ATTACHMENT A

CITY OF NANAIMO
THE HARBOUR CITY

COUNCIL POLICY

RCRS Secondary:	GOV-02	**Effective Date:**	
Policy Number:	COU-223	**Amendment Date/s:**	
Title:	Video Surveillance of Civic Property	**Repeal Date:**	
Department:	Legislative Services	**Approval Date:**	

PURPOSE:

To establish guidelines for the use of video surveillance to enhance the security and safety of persons, properties, things, and activities that are in or on facilities owned or occupied by the City of Nanaimo and used for public civic purposes.

DEFINITIONS:

Personal Information	Means recorded information about an identifiable individual other than business contact information
Privacy Impact Assessment (PIA)	Means a process which assists organizations in identifying and managing the privacy risks arising from new projects, initiatives, systems, or processes. PIAs must be approved by the FOI Head.

SCOPE:

This Policy applies to any video surveillance system operated by or for the City of Nanaimo that collects personal information in any form. This Policy does not apply to video surveillance conducted by the Royal Canadian Mounted Police ("RCMP"), who are subject to the *Privacy Act* (Canada).

POLICY:

1.0 PRINCIPLES

1.1 As an owner of significant public assets that represent a large investment of public money, the City of Nanaimo wishes to make use of video surveillance systems to better protect the security of its people, assets and property.

1.2 The City acknowledges that the use of video surveillance may, in some circumstances, represent an intrusion into personal privacy and does not wish to impair personal privacy any more than is warranted to provide necessary and reasonable protection of its property against crimes such as vandalism, theft, damage and destruction. Video surveillance recordings can be used by the City for an investigation and as evidence in any civil proceedings.

1.3 Video surveillance systems will be installed only after other less intrusive security methods have been considered or attempted and have been found to be insufficient or unworkable.

1.4 Before implementing a new surveillance system or expanding/replacing an existing video surveillance system, a Privacy Impact Assessment (PIA) must be completed and the reason for introducing or expanding the video surveillance is to be clearly

articulated in writing. Approval for the introduction or expansion of video surveillance must be granted by the Chief Administrative Officer (CAO) or designate.

1.5 Existing video surveillance systems that were installed prior to the requirement of a PIA may have existing components repaired and replaced without the completion of a PIA provided the quality, location, and viewing angle of the cameras are not changed in any way. Prior to upgrading an existing video surveillance system a PIA must be approved by the Freedom of Information Head.

2.0 DESIGNATED RESPONSIBILITIES

2.1 The CAO is responsible for approval of the introduction of video surveillance programs.

2.2 The Freedom of Information Head is responsible for approval of Privacy Impact Assessments related to video surveillance programs.

2.3 The General Manager or Director of each department is responsible for ensuring procedures, as established by policy, for the use, access, and storage of video surveillance equipment, including the random audit of such procedures, are in accordance with this policy. This responsibility can be designated to a member of the Senior Leadership Team.

2.4 The Director of IT is responsible for overseeing the life cycle management of authorized video surveillance systems including, but not limited to, specifications, installation, maintenance, replacement, disposal, and related requirements. Equipment specifications and standards are to follow corporate policy.

2.5 The Manager of Bylaw Services is responsible for providing access to the data in accordance with this policy.

2.6 City employees and service providers shall review and comply with the policy in performing their duties and functions related to the operation of video surveillance systems. City employees may be subject to discipline if they knowingly or deliberately breach the policy.

2.7 Service providers having access to video surveillance information must be bonded and sign a privacy protection schedule limiting access to, copying and disclosure of personal information and requiring compliance with this Policy. Breach of the privacy protection schedule may lead to penalties up to and including contract termination.

3.0 VIDEO SURVEILLANCE REQUIREMENTS AND USE

3.1 Before introducing video surveillance in any City owned facility the need for video surveillance must clearly meet the criteria of this Policy and the installation must conform to this Policy and be approved by the CAO in consultation with the City's Freedom of Information Head. The CAO and FOI Head, when considering the proposal, will consider the following:

(a) Incident reports respecting vandalism, theft, property damage, liability and safety concerns.
(b) Safety or security measures in place currently or attempted before installing video surveillance.
(c) Safety or security problems that video surveillance is expected to resolve.
(d) Areas and/or times of operation.

(e) Expected impact on personal privacy.
(f) How the video surveillance will benefit the City or is related to City business.
(g) How the benefits are expected to outweigh any privacy rights as a result of video surveillance.
(h) How it will protect the security and safety of persons.

3.2 Video surveillance must only be in public places and must be practically minimized. Surveillance will not take place in areas considered confidential or normally private, e.g. change rooms, washrooms.

3.3 Video surveillance is not to be used to supervise staff performance or to verify staff attendance in the workplace.

4.0 DAILY USE, ACCESS, AND SECURITY

4.1 Access to video surveillance information is limited to the following individuals:

(a) Chief Administrative Officer (CAO)
Director of Information Technology
Freedom of Information Head
Manager, Technical and Client Services
Manager, Bylaw Services
Records/Information & Privacy Coordinator

A reference to a person in this section includes their deputy, where applicable.

(b) RCMP to access data necessary to investigate a law enforcement matter by submitting an RCMP Records Release Form to applicable City employees. All disclosures will be tracked by the Legislative Services department.

4.2 Any requests for access to incident specific information must be referred to the City's FOI Head or Records/Information & Privacy Coordinator and will only be disclosed in accordance with *FOIPPA*.

4.3 Access and use of video surveillance information is to be for the purposes of investigation of an incident in any public place.

4.4 Senior Technical staff will access the equipment only for the purpose of designing, deploying, maintaining and assisting with the extraction of the portions of the data. Bylaw staff may be authorized to view, retrieve and access video surveillance for the purpose of providing authorized data in response to an RCMP request for records.

4.5 Physical and electronic security must be in place at all times to properly secure access to the recording equipment and video data. Detailed logs that record all instances of access to and use of the recording equipment and video material must be maintained at all times by authorized staff.

4.6 Records of video surveillance systems that collect personal information must be protected in accordance with the *Freedom of Information and Protection of Privacy Act*.

4.7 The locations and times of all video material must be maintained in logs and kept current by authorized staff. The video surveillance equipment or screen must be located so that the public is not able to see any video reproduction. An exception to this

may occur when the video screen is mounted in a public place with the intention of communicating information to the general public by live video feed.

4.8 Video surveillance data or videotapes may not be publicly viewed or distributed in any fashion as provided by this policy and/the *Freedom of Information Protection of Privacy Act* (FOIPPA). Video data must not be altered in any manner, with the exception of saving investigation material related to an incident on public places or information required for law enforcement purposes. Other than release to the RCMP, or use for City of Nanaimo purposes in accordance with this Policy, video surveillance data will only be released on the authority of a production order to seize the recorded data for evidence or other court order.

5.0 RETENTION AND DESTRUCTION

5.1 The City will use a recording system that overwrites data on a continual basis.

5.2 Recorded video data will generally be retained for up to two weeks. Recorded material will automatically be deleted and purged at the expiry of the above retention period.

5.3 Recorded data that has been saved to another medium, for investigation purposes, will be retained for at least one year after being used, so that the affected individual has a reasonable opportunity to obtain access to that personal information. Such recorded data is to be destroyed after one year or after the affected individual has had access to the data, unless otherwise required for legal, administrative or other proceedings.

5.4 Old storage media must be securely destroyed.

6.0 SIGNAGE

6.1 It is a requirement of the *Freedom of Information and Protection of Privacy Act* that individuals be notified when the City collects their personal information. Accordingly, at each facility where video surveillance takes place, signs not less than 30 cm x 30 cm in size must be prominently displayed at entrances to and egresses from the facilities.

6.2 The sign must clearly state the purpose for the collection, the legal authority for the collection, and the title, business address and business telephone number of an employee who can answer the individual's questions about the collection. A pictogram of a video camera must also be shown on the sign.

7.0 TRAINING

When applicable and appropriate, the policy and guidelines will be incorporated into training and orientation programs of the City. Training programs addressing staff involvement with the use and monitoring of video surveillance equipment under the policy and under the *Freedom of Information and Protection of Privacy Act* shall be conducted as required.

8.0 SYSTEM AUDIT

All systems will be audited randomly on an annual basis for adherence to this policy. Audits will be conducted collaboratively by the Legislative Services and Information Technology department designates.

PROCESS:

To obtain instructions for processing RCMP Request for Records contact the Legislative Services Department.

To complete a Privacy Impact Assessment contact the Legislative Services Department.

Authorized staff will perform system audits as required.

RELATED DOCUMENTS:

Freedom of Information and Protection of Privacy Act
COU-207-Privacy Policy
ADM-001-RM Framework Policy
ADM-002-RM Accountability Policy
ADM-003-Records Management Policy
ADM-005-RM Privacy and Information Security Policy
ADM-009-RM Access to Information Policy
ADM-044-Code of Conduct Policy
ADM-089-Acceptable Use of Technology Policy

REPEAL/AMENDS:
COU-178-Video Surveillance of Civic Property