surveillance currently recorded by the Municipality is stored directly to hard drives. Other methods of recording/storage are acceptable provided requirements of this Policy are met.

6.3.2. Given the open and public nature of the Municipality's facilities and the need to provide for the safety and security of employees and the general public who may be present at all hours of the day, a Video Surveillance System may operate at any time in a 24 hour period.

6.3.3. Reception Equipment such as video cameras may be installed in identified public areas where surveillance is a necessary and viable detection or deterrence activity.

6.3.4. Reception Equipment shall not be positioned, internally or externally, to monitor areas outside a building, or to monitor other buildings, unless necessary to protect external assets or to ensure personal safety. Cameras should not be directed to look through the windows of adjacent buildings.

6.3.5. Reception Equipment shall not monitor areas where the public and employees have a reasonable expectation of privacy e.g. showers, restrooms, change-rooms.

6.3.6. Consideration should be given to the use of surveillance being restricted to periods when there is a demonstrably higher likelihood of crime being committed and detected in the area under surveillance, such as when a building is ordinarily not occupied. Only Authorized Personnel shall have access to the Video Surveillance System's controls and to its Reception Equipment.

6.3.7. Reception Equipment should be in a controlled access area. Only Authorized Personnel shall have access to the Reception Equipment. Video monitors shall not be located in a position that enables public viewing.

6.4. **Public Awareness of Cameras:**

6.4.1. The public/individuals must be notified, using clearly written signs prominently displayed at the entrance to and the perimeters of surveillance areas, so the public has ample warning that surveillance is or may be in operation before entering any area under surveillance.

6.4.2. The notification signs must inform individuals of the legal authority for the collection of Personal Information; the principal purpose(s) for which the Personal Information is intended to be used; and the title, business address, and telephone number of the individual who can answer questions about the collection. (Notices should conform with the example in Schedule 2)

6.4.3. In addition, the notice may also be provided via the Municipality's Website, but will not be a substitute for signage in the areas captured by cameras.

6.5. **Covert Surveillance:**

6.5.1. Covert Surveillance will be used only in exceptional cases and only with the approval of the Chief Administrative Officer.

6.5.2. Where it appears that Covert Surveillance may be required, the Director will first conduct an assessment of the specific circumstances of the situation and make a recommendation to the Chief Administrative Officer.

6.5.3. The Director's assessment must demonstrate that Covert Surveillance is the only reasonable option in the circumstances, that the benefits derived from the information obtained outweigh the violation of privacy of the individuals observed and that the Covert Surveillance is consistent with the law.

6.5.4. Surveillance Equipment will be positioned in a way that minimizes unnecessary or collateral surveillance (e.g. in the case of ongoing computer theft problem, the camera will be positioned so that individuals will be recorded only if they approach the equipment of concern).

6.5.5. In all cases, Covert Surveillance will be time-limited.

6.6. **Request to View Live or Recorded Information:**

6.6.1. Only Authorized Personnel are permitted to operate Surveillance Equipment and access live or recorded material. However, in exceptional circumstances, the Chief Administrative Officer may designate other individuals to operate Surveillance Equipment and access live or recorded material on behalf of the Municipality.

6.6.2. Notwithstanding section 6.6.1, all requests by Municipality staff or law enforcement agencies to view live or recorded information must be made to and are subject to the approval of the Chief Administrative Officer. Where the permission is granted to view live or recorded information, that information must be viewed in the presence of Authorized Personnel.

6.6.3. All other requests to view recorded information must be made as a FOIPOP application to the Clerk or a production order under the *Criminal Code*.

6.6.4. The Municipality may, on its own initiative, in connection with reporting a suspected breach of any law, statute or ordinance disclose recordings to an applicable law enforcement agency, with the approval of the Chief Administrative Officer.

6.6.5. Access may be provided to live or recorded content from the Video Surveillance System in the event of an imminent or significant risk of harm to any individual, provided that such access would reasonably be expected to reduce, mitigate or investigate the risk of harm.

6.6.6. The Chief Administrative Officer and /or Clerk can be contacted by Email: info@modl.ca, Phone: 902-543-8181, or Mail: 10 Allée Champlain Drive, Cookville, NS B4V 9E4.

6.7. **Personal Access to Information Request Process:**

6.7.1. The Municipality recognizes that an individual whose Personal Information has been collected by a Video Surveillance System has a right to access his or her Personal Information under FOIPOP.

6.7.2. All inquiries related to or requests for video surveillance Records shall be directed to the Clerk. A person requesting access shall follow the procedure for obtaining access as per Section 6 of FOIPOP or Section 466 of the MGA. Processing of the request will be in accordance with the provisions of FOIPOP and the MGA, and take into consideration the protection of the privacy of third parties.

6.7.3. If the access to a video surveillance record is required for the purpose of a law enforcement investigation, the requesting Officer must complete the Municipality's Request Form and forward it to the Clerk.

6.8. **Custody, Control, of Video Records/Recordings**

6.8.1. The Municipality retains custody and control of all original video surveillance Records. Video Records are subject to the access and privacy requirements of FOIPOP and the MGA, which includes but is not limited to the prohibition of all Municipal Staff from access or use of information from the Video Surveillance System, its components, files, or data base for personal reasons.

6.8.2. Short retention periods minimize risk of improper use and disclosure. The Municipality's video recorders continually record for a period of up to 30 days depending on the recording device and technology before recording over data.

6.8.3. A Record of an incident will only be retained on an external storage device where it may be required as part of a criminal, safety, or security investigation or for evidentiary purposes. Such Record shall be copied from the hard drive onto an external storage device that cannot be over written and stored securely in a locked receptacle located in a controlled access area.

6.8.4. All storage devices that are not in use shall be stored securely in a locked receptacle located in a controlled access area. All storage devices that have been used shall be numbered and dated.

6.8.5. Access to storage devices shall only be by Authorized Personnel.

6.8.6. A logbook will be kept with regard to the use of each external storage device. The Authorized Personnel will take control of the external storage device in question and secure it in a sealed envelope with the time and date of the seizure and initials of the Authorized Personnel on the seal of the envelope.

6.8.7. A logbook shall be kept by Authorized Personnel with regards to the use of Surveillance Equipment. The logbook shall reflect all instances where:

6.8.7.1. Authorized Personnel or person designated under Section 6.6.1 views a recording;

6.8.7.2. A request is made to view a video Record/recording;

6.8.7.3. The Chief Administrative Officer denies a request to view a video Record/recording and the reasons for the denial;

6.8.7.4. The Chief Administrative Officer permits an individual to view a recording (this will include the reasons the request was granted, who viewed the recording, when, and identify the Authorized Personnel who was present during the viewing);

6.8.7.5. A request for Release of Record to Law Enforcement Agency (Schedule 3); and

6.8.7.6. The Chief Administrative Officer releases a Record to a Law Enforcement Agency.

6.8.8. Personal Information stored on an external storage device used for law enforcement, safety, or security investigation or for evidentiary purposes shall be retained for one year after its use.

6.8.9. Video Records requested by the RCMP for investigation purposes must be accompanied by a warrant or production order and shall be copied on an external storage device and kept secure by the Authorized Personnel until it is retrieved by the RCMP. Following the investigation and any corresponding legal action the RCMP shall be required to destroy the video record.

6.9. **Unauthorized/Inadvertent Disclosure:**

6.9.1. A person who becomes aware of any unauthorized or inadvertent disclosure of a video Record in contravention of this Policy should immediately notify the Chief Administrative Officer.

6.9.2. After this disclosure is reported the Chief Administrative Officer shall confirm the existence of the disclosure.

6.9.3. Upon confirmation of the existence of the disclosure, the Chief Administrative Officer will make reasonable efforts to mitigate the extent of the disclosure, take all reasonable actions to recover the video record, review the adequacy of privacy protection with the existing Policy, and, where required, notify the affected parties whose personal information was inappropriately disclosed.

6.9.4. Intentional unauthorized disclosure, or disclosure caused by negligence, by employees of the Municipality may result in disciplinary action up to and including dismissal. Intentional unauthorized disclosure, or disclosure caused by negligence, by service providers to the Municipality, may result in termination of their contract.

6.10. **Retention and Disposal of Video surveillance record:**

6.10.1. The Municipality's Video Surveillance System(s) continually record for a period of up to thirty (30) days depending on the recording device and technology, before recording over data. Video records shall not be retained on an external storage device unless in accordance with Section 6.8.3.

6.10.2. A Record retained on an external storage device in accordance to Section 6.8.3 shall be retained for a period of one (1) year.

6.10.3. The Municipality will take all reasonable efforts to ensure the security of Records in its control/custody and ensure their safe and secure disposal.

6.10.3.1. Storage devices must be securely disposed of by shredding, burning or magnetically erasing the information.

Clerk's Annotation for Official Policy Book

Date of Notice to Council Members: November 17, 2020

Date of Passage: November 24, 2020

I certify that this MODL Policy 089 " Video Surveillance" was adopted by Council as indicated above.

November 25, 2020

Municipal Clerk

Date

Schedule 1 – Surveillance Video Security Threat Assessment

To Determine the Requirements for a Video Surveillance System

Site Name:

Location:

Proposed Video Location:

Requestor:

Department:

Date:

1. Is there already a video surveillance and/or camera on site? If so, please describe and advise if their setup adheres to Municipality of the District of Lunenburg's Video Surveillance Policy. (use separate page if required).

2. Video surveillance must only be considered after other measures of deterrence or detection have been considered and rejected as unworkable.

   Have the following security counter measures been reviewed and rejected as unworkable?

Security Counter Measure	Reviewed (Y/N)	Rejected (Y/N)	Comments
a. Security Procedures	☐	☐	
b. Duress Buttons	☐	☐	
c. Door Locking Hardware	☐	☐	
d. Alarm System	☐	☐	
e. Access Control Panel	☐	☐	
f. Signage	☐	☐	
g. Security Guard/Officer Patrols	☐	☐	
h. Lighting	☐	☐	
i. Other	☐	☐	

3. The use of each video surveillance camera should be justified on the basis of verifiable, specific reports of incidents of crime of significant safety concerns.

   Are there any documented incidents of crime or significant safety concerns in any of the following formats?

Documentation Formats	Yes	No	Comments
a. Security Occurrence Reports	☐	☐	
b. Police Reports	☐	☐	
c. JOH&S Committee	☐	☐	
d. Internal Memos	☐	☐	
e. Other	☐	☐	

4. An assessment must be conducted on the effects that the proposed video surveillance system may have on personal privacy and the ways in which adverse effects can be mitigated.

   Have the following effects and mitigation strategies been considered?

Effects & Mitigation Strategies	Yes	No	Comments
a. Is proposed camera situated in an area that will minimize privacy intrusion?	☐	☐	
b. Is the proposed camera location one where the public and employees do not have a higher expectation of privacy (i.e. not in washroom or change room, etc.)?	☐	☐	
c. Is the location of the proposed video camera visible?	☐	☐	
d. Can the video surveillance be restricted to the recognized problem area?	☐	☐	
e. Is space allocated for proper video surveillance signage?	☐	☐	
f. Has a drawing been attached showing the camera location?	☐	☐	
g. Have any other effects/mitigation strategies been considered?	☐	☐	

5. The proposed design and operation of the video surveillance system should minimize privacy intrusion. Have the following design and operation factors been considered for each proposed camera location?

Measure to Mitigate Effects	Yes	No	Comments
a. Can the proposed camera be restricted through hardware or software to ensure that operators cannot adjust or manipulate cameras to overlook spaces that a threat assessment has not been completed for?	☐	☐	
b. Will the reception equipment be located in a strictly-controlled access area?	☐	☐	
c. Can the video surveillance monitor be installed in such a way that it will be hidden from public view?	☐	☐	
d. Other	☐	☐	

Comments:

Completed By (Print) Signature Position Title Date

Schedule 2 – Public Awareness of Cameras

This area may be monitored by (Closed Circuit TV Video Surveillance - CCTV)

The personal information collected by the use of the CCTV is collected under the authority of the *Municipal Government Act*, 1998. This information is used for the purpose of security, promoting public safety and the reduction of crime at this site.

Questions about the collection of the personal information may be addressed to the Chief Administrative Officer of the Municipality of the District of Lunenburg, 10 Allée Champlain Drive, Cookville, NS B4V 9E4.

Phone (902) 541-1320

Schedule 3 – Law Enforcement Officer Request Form

Release of Record to Law Enforcement Agency

(Under Section 27(m) of the *Freedom of Information and Protection of Privacy Act*)

To: Municipality of the District of Lunenburg

I, , of the
Print Name of Officer Print Name of Police Force

Request a copy of the following record(s):

Date: Time Period: to

Municipal Facility:

To aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result as duly noted on the attached warrant/production order.

I confirm that the record will be destroyed by the RCMP after use by the agency.

Signature of Officer Badge # Date

Return completed original forms to the Clerk at the Municipality of the District of Lunenburg, 10 Allée Champlain Drive, Cookville, NS B4V 9E4

I ☐ consent to; OR ☐ refuse; this release of record.
Chief Administrative Officer

Signature

Personal information is collected under the authority of the *Municipal Government Act* for the purpose of creating a record relating to the release of video surveillance record to a law enforcement agency. Questions about the collection of personal information may be addressed to the Chief Administrative Officer of the Municipality of the District of Lunenburg, 10 Allée Champlain Drive, Cookville, NS B4V 9E4 Phone: 902-543-8181.