CITY OF NANAIMO
THE HARBOUR CITY

COUNCIL POLICY MANUAL

RCRS Secondary:	GOV-02	**Effective Date:**	2008-MAY-26
Policy Number:	COU-158	**Amendment Date/s:**	
Title:	Video Surveillance of Civic Property	**Repeal Date:**	
Department:	Facilities and Parks Operations	**Approval Date:**	2008-MAY-26

POLICY

1.0 PURPOSE

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

2.0 AUTHORITY AND RELEVANT LEGISLATION

2.1 The *Community Charter* (British Columbia) and the *Freedom of Information and Protection of Privacy Act* (British Columbia).

3.0 SCOPE

3.1 This Policy applies to any video surveillance system operated by or for the City of Nanaimo that collects personal information in any form. It does not apply to video surveillance systems that do not collect personal information about identifiable individuals. This Policy does not apply to video surveillance conducted by the Royal Canadian Mounted Police ("RCMP"), who are subject to the *Privacy Act* (Canada), to covert video surveillance, and, in particular, this Policy does not expressly permit "community safety cameras" as defined and addressed in Section 11.1 of this Policy.

4.0 PRINCIPLES

4.1 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.

4.2 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 vandalism, theft, damage and destruction. Video surveillance recordings can be used by the City for the investigation and as evidence in any civil proceedings.

4.3 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.

4.4 Before implementing a surveillance system or expanding an existing video surveillance system, the reason for introducing or expanding the video surveillance is to be clearly articulated in writing and approval for the introduction or expansion of video surveillance must be granted by the City Manager or Deputy City Manager as designate.

5.0 DESIGNATED RESPONSIBILITIES

5.1 The City Manager is responsible for the overall video surveillance program. This responsibility can be designated to the Deputy City Manager.

5.2 The Director of each department is responsible for ensuring procedures, as established by policy, for the use of video surveillance equipment, including the random audit of such procedures, are in accordance with this policy.

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

5.4 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 officers and employees may be subject to discipline if they knowingly or deliberately breach the policy.

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

6.0 VIDEO SURVEILLANCE REQUIREMENTS AND USE

6.1 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 City Manager in consultation with the City's Freedom of Information (FOI) Officer. The City Manager, when considering the proposal, will consider the following:

(a) Incident reports respecting vandalism, theft, property damage, 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.

The City has the right to investigate activity of a criminal nature on its property.

6.2 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.

6.3 Notwithstanding Sections 6.1 and 6.2, where there is a risk to people, property, or things in areas normally used to conduct City business, the City Manager may authorize video surveillance to investigate individuals for a specific matter affecting the substantial interest of the City.

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

7.0 DAILY USE, ACCESS, AND SECURITY

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

(a) Mayor
City Manager
Deputy City Manager
General Managers
Department Directors and/or Division Manager
Manager of Bylaw Services
Freedom of Information Head
Freedom of Information Coordinator
City Solicitor
Risk Manager and/or Financial Analyst
An Agent appointed by the City.

A reference to a person in this section includes his or her deputy, where applicable.

(b) RCMP to access data necessary to investigate a law enforcement matter.

7.2 Use of video surveillance information is to be for the purposes of investigation of an incident in any public place. Information Technology staff will access the equipment only for the purpose of maintaining, backing up the software, and assisting with the extraction of the portions of the data. City staff may be authorized to view, retrieve and access video surveillance for a specific purpose.

7.3 Physical and computer related 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 the relevant department.

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

7.5 The locations and times of all video material must be maintained in logs and kept current by the relevant department. Generally, 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.

7.6 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 warrant to seize the recorded data for evidence or other court order.

7.7 Any other requests for access to incident specific information must be referred to the City's Freedom of Information Coordinator and will only be disclosed in accordance with the FOIPPA.

8.0 RETENTION AND DESTRUCTION

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

8.2 Retention of the recorded video data is determined by the amount of available space within the City's storage facilities and the type of medium used to store such data.

8.3 Recorded video data will generally be retained for up to four weeks depending on the system configuration and available memory. Recorded material will automatically be deleted and purged at the expiry of the above retention period.

8.4 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.

8.5 Old storage devices must be securely disposed of based on medial format by shredding, burning or magnetic erasure.

9.0 SIGNAGE

9.1 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, other than monitoring undertaken in Section 6.3, signs not less than 30 cm x 30 cm in size must be prominently displayed at entrances to and egresses from the facilities.

9.2 The sign must clearly state the following:

"This area may be monitored by video surveillance cameras. Please direct inquiries to the City of Nanaimo."

and will include the name of the relevant Division Manager and phone contact number, as well as the business hours they can be contacted. A pictogram of a video camera must also be shown on the sign.

10.0 TRAINING

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

11.0 SURVEILLANCE IN PUBLIC PLACES FOR OTHER CRIMINAL ACTIVITY

11.1 “Community safety cameras” are those used to support the suppression of criminal activity and police investigation of high crime areas within a community, such as; city parks, streets or public areas. Community safety cameras fall outside the intention of this policy and would require the approval of a new policy designed to address issues specifically related to such cameras and the consideration and approval of Council in open session.

12.0 SYSTEM AUDIT

All systems will be audited randomly on an annual basis for adherence to this policy. Audits will be conducted by the Manager of Bylaw, Regulation and Security or his designate.

AUTHORITY TO ACT

Delegated to Staff.

RELATED DPCUMENTS:
N/A

REPEALS/AMENDS:
N/A