

Approval date: June 5, 2018

Resolution No.: 248/2018

Subject: Video Surveillance on City Owned Property

Scope:

The City of Penticton may implement Video Surveillance on City owned property where personal safety or property security matters warrant.

Goal:

The purpose of this policy is to set guidelines for the implementation of any Video Surveillance in City owned or occupied buildings or outdoor public space, and set the rules for governing access and disclosure of stored video images.

Definitions:

In this policy,

“PERSONAL INFORMATION” means information about an identifiable individual.

“VIDEO SURVEILLANCE” means a system of monitoring activity in an area or building using a television system in which signals are transmitted from a camera to the receivers by cables or telephone links forming a closed circuit.

Policy:

The City has a legal right and obligation to protect individuals in or around its buildings and its assets and the right to use Video Surveillance for this purpose. Video Surveillance can be useful in deterring crime and nuisance in unsupervised areas where full time live surveillance is an unreasonable expectation due to the risks involved to City staff, or where costs are prohibitive. It should be acknowledged that Video Surveillance can be construed as an unreasonable invasion of personal privacy and the installation of Video Surveillance equipment should only be considered in unique and exceptional circumstances. It should also be acknowledged the deployment of video surveillance by the City is not intended to infringe on the guaranteed rights and freedoms of individuals in any way by

monitoring personal activity in public spaces. The intended purpose is to safe guard city owned assets and individuals who use those assets.

Procedures:

1. Prior to the installation of any Video Surveillance equipment, the department contemplating the installation must consult with Facilities Management, Information Technology services and the City of Penticton Head of Freedom of Information and Protection of Privacy. Information Technology will be responsible for all costs including hardware and services subject to a budget request submitted to Information Technology through the annual budget process.
2. The Head of the Freedom of Information and Protection of Privacy will determine the appropriateness of the installation and determine the legal authority required under the Freedom of Information and Protection of Privacy Act (the Act). Video Surveillance will be considered only after less intrusive security measures have been considered and have been found to be unworkable or inappropriate.
3. The Head of the Freedom of Information and Protection of Privacy will develop any specific procedures required that exceed this policy.
4. Head of the Freedom of Information and Protection of Privacy will provide the information required to be included in signage, to be placed in the location of the Video Surveillance. The department requesting the Video Surveillance will be responsible for signage costs.
5. The manager responsible for Information Technology services will confirm the availability of server, or other technical, capacity and any other technical requirements. If capacity or other technical requirements are required, the department implementing the Video Surveillance will be responsible for the costs.
6. Cameras should be secured to a permanent wall or ceiling, out of reach, and preferably protected from vandalism. Camera range should cover areas needing surveillance, and no more. Cameras are only to be installed in public spaces under this policy. Cameras will not be aimed at areas where people have a heightened expectation of privacy (e.g. washrooms, change rooms, private offices). Cameras should be positioned to reduce capturing images of individuals who are not being targeted, for example positioned to capture images of people on other properties than those owned by the City. Sound is not to be recorded. Appropriate signage will be posted as per 4. above.
7. The City will exercise a high degree of care when using Video Surveillance systems in order to protect the privacy of individuals who visit or work at monitored places. Although Video Surveillance may be warranted for legitimate operational purposes, it must be used in accordance with the Freedom of Information and Protection of Privacy Act.
8. The video recording software and data will be stored on the City's secure servers and data storage infrastructure. Access to the data will be password protected.
9. Video recording equipment will be securely stored in a server room, with controlled access.

10. Those individuals assigned by the Chief Administrative Officer with responsibilities for security with support from Information Technology services will have sole authorization to access and operate the video recording system and stored video recording data, and may grant access to other employees only if it is deemed necessary, and under supervision.
11. Reasons to access video recording data include such instances as:
 - a. The need to identify individuals that have been involved with, or incidents that have resulted from:
 - i. Mischief
 - ii. Criminal behavior
 - iii. Vandalism
 - iv. Harm to another individual
 - v. Theft, including theft from vehicles
 - vi. Other such nuisances that the City finds necessary to investigate
 - vii. Other instances that may arise but access to the data must first be approved by the Head of Freedom of Information and Protection of Privacy, or the Council of the City of Penticton– unless life or safety is at risk, at which point it would be considered an emergency and emergency personnel (Fire, Police, Ambulance, or other) may request access.
 - viii. A personal injury accident
12. All access to video recording data will be logged. Access will be granted through the Information Technology services manager or a designate or a person assigned security responsibilities by the Chief Administrative Officer. Access will require a user name and password granted by the system administrator. Alerts of access will be sent to the system administrator by email, and this logged.
13. Only the data from the estimated time of the incident will be accessed, reviewed and captured on separate media for distribution to law enforcement agencies and the like.
14. Cameras that are turned on for limited periods in the day are preferable to “always on” surveillance e.g. motion activated. Video Surveillance should be limited to the times when the location is open to the public, or subject to unauthorized access.
15. Video data will be retained for approximately 14 – 60 days. Video deletion is directly related to storage availability. The system is designed to fill the storage and then recycle the space through degradation and termination. Data will be deleted, at latest, according to the Records Management policy. Old storage devices must be securely disposed of by shredding, burning or magnetically erasing the images/sounds. When the recorded data/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 data/information should be retained for one year after the decision is made.
16. Video data may be disclosed to police or other appropriate authorities only when the authorities are known and recognized authorities of the City, or court/official documentation is presented requiring access through a written request that can be other than Attachment A.
17. Individuals have the right to access to images relating to them. When disclosing recordings to individuals who appear in them, the organization must ensure that identifying information about any other individuals on the recording is not revealed. This can be done through technologies that mask identity.

18. Any person accessing video data from the system must complete a Disclosure Release Form (Attachment A). These forms will become a permanent record and must be saved into the records or document management system.
19. Video Surveillance and storage of video data is subject to audit and individuals accessing or implementing Video Surveillance may be called upon by other jurisdictional authorities to justify their surveillance interest in any given individual.
20. Should unauthorized disclosure of images occur, staff responsible under the policy will determine the nature of the disclosure, the potential impact to the individuals and if there is a means to reduce same. Individuals whose images have been released must be notified of the breach if their image is publicly available or available to unauthorized sources. Retrieving the images would be preferable. Any disclosure must be reported this to the Head of Freedom of Information and Protection of Privacy, who will report this to the Office of the Information and Privacy Commissioner of British Columbia if the situation has not been resolved.
21. Any employee or contractor of the City failing to adhere to this policy will face discipline and depending of the severity of any breach may be terminated.
22. The Head of Freedom of Information and Protection of Privacy will review with departments the ongoing need for video surveillance at least every two years.

Exclusions:

This policy is not applicable to any requirements imposed by another level of government on the RCMP (Royal Canadian Mounted Police) or other police services.

This policy does not apply to videotaping or audio taping of City Council meetings or events.

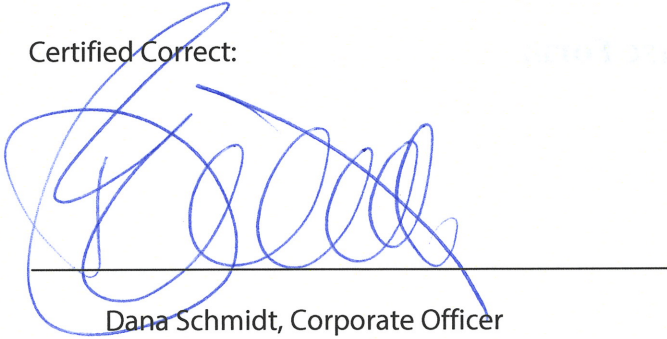
Key Areas of Responsibility:

Action to Take	Responsibility
Appoint those individuals who will have access to the stored video system and data referred to in S. 10 above. These individuals should be responsible for security for the City.	Chief Administrative Officer
Ensure the security of data captured and stored through video surveillance and managing its retention per this policy.	Information Technology Manager
Maintain and update this policy as required.	Head of Freedom of Information and Protection of Privacy
Be aware of this policy, disseminate this policy, and ensure all employees adhere to the policy.	All department heads
Abide by the policy.	Council members, all Staff and contractors where applicable.

Previous revisions:

Revision Date	Author
N/A	

Certified Correct:



Dana Schmidt, Corporate Officer



Disclosure Release Form

Name of Requester:

Department:

Telephone/Email:

Date of Request:

Reason for Request for Video Surveillance Footage:

Date and time of Video requested:

Police File No. (if applicable):

Purpose for which Video will be used:

Note that any video surveillance footage obtained by the City must be kept confidential and is subject to the Freedom of Information and Protection of Privacy Legislation. All video must be safely destroyed at the latest one year after a decision is made (e.g. court decision complete, legal action finalized).

Signature: