Town of Digby
Administrative Policy # 2017-12
Video Surveillance System Policy

1. Purpose:

1.1. Develop a Video Surveillance System Policy that complies with the Freedom of Information and Protection of Privacy Act.

1.2. Ensure consistency of corporate surveillance.

1.3. Outline the responsible use of Video Surveillance System as it is used for recording, monitoring and storing video on all properties owned or occupied by the Town of Digby (the "Town") 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 Town; 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 Town environment includes all streets, public places, land and buildings that are owned or leased by the Town.

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. **Chief Administrative Officer –** means the Chief Administrative Officer of the Town of Digby.

3.3. **Clerk –** means the Clerk of the Town of Digby.

3.4. **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.

3.5. **Director –** means director or department head of the Town of Digby, and includes RCMP Staff Sergeant, or Corporal.

3.6. **FOIPOP -** means the Freedom of Information and Protection of Privacy Act. 1993, c. 5, s. 1.

3.7. **MGA –** means Municipal Government Act of Nova Scotia

3.8. **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.

3.9. **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.

3.10. **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.

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

3.12. **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.

3.13. **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.

3.14. **Surveillance Equipment –** means any closed circuit television 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 Town of Digby.

3.15. **Town –** means the corporation of the Town of Digby, and as referred to in this policy shall include all departments and offices which make up the Town of Digby's administration, as well as any agency of the Town of Digby which has agreed to be bound by this policy.

3.16. **Video Surveillance System (CCTV) -** refers to a mechanical or electronic system or device that enable 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 all Video Surveillance Systems on Town of Digby Property.

4.2. The Town recognizes the needs 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.

4.3. Video Surveillance Systems under this policy will be designed and operated in a manner that minimizes privacy intrusion and that is absolutely necessary to achieve the lawful goals of the Town.

4.4. Video Surveillance Systems are to be used by the Town to record unlawful acts and breaches of Town security, and public health and safety, to prevent or deter such activities; information obtained from Video Surveillance Systems are also used to aid law enforcement investigations.

4.5. Personal information obtained through the Town's Video Surveillance Systems will be used for security, health and safety and law enforcement purposes only. For greater certainly, Video Surveillance Systems will not be used for employee performance purposes, 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. This Policy is intended to assist the Town in deciding whether collection of personal information by means of surveillance camera is both lawful and justifiable, and if so, in understanding how privacy protection measures can be built into the use of surveillance system.

4.8. It is recognized that each situation has unique needs and practices. While these requirements will remain, it is necessary to standardize Town procedure in the order that all citizens have an expectation of consistency, regardless where the equipment is installed.

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

4.10. All existing uses of Video Surveillance Systems will be brought into compliance with this policy within twelve months of the approval of this policy.

5. Responsibilities:

5.1. **Town 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. Oversee and coordinate the use of all Video Surveillance Systems on Town of Digby Property.

5.2.2. Ensuring the requirements of this Policy are adhered to.

5.2.3. The approval of the installation of video cameras on all Town owned and leased properties.

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

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

5.3.1. Establish and maintain an internal reporting network relating to control mechanisms and advise the Chief Administrative Officer;

5.3.2. Budget for the cost of the video surveillance requirements;

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

5.3.4. Inform the Chief Administrative Officer of:

5.3.4.1. Proposed changes to authorized video surveillance which may affect Town Security;

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

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

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

5.4. **Employees are responsible for:**

5.4.1. Review and comply with this Policy in performing their duties and functions related to the operation of a surveillance system;

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

6. Procedures:

6.1. Privacy Impact Assessment (PIA):

6.1.1. A PIA shall be conducted on the effects that the proposed video surveillance system may have on personal privacy and the ways in which any adverse effects can be mitigated;

6.1.2. The following steps must be considered:

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

6.1.2.2. The use of video surveillance cameras should be justified on the basis of verifiable, specific reports of incidents of crime or significant safety concerns;

6.1.2.3. A video surveillance system should only be considered after other measures of deterrence or detection have been considered and rejected as workable;

6.1.2.4. The proposed design and operation of the video surveillance system should minimize privacy intrusion.

6.2. Public Consultation:

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

6.2.2. When new or additional video surveillance installations are being considered for open public spaces such as streets or parks, the Town shall consult with relevant stakeholders and the public to determine the necessity and acceptability. When new or additional video surveillance are being considered for Town owned or operated buildings to which the public are invited, such as a library, art gallery, or Town Hall, notice shall be provided at the site with an opportunity for public feedback. When new or additional systems are contemplated inside town buildings or parking lots where there may be a high security risk to staff or clients, consultation shall not be required.

6.3. Designing and Installing Surveillance Equipment:

6.3.1. Video surveillance currently recorded by the Town 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 Town's facilities and the need to provide for the safety and security of employees, clients and the general public who may be present at all hours of the day, the video surveillance systems 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. Equipment shall not monitor areas where the public and employees have a reasonable expectation of privacy e.g. showers, restrooms.

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. Only authorized personnel shall have access to the system's controls and to its reception equipment.

6.3.7. Reception equipment should be in a controlled access area. Only the 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 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.

6.4.1.1. The notification requirements of the 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. (Schedule 2)

6.4.2. In addition, the notice may also be provided via the Town of Digby Website.

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 a 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 available option in the circumstances, that the benefits derived from the information obtained far outweigh the violation of privacy of the individuals observed and that the covert surveillance is not otherwise in violation of the law.

6.5.4. Surveillance equipment will be positioned in a way that minimizes unnecessary 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 (RCMP members) to operate surveillance equipment and access live or recorded material.

6.6.2. Notwithstanding section 6.6.1 all requests by Town of Digby 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.

6.6.4. The Chief Administrative Officer and /or Clerk can be contacted by Email: townhall@digby.ca, Phone: 902-245-4769, or Mail: PO Box 579 Digby NS. B0V 1A0.

6.7. Personal Access to Information Request Process:

6.7.1. The Town 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.

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 Town's Law Enforcement Officer Request Form and forward it to the Clerk.

6.8. Custody, Control, of Video Records/Recordings

6.8.1. The Town of Digby 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 Town 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 Town'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 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. The record of incident 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), and

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

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

6.10. Retention and Disposal of Video surveillance record:

6.10.1. The Town of Digby Video Surveillance System(s) continually record for a period of up to (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 (1) one year.

6.10.3. The Town 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: September 18, 2017

Date of adoption: October 2, 2017

Policy effective date: October 2, 2017

I certify that this **Video Surveillance System Policy** was adopted by Council as indicated above.

Edwin L. Oesinger — October 3, 2017

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 set-up adheres to the Town of Digby's Video Surveillance System Policy. (use Separate Page if Required)

   _____
   _____
   _____

2. Video Surveillance should only be considered after other measures of deterrence or detection have been considered and rejected as unworkable. Have the following security counter measures been considered and rejected as unworkable?

Security Counter Measure	Yes	No	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) H&S Committee Minutes	☐	☐	_____
d) Internal Memos	☐	☐	_____
e) Other	☐	☐	_____

4. An assessment should 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) The location of the proposed camera is 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) Other	☐	☐	_____

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) Is the reception equipment going to be located in a strictly controlled access area?	☐	☐	_____
c) Can Video Surveillance Monitor be installed in such a way that it will be hidden from public view?	☐	☐	_____
d) Other	☐	☐	_____

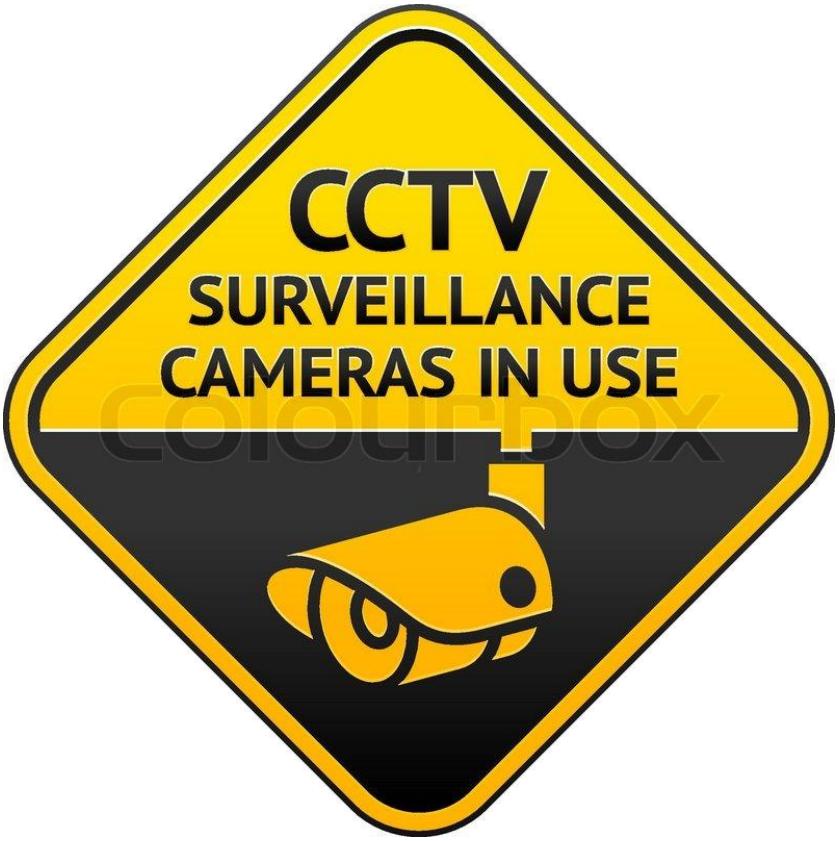
Comments:

_____
_____
_____
_____

_____	_____	_____	_____
Completed by (Print)	Signature	Date	Position Title

Schedule 2 – Public Awareness of Cameras

NOTICE



This area may be monitored by Video Surveillance Cameras (CTTV)

The personal information collected by the use of the CTTV 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 Town of Digby, PO Box 579, 147 First Avenue, Digby NS B0V 1A0 Phone: 902-245-4769

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: Town of Digby

I, _____, of the _____
Print Name of Police 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.

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 Digby Town Hall 147 First Avenue Digby NS. B0V 1A0

I _____ ☐ consent to; ☐ 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 a video surveillance record to a law enforcement agency. Questions about the collection of the personal information may be addressed to the Chief Administrative Officer of the Town of Digby, PO Box 579, 147 First Avenue, Digby NS B0V 1A0 Phone: 902-245-4769