



**THE CORPORATION OF THE CITY OF VERNON**  
3400 – 30<sup>th</sup> Street, Vernon, B.C. V1T 5E6  
Telephone: (250) 545-1361 Fax: (250) 545-4048  
website: www.vernon.ca

---

## Administrative Policy

Section:	Legislative Services	
Sub-Section:		
Title:	Video Monitoring Policy	

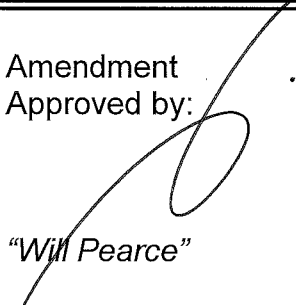
---

### RELATED POLICIES

Number	Title
5608	Freedom of Information Bylaw 5608, 2016
5057	Parks and Public Places Bylaw 5057, 2007
	Privacy Impact Assessments Administrative Policy
	Freedom of Information and Protection of Privacy Act

---

### APPROVALS

POLICY APPROVAL:	AMENDMENT APPROVAL:	SECTION AMENDED
Approved by:  "Leon Gous"	Amendment Approved by:  "Will Pearce"	Replaced and revamped the Video Surveillance Policy and added a lot more information
Chief Administrative Officer: Date:  November 24, 2007	Chief Administrative Officer Date:  April 5, 2018	

## POLICY

It is the policy of The Corporation of the City of Vernon (the City) to utilize video monitoring to enhance the security of individuals, assets and property.

## PURPOSE

Video security monitoring systems are a resource used by the City at selected sites within the jurisdiction of the Corporation of the City of Vernon. The City may use video monitoring systems to monitor and/or record activities within City owned or occupied locations:

1. To assist in the protection of individuals, assets and property;
2. To assist in the prevention and investigation of:
  - a. Criminal activity, injury and property loss; and
  - b. Violations of City policies related to safety and security

The City recognizes that video monitoring technology has a high potential for infringing upon an individual's right to privacy and although video monitoring technology may be required for legitimate operational purposes, its use must be in accordance with the provisions of the *Freedom of Information and Protection of Privacy Act* (the Act).

This policy will provide guidelines designed to assist City Divisions that have identified an appropriate use for video monitoring technology, to manage records that may be created using this technology in a manner that complies with the Act, and records management requirements.

## SCOPE

This policy applies to any video monitoring system owned or operated by the City within its municipal boundaries which may collect personal information about identifiable individuals in any form. These Guidelines **do not apply** to:

1. Video monitoring systems, such as certain traffic cameras, that do not collect information about identifiable individuals.
2. Video monitoring conducted by the RCMP, who are subject to federal legislation, or to covert (hidden) video monitoring.
3. Videotaping or audio taping of City Council Meetings that are open to the public.
4. Communications such as videoconferencing, or reception area systems used to permit staff to ensure service is available to approaching customers (e.g. Electronic door opening, staff coverage)

## DEFINITIONS

**“Act”** means the *Freedom of Information and Protection of Privacy Act* (FOIPPA), R.S.B.C. 1996 Ch. 165, as amended from time to time.

**“City”** means the Corporation of the City of Vernon

**Personal Information** is defined in Schedule 1 of the “Act” means recorded information about an identifiable individual other than contact information.

**Record** as defined in Schedule 1 of the “Act” means books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records.

**Video Monitoring System** refers to an, electronic or digital monitoring system or device that enables continuous or periodic video recording, observing or monitoring of individuals, assets and/or property, including the equipment or device used to receive or record the information collected, including a camera or any other video, audio, physical or other mechanical, electronic or digital device.

**Storage Device** refers to a videotape, computer disk or drive, CD ROM, computer chip or other device used to store the recorded data or visual, audio or other images captured by a video monitoring system.

**Transitory Record** for the purpose of this policy means records that are created to be used only for a limited period of time for the preparation of an ongoing or final record. In this case regarding video monitoring, all monitoring records which do not record an incident providing the basis for an investigation will be considered transitory.

## **GUIDELINES**

**The following guidelines are applicable to all City Divisions:**

### **1. Designated Responsibilities**

The Chief Administrative Officer is responsible for the overall Corporate Video Monitoring Program.

The Division Manager is responsible for ensuring the establishment of divisional procedures of video monitoring equipment, in accordance with this policy. The Division Manager or his/her delegate will ensure procedures for video monitoring are being met within their Division’s mandate.

The Division Manager, or his/her delegate, in consultation with the Information Services Manager is responsible for the life-cycle management of authorized video security monitoring systems [specifications, equipment standards, installation, maintenance, replacement, disposal and related requirements (e.g. signage)] including:

- (a) Preparation and submission of a Privacy Impact Assessment **prior to** installation and use of any new video monitoring systems as per the current Privacy Impact Assessment Policy.
- (b) Completion of a Privacy Impact Assessment for any existing video monitoring systems as soon as reasonably possible.

- (c) Maintaining a record of the locations of the video monitoring equipment.
- (d) Maintaining a list of personnel who are authorized to access and operate the system(s).
- (e) Maintaining a record of the times when video monitoring will be in effect.
- (f) Posting of a **NOTICE OF COLLECTION OF PERSONAL INFORMATION** (Refer to Section 4).
- (g) Assigning a person responsible for the day-to-day operation of the system in accordance with the policy, procedures and direction/guidance that may be issued from time-to-time.

City employees and service providers shall review and comply with the policy and the Act in performing their duties and functions related to the operation of the video monitoring system.

Where the City has a contract with a service provider, the contract shall provide that failure by the service provider to comply with the policy or the provisions of the *Act* is considered a breach of contract leading to penalties up to and including contract termination. Employees of institutions and employees of service providers shall sign written agreements regarding their duties under the policy and the *Act*, including an undertaking of confidentiality.

- (h) Conducting random **audit** of procedures, in accordance with this policy, including monitors and storage devices, at irregular intervals with the results of each review documented in detail with any concerns addressed promptly and effectively.

## 2. Considerations

Prior to use of video monitoring equipment, the City Division must consider the following through preparation of a Privacy Impact Assessment:

- (a) Rationale
  - i. The purpose/objective for installing the video monitoring system
  - ii. The necessity for the use of the video monitoring system in this area
  - iii. What less privacy-intrusive alternatives to the use of video monitoring have been considered and why they have been rejected
- (b) Scope
  - i. Description of area(s) to be monitored and placement of video monitoring system, including diagrams where feasible
  - ii. How many video monitors will be installed
  - iii. Whose activities will be viewed by these video monitors (e.g. public, employees)
  - iv. What types of Data will be captured (i.e. video, audio or both)
  - v. Any special capabilities of the system (e.g. Zoom, facial recognition or night vision features)
- (c) Privacy

- i. How the video monitors have been positioned or configured to collect the minimum amount of personally identifiable information necessary to achieve the purpose of the collection
- ii. How individuals will be notified that they are entering an area that is being monitored
- iii. Whether and when video monitors will be monitored in real time
- iv. Whether and when recording of video monitor data will occur

(d) Security of Video Monitoring Data

- i. The place where video monitoring data will be received and/or monitored
- ii. Arrangements in place to protect against unauthorized viewing of the video monitoring data
- iii. How and where any recorded video monitoring data will be stored
- iv. The protocol for accessing and viewing any recorded video monitoring data
- v. Technical and physical security arrangements in place to protect against unauthorized access or disclosure of any recorded video monitoring data
- vi. The protocol for logging access, use and disposal of any recorded video monitoring data
- vii. Any agreements between the City and service providers must state that the records dealt with or created while delivering a video monitoring program are under the City's control and subject to privacy legislation (FOIPPA).
- viii. Employees and service providers must review and comply with the policy and the Act in performing their duties and functions related to the operation of the video monitoring system.
- ix. Service providers having access to video monitoring information must be bonded and sign a confidentiality agreement (Attachment 'A'), 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.
- x. Requests for video monitoring systems that involve the collection, use, retention, or access of images on a server or are accessed via the City network require the approval of the Information Services Manager to ensure that adequate resources are available to support the web-based video monitoring system.

### 3. Installation and Placement

Video monitoring equipment should never monitor the inside of areas where the public and employees have a higher expectation of privacy such as change rooms and washrooms.

- (a) Equipment should be installed in a strictly controlled access area. Only authorized controlling personnel should have access to the access area and the equipment.
- (b) Equipment should be installed in such a way that it **only** monitors those spaces that have been identified as requiring video monitoring.
- (c) Adjustment of the video monitor position should be restricted, if possible, to ensure only designated areas are being monitored.

- (d) Video monitoring should be restricted to periods when there is demonstrably a higher likelihood of crime being committed and detected in the area under monitoring.

#### 4. Notification

As a general rule, the Act requires the City to notify individuals that it is collecting their personal information. The public must be notified of the existence of video monitoring equipment by clearly written signs prominently displayed at the entrances, exterior walls, interior of buildings and/or perimeter of the video monitoring areas.

Video monitoring cameras must not be hidden or disguised. Signage must also be posted to notify the public of video monitoring locations(s) so that individuals have ample warning before entering a monitored area. Where practicable this signage must provide an internet address for the public notification described in the section.

The City will post a public notification on it's website of the purpose(s) for the use of its video monitoring systems; the legal authority for the collection of information using these video monitoring systems; and the title, business address, business telephone number and email address of an employee who can answer questions about the collection

The following is suggested wording for use in building signage, based on a minimum requirement of the Office of the Information and Privacy Commissioner:

**“THIS AREA IS MONITORED BY VIDEO CAMERAS. Please direct inquiries to:** *(title, business address and phone number of someone who can be contacted) Monday through Friday, between the hours of 8:30 am and 4:30 pm, except on statutory holidays, to answer questions about the collection of personal information and more information can be found at [www.vernon.ca](http://www.vernon.ca)*

#### 5. Access, Use and Disclosure

In accordance with section 26(c) of the Act, the City may only collect personally identifying information using video monitoring systems when the information relates directly to and is necessary for one or more of the objectives set out in the 'Purpose' section of this policy, and only under the following conditions:

- (a) Other means for achieving the same objectives are substantially less effective than using cameras;
- (b) The benefits of using cameras substantially outweigh any privacy intrusion, and
- (c) The cameras have been configured to collect the minimum amount of personally identifiable information necessary to achieve the purpose of the collection

In accordance with section 32(a) of the Act, the City may only use personally identifying information collected by video monitoring systems for one of the objectives set out in the 'Purpose' section of this policy, or for a use consistent with those objectives

Access to video monitoring footage is limited to the following individuals:

- Chief Administrative Officer
  - Division Director or delegate responsible for the video monitoring system
  - FOIPPA Head
  - Information Services Technicians (only as noted in section 5(e) )
  - City of Vernon Solicitor
  - RCMP in relation to a law enforcement matter
  - An Agent appointed by the City of Vernon
- (a) Any records (videotapes, still photographs, digital images, etc.) produced by monitoring systems shall be kept in a secure, locked facility and managed appropriately to protect legal obligations and evidentiary values.
- (b) Access to the storage devices should only be by authorized personnel. Logs must be kept of all instances of access to, and use of, recorded material to enable a proper audit trail. The personal information recorded by video monitoring is subject to access and privacy legislation.
- (c) Access to the storage devices should be possible only by authorized personnel. The system will generate a log for each time it is accessed. In addition, the system will ensure that a log file would be generated if the log file itself was deleted, and that the user performing the deletion would also be recorded. Logging cannot be turned off. Access logs, both physical (**attachment 'B'**) and electronic, must be kept of all instances of access to, and use of recorded material.
- (d) Video monitors must be located so that the public is not able to see any video reproduction.
- (e) Information Technology service providers will access the equipment only for the purpose of installing, maintaining, backing up the software, and assisting with the extraction of the portions of the data.
- (f) Physical and computer software security must be in place at all times to properly secure access to the recording equipment and video data.
- (g) Video monitoring data may not be publicly viewed or distributed in any fashion as provided by the policy and the *Act*.
- (h) Video monitoring data must not be altered in any matter, with the exception of saving investigation material related to an incident required for law enforcement purposes, or as required to protect personal privacy in accordance with the *Act*.
- (i) Requests for access to incident specific information must be referred to the FOIPPA Head and will only be disclosed in accordance with the *Act*.

## 6. Retention & Destruction

- (a) Recorded information should be erased every thirty (30) days where no incident of concern to the City has been reported, or where viewing the recorded information reveals no such incident. Such recordings will be considered a transitory record.
- (b) Where the City is advised, or the City becomes aware that an incident may have occurred, the video recording is reviewed for the incident. When recorded information (that contains personal information about an individual) reveals an incident, and the City uses this information to make a decision that directly affects the individual, the information will be retained for one (1) year after the decision is made, unless otherwise required for legal or other proceedings.
- (c) Old storage devices must be securely disposed of by shredding, crushing, burning or magnetically erasing any and all recorded images and sounds.
- (d) Logs as identified in Section 5 *Access, Use and Disclosure* and in Section 8. *Procedures* will have a retention period of the current year plus one year (CY + 1y) and will be destroyed at the expiry of the retention period by authorized personnel, unless otherwise required for legal or other proceedings.
- (e) Reviews and audits per Section 1. *Designated Responsibilities* and in Section 8. *Procedures* will be retained for a total of eight (8) years (CY + 1y/6y/D).

## 7. Training

- (a) Where applicable and appropriate, the policy and guidelines will be incorporated into training and orientation programs of the City of Vernon and service provider(s). Training programs addressing staff obligations under the Act will be conducted as considered necessary by the FOIPPA Head.

## 8. Procedures

### (a) Procedures for RCMP Access to Video Monitoring Records

- i. Should the RCMP require access to video a formal FOI Request shall be completed and will include an RCMP file number
- ii. The Division Manager or designate responsible for the video monitoring system will review the footage for relevant footage
- iii. The Division Manager, or designate will provide copies of relevant footage as requested to the FOI Head or designate who then formally provides to the RCMP FOI requester.

### (b) Procedures for Maintaining Logs:

**The Director or Designate responsible for the video monitoring system shall ensure that:**

- i. Detailed logs, both physical and electronic, recording all instances of access to and use of the recording equipment and information collected are maintained at all times in accordance with this Policy.



- ii. Locations and times of all recordings is maintained in logs, and kept current with the installation, maintenance and monitoring noted in the log.
- iii. Physical logs are kept in a secure, locked facility and managed appropriately to protect legal obligations and evidentiary values.
- iv. Electronic logs are kept appropriate securities applied and maintained.

**(c) Procedures for Conducting Audit:**

**The Director or Designate responsible for the video monitoring system shall ensure that:**

- i. Once a video monitoring system has been put into place, an annual audit is undertaken which assesses if the system is accomplishing its intended purpose. The audit shall be submitted to the Chief Administrative Officer for review and consideration with a copy provided to the FOIPPA Head.
- ii. The annual audit assesses the efficiencies of the equipment, monitoring processes and results. The audit evaluates whether the policy is being adhered to and whether unintended negative effects on personal privacy are occurring. Such a review may recommend termination of the system if the intended purposes are not being accomplished or this policy is not being adhered to.
- iii. Random audits are undertaken to ensure that all authorized personnel is complying with the procedures in accordance with this policy. The random audits shall be noted in the annual audit report.

**SAMPLE: Confidentiality Agreement for Third Parties**  
**Monitoring of Video Monitoring**

THIS CONFIDENTIALITY AGREEMENT (the 'Agreement') is dated this \_\_\_ day of \_\_\_\_\_, 20\_\_.

BETWEEN: THE CORPORATION OF THE CITY OF VERNON  
3400 – 30TH STREET, VERNON, BC V1T 5E6  
(The "City")

AND NAME OF CONTRACTOR  
ADDRESS  
(The "Contractor")

NAME OF CONTRACTOR'S DESIGNATED INDIVIDUAL  
ADDRESS  
(The "Recipient")

OR / AND NAME OF EMPLOYEE  
ADDRESS  
(The "Employee")

(If applicable) WHEREAS \_\_\_\_\_ (name of Contractor) has entered into an agreement with the City of Vernon for \_\_\_\_\_ services at \_\_\_\_\_ ('the contract site');

(If applicable) AND WHEREAS the Recipient is the individual designated by \_\_\_\_\_ (name of Contractor) who may, from time to time, be asked by the City to monitor recordings made by way of video monitoring at the contract site solely for the purpose of law enforcement as requested by the City;

**OR**

(If applicable) WHEREAS the Employee may, from time to time, be asked by the City of Vernon to monitor recordings made by way of video monitoring solely for the purpose of law enforcement as requested by the City;

AND WHEREAS the City of Vernon requires that the Recipient/Employee enter into a Confidentiality Agreement prior to accessing personal information contained in the video monitoring recordings;

(If applicable) NOW THEREFORE the Contractor agrees as follows:

1. The Contractor does hereby designate the Recipient as the designated individual for the purposes of this agreement.
2. The Contractor agrees that adherence to this confidentiality agreement and the City's Video Monitoring Policy is the responsibility of both the Contractor and the Recipient and agrees that breach of this confidentiality agreement or non-compliance of the Video Monitoring Policy may result in contract termination.

NOW THEREFORE the Recipient/Employee agrees that:

1. They will keep all information contained in the video recordings strictly confidential and access to such recordings and associated data must be solely for the purposes of law enforcement as requested by the City, and only to the extent required for that purpose;
2. They will keep all video recordings and data secure, not allow access to any other individual or group, and will not make copies of any recordings or data in any format, including electronic formats, unless given written and explicit approval by the City's Head of Freedom of Information and Protection of Privacy;
3. All information shared with the Recipient/Employee is governed by the *Freedom of Information and Protection of Privacy Act* (The "Act") and that the Recipient/Employee will abide by the terms of this Act;
4. All recordings and data provided to the Recipient/Employee must be returned to the City promptly after use, must be viewed and returned within one week of receipt, and must not be destroyed by the Recipient/Employee. The Recipient/Employee must not keep any copies of such recordings and data in any format, including electronic formats;
5. They will ensure the security and integrity of the recordings and data, and will keep them in a physically secure and separate location safe from loss, alteration, destruction, intermingling with other records and data, and access by any unauthorized individuals;
6. At all times, they will take all reasonable precaution to prevent inadvertent use, copying or transferring of the data or information provided by the video recordings and will not email or otherwise transmit the recordings or data in any format;
7. They will not disclose, divulge or communicate in any way to any person, firm or corporation, including but not limited to the Contractor or any other employees of the Contractor, any information of which the Recipient/Employee becomes aware of by means of accessing such recordings and data and will observe strict secrecy in regards to that information;

8. They will promptly deliver all data and recordings, in all media formats provided, to the City upon completion of any task performed by request of the City.
9. All recordings and data and any information from such recordings and data shall at all times remain the exclusive property of the City;
10. They will abide by the City's Video Monitoring Policy as attached to this Agreement and as updated from time to time. The Recipient/Employee agrees that breach of this confidentiality agreement or non-compliance of the Video Monitoring Policy may result in termination of employment or termination of contract.
11. They will immediately inform the City if they receive notice that they may, or will, be legally required to disclose video recordings or data in their possession, or to disclose information regarding recordings or data. Prior to disclosing any information, the City must be consulted so that, if necessary, they can attempt to prevent or limit such disclosure.
12. The Recipient/Employee's obligations under this Agreement are to remain in effect perpetually and will exist and continue in full force and effect regardless of whether the Recipient is no longer a designated individual for the Contractor or the Contractor is no longer providing the services to the City OR the Employee is no longer an employee of the City.

**IN WITNESS WHEREOF** the parties have signed this agreement as of the day and year above first written.

**CITY OF VERNON**

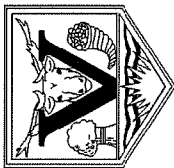
**CONTRACTOR/EMPLOYEE**

\_\_\_\_\_  
 (Print name)  
 Head, Freedom of Information and  
 Protection of Privacy

\_\_\_\_\_  
 (Print name)

**RECIPIENT**

\_\_\_\_\_  
 (Print name)



# Access Log Sheet for Video Monitoring System

Video Monitoring Location	Date of Recording	Time of Recording	Date of Viewing	Reason for Viewing Recording	Name of Viewer (Please Print)	Signature of Viewer

**Note:** To be retained by the City of Vernon till the end of the current year, plus 1 year after the last entry, unless otherwise required for legal or other proceedings.