The West Hants Regional Municipality recognizes the delicate balance between an individual's privacy and the need to protect the safety and security of the public. In respecting this balance, the Municipality is committed to integrating security best practices with the responsible use of technology. The information that is obtained through the use of video surveillance will be used for security and law enforcement purposes only. The Municipality ensures that the information captured on video surveillance is maintained as private, confidential, and secure, except in situations outlined by this policy.

1. PURPOSE

The purpose of this policy is to regulate the use of security cameras within the Municipality to address ongoing problems/challenges with undesirable and/or unlawful activities to enhance protection and increase security of the residents and visitors, employees or benefit these parties through the deterrence and detection of criminal activity including but not limited to theft, vandalism, property damage, illegal drug possession, trafficking and/or bomb threats. This policy applies to all streets and properties within the Municipality in the use of security camera monitoring and recording.

In this policy, video surveillance includes any associated audio recordings captured as part of the video recording process. Where warranted, the Municipality may use video surveillance systems in and around its facilities, properties, employees, and vehicles. For clarity, "video surveillance records" do not include traffic monitoring systems, webcams, or other media which may stream or broadcast video but have no recording function in operation.

The Municipality will develop a Video Surveillance System Policy that complies with the Freedom of Information and Protection of Privacy Act.

2. DEFINITIONS

Term	Definition
Access & Privacy Officer	The responsible officer under Part XX of the Municipal Government Act, S.N.S. 1998, c. 18, or his or her delegate.
Archive	The process of moving data that is no longer actively used to a separate storage device for long-term retention.
Authorized Personnel	Personnel authorized by the Chief Administrative Officer to operate surveillance equipment and access live or recorded material.
Chief Administrative Officer	The Chief Administrative Officer of the West Hants Regional Municipality

Designated Alternate	Person(s) designated by the Chief Administrative Officer
Consistent purpose	Means personal information collected by the Municipality used for the purpose for which it was collected or similar consistent purposes when carrying out Municipal business. The individual to whom the information relates might reasonably expect the use/disclosure of their personal information for those consistent purposes.
Control of Record	Means the keeping, care, watch, preservation or security of a record for a legitimate business purpose. While physical possession of a record may not always constitute custody, it is the best evidence of custody.
Destruction	Is the physical or electronic disposal of records or data by means of disposing, recycling, deletion or overwriting. This also includes the destruction of records or data residing on computers and electronic devices supplied or paid for by the Municipality.
Digital Video Recording Equipment	Means any type of video recording and reception equipment used as part of the video surveillance system.
Freedom of Information process	Means a formal process for access to records made under the Freedom of Information and Protection of Privacy Act (FOIPOP).
Information and Privacy Commissioner	Means the Office of the Information and Privacy Commissioner of Nova Scotia (OIPC). The OIPC hears appeals of decisions made by the public body, issues binding orders, conducts privacy investigations and has certain powers relating to the protection of personal privacy ad set out in the Freedom of Information and Protection of Privacy Act (FOIPOP).
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.

Privacy Impact Assessment (PIA)	The process 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.
Personal Breach	Means an incident involving unauthorized disclosure of personal information, including it being stolen, lost or accessed by unauthorized persons.
Record	Means information however recorded or stored, whether in printed form, on film, by electronic means or otherwise, and included documents, financial statements, minutes, accounts, correspondence, memoranda, plans, maps, drawings, photographs and films; includes transitionary records.
Retention Period	Is the period of time during which a specific record series must be kept before records in that records series may be disposed of.
Service Provider	Means a video service provider, consultant or other contractor engaged by the Municipality in respect to video surveillance system.
Video Surveillance System	Means a mechanical or electronic system or device that enables continuous or periodic recording, and which may have the capacity of recording audio in addition to video images, observing or monitoring of Personal Information about individuals in open spaces, public buildings, or public transportation, and includes all recorded video collected by same.

3. Policy Statement:

3.1 Subject to this Policy, the Chief Administrative Officer or "designated alternate" has the sole authority to oversee and coordinate the use of any Video Surveillance System on Municipal Property.

3.2 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.

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

- detecting, deterring, and investigating unlawful activities, which may include possible contraventions of any federal or provincial law or municipal by-laws;
- to ensure public health and safety;
- to safely monitor System Facility Operations
- to prevent or deter unlawful acts and breaches of Municipality security; and
- to investigate and resolve personal injury, damage to assets, and other legal claims;
- to aid law enforcement investigations.

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

3.5 Personal Information obtained by the Municipality through its Video Surveillance System will be used for security, health and safety and law enforcement purposes only.

3.6 All Personal Information obtained through the Video Surveillance System is confidential and will only be viewed or released as per Sections 6.4, 6.5 & 6.6 of this Policy.

3.7 Authorized Personnel involved in the use of the Video Surveillance System will be appropriately trained in the responsible use of the Video Surveillance System and Freedom of Information and Protection of Privacy legislation.

3.8 Ownership of the video surveillance records shall remain with the Municipality; except in instances where video surveillance records are transferred into the custody of a law enforcement agency.

3.9 All existing uses of a Video Surveillance System will be brought into compliance with this Policy.

4. Responsibilities

4.1 Municipal Council is responsible for:

- Approval of this Policy and any subsequent amendments.

4.2. Chief Administrative Officer or alternate designate is responsible for:

- Overseeing, coordinating the use of any Video Surveillance System on Municipality Property and compliance with the policy.
- Overseeing consistent adherence to this Policy.
- The approval of the installation of Surveillance Equipment, including video cameras, on all Municipality owned and leased properties.
- Monitoring the effectiveness of the Policy and recommending changes to the Policy where appropriate.

4.3. Authorized Personnel/Employees are responsible for:

- Establishing and maintaining an internal reporting network relating to control mechanisms and advising the Chief Administrative Officer or alternate designate;
- Budgeting for the cost of the Video Surveillance System requirements;
- Ensuring Privacy Impact Assessments are conducted on new surveillance initiatives and on significant upgrades to existing surveillance systems;
- Informing the Chief Administrative Officer or alternate designate of:
    - Proposed changes to authorized video surveillance which may affect the security of the Municipality;
    - Proposed changes in internal reporting network relating to proposed installation of new Surveillance Equipment that may be affected by this Policy.
    - Any new legislation pertaining to the use of video surveillance that must be incorporated into this Policy.
    - 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. Employees are responsible for:

- Reviewing and complying with this Policy in performing their duties and functions related to the operation of a Video Surveillance System;
- Attending training relating to this Policy, when/where available.

6. Procedures:

6.1. Privacy Impact Assessment:

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

6.1.1 A Privacy Impact 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;

6.1.2 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;

6.1.3. All attempts will be made to the proposed design and operation of the Video Surveillance System to minimize privacy intrusion within public spaces and facilities.

6.2. Design and Installation and Acceptable Use of Surveillance Equipment:

6.2.1. 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.

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

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

6.2.4. 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.

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

6.2.6. 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.

6.3. Public Awareness of Cameras

6.3.1. 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 are aware that surveillance is or may be in operation before entering any area.

6.3.2. A QR code will be place on notification signs to direct individuals to an online resource explaining 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.

6.3.3. 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.

6.4. Request to View Live or Recorded Information

6.4.1. 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.

6.4.2. Notwithstanding section 6.4.1, all requests outside of the Municipality or law enforcement agencies to view live or recorded information must be made through a formal FOIPOP application to the Clerk and are subject to the approval of the Chief Administrative Officer or alternate designate. Where the permission is granted to view live or recorded information, that information must be viewed in the presence of Authorized Personnel.

6.4.3. 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 or alternate designate.

6.4.5. 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.

6.5 Personal Access to Information Request Process:

6.5.1. 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.

6.5.2. 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.

6.5.3. If access to a video surveillance record is required for the purpose of a law enforcement investigation, the requesting Officer must contact the Chief Administrative Officer or designate for approval and complete the Municipality's Request Form for record keeping purposes.

6.6 Custody, Control, of Video Records/Recordings

6.6.1. 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.

6.6.2. The Municipality strives to maintain video recordings for a minimum period of up to 30 days; however as new technologies become available, greater retention periods are achievable.

6.6.3 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 6.7.3.

6.6.4. 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.

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

6.6.6. 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.

6.6.7 A log must be maintained for all requests for access to video surveillance records and retained for the period set out in the Municipal Records Management Policy. The log must include:

i. the date and time range of the recorded video requested;
ii. the date of the request;
iii. the name of the requester;
iv. the file / case number, where applicable; and
v. the name of the agency (if applicable)

The logbook shall reflect all instances where:

6.6.7.1. Authorized Personnel or person(s) designated under Section 4.3 views a recording;

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

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

6.6.7.4. The Chief Administrative Officer or alternate designate 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).

6.6.8. Personal Information stored on an external storage device used for law enforcement, safety, or security investigation or for evidentiary purposes shall be transferred to an external hard drive and provided to the law enforcement agency, who assumes responsibility for the record(s) and the destruction of the record after its intended purpose has been fulfilled.

6.7 Unauthorized/Inadvertent Disclosure

6.7.1. 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 or alternate designate.

6.7.2. After this disclosure is reported the Chief Administrative Officer or alternate designate shall confirm the existence of the disclosure.

6.7.3. Upon confirmation of the existence of the disclosure, the Chief Administrative Officer or alternate designate 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.

6.7.4. 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.

6.8 Retention and Disposal of Video surveillance record:

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

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

I, Deanna Snair, Municipal Clerk of the West Hants Regional Municipality, in the Province of Nova Scotia, do hereby certify that this is a true copy of the Policy as adopted by the Council of the West Hants Regional Municipality at a meeting duly called and held on the **25th** day of **March 2025**.

Deanna Snair

Deanna Snair, Municipal Clerk

Adoption	
Notice to Council:	*Date: November 14, 2023*
Approval:	*Date: November 28, 2023*
Description: Initial approval of Video Surveillance Policy RCOFN-014.00	
Amendment	
Notice to Council:	*Date: March 11, 2025*
Approval:	*Date: March25, 2025*
Description: First Amendment of Video Surveillance Policy RCOFN-014.00 to remove barriers identified by RCMP when investigating incidents, provide additional clarity in areas within the policy, add a designate for when the Chief Administrative Officer may not be available and add an increased level of compliance within the policy.	

Schedule 1

Release of Record to Law Enforcement Agency
(Under Section 27(m) of the Freedom of Information and Protection of Privacy Act)

To: West Hants Regional Municipality

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 West Hants Regional Municipality, 76 Morison Drive PO Box 3000, Windsor, N.S. B0N 2T0

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 West Hants Regional Municipality, 76 Morison Drive PO Box 3000, Windsor, N.S. B0N 2T0