TOWN OF CORNWALL
RESOLUTION

DATE:	**September 27, 2023**
COMMITTEE:	**UTILITY (U)**
MOTION NUMBER:	**U 08-2023 ~ Camera Policy**
MOTION CARRIED	√ 5-0
MOTION LOST	
MOTION WITHDRAWN	
Moved by Councillor	**Elaine Barnes**
Seconded by Councillor	**Jill MacIsaac**

Whereas: The Town of Cornwall has been increasing the number of security cameras it has in use in the community and recognizes that a balance needs to be struck between the use of such equipment and the reasonable expectation of privacy of members of the community and visitors;

And Whereas: The Town recognizes the need for a policy to govern the use of security cameras to ensure this balance is struck;

Therefore, be it Resolved: That the Town of Cornwall adopt the Draft Security Camera Policy previously considered by Councillors and attached to this resolution.

TOWN OF CORNWALL
SECURITY CAMERA POLICY

1. INTRODUCTION

1.1 The Town of Cornwall (the "Town") recognizes the delicate balance between (1) the need to protect the safety and security of the public, Town employees and Town property and (2) an individual's right to be free from invasion of privacy. In respecting this balance, the Town is committed to integrating security best practices with the responsible use of technology.

1.2 The Town is the owner of significant public assets that represent a large investment of public money; the Town will make use of security camera systems to better protect the security of the public, employees, assets, and property.

1.3 The use of security cameras is a necessary and reasonable protection of property against vandalism, theft, damage, and destruction. Information obtained from security camera systems can be used by the Town in potential proceedings.

1.4 The use of security camera systems will be conducted in a professional, ethical, and legal manner. Personnel will be appropriately trained and supervised in the responsible use of the technology. Violations of the procedures referenced in this Policy can result in disciplinary action consistent with the rules and regulations governing employes of the Town, or as prescribed by law.

2. PURPOSE

2.1 The purpose of this policy (the "Policy") is to set guidelines for the establishment and use of Security Camera Systems on Town property. Specifically, this Policy addresses requirements and responsibilities with respect to:

a) the establishment of Security Camera Systems;
b) the operation of Security Camera Systems;
c) the use of information obtained through Security Camera Systems; and
d) custody, control and access to records created through Security Camera Systems.

3. POLICY

3.1 Security Camera Systems will only be installed and used for one or more of the following purposes:

a) safety and welfare of the public;
b) safety and welfare of the Town's Employees;
c) protection of Town property; or
d) preventing unauthorized use of Town's facilities.

4. DEFINITIONS

In this Policy:

"Authorized Employee" means an individual authorized by the Chief Administrative Officer or their designate.

"Camera" means video technology of any kind whatsoever that enables the continuous or periodic observation, monitoring or recording of individuals, and includes any related audio information.

"Employee" means an employee of the Town and any person who volunteers for the Town on an ongoing basis.

"CAO" means the Chief Administrative Officer of the Town.

"Security Camera System" means a Camera, or set of Cameras, that are used to monitor a particular area.

"Security Information" means any information, including without limitation video, audio, and still images, produced or captured by a Security Camera System.

"Specific Issue" means the issue giving rise to the need for a Security Camera System as set out in the Policy.

5. APPLICATION

5.1 This Policy applies to security camera systems on all municipal property and municipal assets.

5.2 This Policy does not apply to security camera systems or other recording devices used by the RCMP, or to the digital records produced as a result of the operation of such devices and their use by the RCMP.

5.3 This Policy does not apply to security camera system installed for the purpose of traffic management, including for the enforcement of traffic laws or regulations.

6. REQUIREMENTS

6.1 A Security Camera System must:

a) only be established and used when:
   i) it is demonstrably necessary to address a Specific Issue;
   ii) it is likely to be effective in addressing the Specific Issue;
   iii) the loss of privacy is proportional to the need to address the Specific Issue; and
   iv) there are no feasible less privacy-invasive ways of addressing the Specific Issue;

b) be accessible to as few Employees as necessary to address the Specific Issue;

c) only be accessible by Authorized Employees, the CAO, the Town's solicitor, and other individuals whose access is deemed necessary by the CAO;

d) only be used to monitor Town assets and property as set out in the Policy;

e) where possible, restrict the periods when observing, monitoring or recording will occur to times when there is a demonstrably higher likelihood of the Specific Issue occurring; and

f) not be used in areas where the public and Employees have a higher expectation of privacy (e.g. change rooms and washrooms).

7. SIGNAGE

7.1 Signs must be posted at all public entrances to a facility where Security Camera Systems are used and in prominent places where the surveillance is occurring. At a minimum, signs must contain the following information:

a) a statement that images are being monitored and/or recorded;
b) that the Town is responsible for the Security Camera System.

8. CUSTODY AND CONTROL OF DIGITAL RECORDINGS

8.1 The Town is responsible for the custody and control of digital recordings.

8.2 Security camera systems will be setup to ensure recordings are cleared or overwritten on a regular basis. Normally, systems will be setup to maintain records for up to 30 days. In some cases, system capacity may limit the time records are maintained. In the event that authorized employees need to remove information from the system (still images, video footage) for authorized reasons, the resulting record(s) will be maintained for a minimum of one (1) year.

8.3 Security camera system recording equipment shall be located such that only designated individuals authorized by the CAO or Contractor may access the equipment.

8.4 All wireless transmissions of digital recordings shall be encrypted.

8.5 The CAO or their designate, may designate employees or contractors who are authorized to access security camera systems and digital recordings for the purpose of monitoring a security camera system at a given location.

8.6 The CAO or their designate, may designate employees or contractors to:

a) retrieve, download, view and/or secure a digital recording;
b) perform maintenance and repairs on security camera systems.

9. THIRD PARTY ACCESS TO DIGITAL RECORDINGS

9.1 Law enforcement personnel (RCMP) may request access to digital recordings for law enforcement or investigative reasons by contacting the CAO or their designate.

9.2 Third parties may request access to digital recordings in the following manner:

a) an application pursuant to FOIPOP;
b) as part of a legal action against the Municipality; or
c) by way of a court order or otherwise as provided for by law.

9.3 Applications for records must be received within twenty-five (25) days from the requested date of incident to allow designated employees time to preserve information before information is cleared or overwritten as per section 8.2.

9.4 A statutory body may request access to digital recordings pursuant to its legislative authority.

9.5 A third party who is given access to digital recordings may be required to acknowledge their duties, obligations and responsibilities with respect to the confidentiality, use and disclosure of the digital recordings in writing.

9.6 Any unauthorized access to digital recordings or security camera systems shall be reported to the CAO for investigation.

9.7 Any employee who provides digital recordings to unauthorized parties, either as a result of intentional wrongful disclosure or disclosure caused by negligence, are subject to disciplinary action, up to and including dismissal.

9.8 Any contractor who provides digital recordings to unauthorized parties, either as a result of intentional wrongful disclosure or disclosure caused by negligence, are subject to termination of their contract.

10. TRAINING

10.1 When Applicable and appropriate, the policy and guidelines will be incorporated into training and orientation programs of the Town.