CORPORATION OF THE TOWNSHIP OF ESQUIMALT

MANAGEMENT POLICY

TITLE:	Video Surveillance Systems	NO.	M-ADM-16

Effective Date:	XXXX XX, 2025
Approved by:	CAO
Reference:	ADM-25-057
Amends:	to replace Council Policy ADMIN-76 Video Surveillance

1. POLICY OVERVIEW

The Township of Esquimalt (the Township) recognizes the need to balance an individual's right to privacy and the need to ensure the public safety and security of Township staff, clients, visitors, facilities, and properties.

As a public body governed by the *Freedom of Information and Protection of Privacy Act* (FIPPA), the Township has obligations with respect to notice, access, use, disclosure, retention, and disposal of Records. While video surveillance cameras are installed for public safety and security reasons, any Video Surveillance System installed on Township property must also be designed to minimize privacy intrusion.

Proper video surveillance, where deemed necessary, is one of the most effective means of helping to keep the Township's facilities and properties operating in a way that protects public safety, security, and privacy. Video surveillance is useful when used in areas where full time live surveillance is unreasonable due to the risks involved to staff or where costs are prohibitive.

Covert surveillance and/or camera usage without proper signage, is not permitted under this Policy.

This Policy does not refer to videotaping or audiotaping of Township Council or Committee Meetings, traffic flow cameras, or any recordings on mobile devices captured by Township employees, elected officials, volunteers, agents, or service providers.

2. POLICY DESCRIPTION

This Policy has been developed to govern video surveillance at Township owned properties in accordance with the privacy provisions of FIPPA.

This Policy has been drafted to conform to practices outlined by the Office of the Information and Privacy Commissioner for British Columbia (OIPC) in a document entitled "Public Sector Surveillance Guidelines".

3. DEFINITIONS

Video Surveillance System includes all the various components of the video surveillance process used to Record digital images, to connect, view, store, retain, provide access to and dispose of such digital images (and sound if also collected).

Equipment includes the video Recording cameras that digitally Record images, any digital video Recorder (DVR) on which Recorded images are temporarily stored, monitors on which the Recorded images can be viewed, and any server on which the Recorded images are retained during the specified period. This may include Township issued devices such as cell phones, laptops, or tablets if they are used to view recorded digital images of an incident or possible incident.

Record means the Recorded digital material, electronic images and sound files that may be produced by the Equipment.

Third Party refers to a contractor, sub-contractor, service provider or other agent engaged by the Township for the provision of the installation and/or operation of video monitoring systems.

Township Facilities or Properties means any land, building, or structure that is owned, leased, or operated by the Township of Esquimalt.

4. RESPONSIBILITIES

As the property owner or operator, the municipality is ultimately responsible for all video surveillance systems and all personal information collected by Township implemented Video Surveillance Systems, to protect against risks such as unauthorized access, collection, use, disclosure or disposal of any personal information.

Staff responsible for the administration of this Policy include:

Information Technology Manager

The duties of the Information Technology Manager (IT Manager) or their designate include:

1. Ensuring policy compliance and providing status updates to the Chief Administrative Officer (CAO) annually regarding compliance with the Policy.
2. Undertaking regular evaluations of the Township's Video Surveillance Systems to ensure compliance with this Policy.
3. Subject to prior approval by the CAO, approving the installation of video Recording cameras at specified locations on Township owned, leased, or operated properties.
4. Overseeing day-to-day operation of the Video Surveillance System (unless contracted to a Third Party).

5. Ensuring all Records and Equipment are stored in a safe and secure location and that access is restricted to authorized staff only.

Information Technology Department Staff

The duties of the Information Technology Staff (IT Staff) include:

1. Assisting with facilitating access to recorded digital images for authorized staff.
2. Assisting with creating or editing footage or stills from recorded digital images when requested by authorized staff.
3. Assisting with the day-to-day operation of the Video Surveillance System (unless contracted to a Third Party).

Corporate Officer

As the Head for the purposes of FIPPA, the Corporate Officer is responsible for providing a response to access requests and for investigating and reporting any alleged privacy breaches to the CAO and the OIPC.

The key duties of the Corporate Officer include:

1. Acting as the primary contact for all requests by law enforcement agencies or by members of the public for access to Records.
2. Providing ongoing support and guidance to ensure compliance with FIPPA and this Policy to staff authorized to access any part of the Video Surveillance System.
3. Ensuring proper public notification is provided in any location where video recording is established including appropriate placement of signage.

Sponsoring Director

A sponsoring Director is the Director of the Department procuring the system. They are responsible for promoting public safety and security and reducing property damage at Township properties and facilities. They will work in collaboration with the IT Manager to ensure the system aligns with this policy and meets the needs of the Township.

The key duties of this position include:

1. Completing a Privacy Impact Assessment (PIA) early in the planning process.
2. Ensuring the appropriate placement of video surveillance Equipment that is justified based on verifiable, specific reports of incidents of significant public safety or security concerns.
3. In collaboration with the IT Manager, seek authorization for the system by the CAO, in part by providing a completed PIA.
4. In collaboration with the IT Manager, provide training on the obligations to and compliance with FIPPA and this Policy to any staff (including Third Party staff) that is to be authorized to be involved with any part of the Video Surveillance System. Such training is to occur prior to authorized staff being provided access to any part of the Video Surveillance System.

5. Conducting investigations or working with local police services where property damage to Township properties or facilities or other unlawful activity has occurred.
6. Removing video surveillance Equipment from locations no longer meeting the justifications for initially installing it.

Chief Administrative Officer (CAO)

The key duties of this position include:

1. Authorizing the procurement, installation and operation of any video surveillance system for the Township of Esquimalt in accordance with the Purchasing and Disposal Bylaw, 2023, No.3133.
2. Designating other staff (including approval of Third Parties) to be permitted to operate a Video Surveillance System for the Township of Esquimalt.
3. Initiating any discipline or legal action for a privacy breach.

Other Staff

In addition to the IT Manager, Corporate Officer, and a sponsoring Director, only staff with the approval of the department head and designated by the CAO (including approval of Third Parties) shall be permitted to operate a Video Surveillance System for the Township of Esquimalt.

The key duties of other authorized staff include:

1. Must comply with this Policy.
2. Must not access or use any information contained in any Record for personal or another purpose except as authorized under this Policy.
3. Staff must not copy, dispose, destroy, erase or alter any Record without the authorization of the Corporate Officer as per ADMIN-42 Records Management Policy.

5. COLLECTION OF PERSONAL INFORMATION

Personal information must only be collected as permitted under FIPPA.

6. APPROVAL

All new video surveillance systems, or significant changes or expansions to existing video surveillance systems, must be approved in advance by the CAO.

To obtain approval, the Sponsoring Director must first submit a PIA to the Corporate Officer for review and approval prior to seeking final approval from the CAO.

7. DOCUMENTATION REQUIRED PRIOR TO INSTALLATION

1. An approved PIA completed by the responsible department of the Township of Esquimalt in collaboration with the Township's privacy team (Corporate Services).

2. A map of the area being monitored with notations for camera locations and approximate coverage area(s). When used outside, include the full road(s) and buildings adjacent to the property and when used inside, include the full floor plan for the floor(s) to be covered.
3. The system's operating procedures and any other documents or Records identified in the system's operating procedures.

8. GUIDELINES PRIOR TO THE INSTALLATION OF A VIDEO SURVEILLANCE SYSTEM

Before deciding to install video surveillance, the following factors must be considered:

1. The use of a Video Surveillance System at a specific location should be justified based on verifiable, specific reports of incidents of significant public safety, or security concerns.
2. A Video Surveillance System should only be pursued after other measures of deterrence or detection have been considered and rejected as being unfeasible or significantly less effective.
3. An assessment must be conducted on the effects that the proposed Video Surveillance System at a specific location may have on personal privacy, and the ways in which any adverse effects can be mitigated.
4. The proposed design and operation of the Video Surveillance System should minimize privacy intrusion.

To minimize privacy intrusion, the following must be considered:

1. The Equipment should be installed to only monitor those areas that have been identified as requiring video surveillance.
2. The ability to adjust or manipulate video recording cameras is restricted so that the cameras do not record areas that are not intended to be covered by the Video Surveillance System, such as through windows in adjacent buildings or onto adjacent properties.
3. Equipment should never monitor or record the inside of areas where the public and /or staff have a higher expectation of privacy (e.g. change rooms and washrooms).
4. Video surveillance should be restricted to periods when there is a demonstrably higher likelihood of significant public safety or security concerns in the area under surveillance.
5. Viewing and recording Equipment must be in a restricted access area where only authorized staff have access.

9. EQUIPMENT

Any monitors that may be used for viewing of Records will be kept in a secure access-restricted location where they are not visible to the public or unauthorized staff.

All Equipment that is not in use must be stored securely in a locked receptacle located in an access-restricted area.

The Township IT Manager and/or the Third Party shall ensure that any Equipment and related storage devices such as disks, tapes, drives, etc., used in the Video Surveillance System, are disposed of in accordance with an applicable technology asset disposal process ensuring personal information is erased prior to disposal so that such personal information cannot be retrieved or reconstructed. Acceptable disposal methods may include shredding, burning, or erasing, depending on the type of Equipment. The IT Manager and/or the Third Party shall prepare a Record of the details of the secure destruction of the Equipment and provide it to the Corporate Officer upon completion.

If the original purpose for which a Video Surveillance System was approved is no longer applicable, or the system no longer meets the above criteria, the video surveillance system must be discontinued. Discontinued systems must be disabled and removed and the Corporate Officer advised. No non-functioning system should remain to imply security protection.

10. SECURITY OF INFORMATION

1. Only authorized employees of the Township or a defined Third Party noted in the Township of Esquimalt PIA for the initiative may access or operate the Video Surveillance System or access the Video Surveillance System recordings.
2. Security arrangements must be in place to prevent unauthorized monitoring, interception, or interference with transmissions from the Video Surveillance System.
3. Information stored on tapes or other removable storage devices must be dated, labeled, and stored securely in a locked container located in a controlled access area. Information stored on a computer or server must be protected in accordance with the Township's policies.
4. Any agreement between the Township and a Third Party involving installation or operations of a Video Surveillance System must contain confidentiality and ownership provisions clarifying that all Records produced under the agreement will remain the property of the Township even where the service provider has physical possession of them and Records shall remain subject to privacy legislation (*FIPPA*) and other applicable statutes.
5. Township employees and Third Parties responsible for the installation or operation of a Video Surveillance System on Township premises must review and comply with the Esquimalt Privacy Policy, this policy, and *FIPPA.*

11. PUBLIC NOTIFICATION

FIPPA requires that the Township notify individuals when their personal information may be collected unless a specific exception applies. The method used to give notice will be consistent with the location, use and purpose of the Video Surveillance System.

The notification will also be posted on the Township's website for the public's information.

The notification must inform individuals of the legal authority for the collection of personal information, the principal purposes for which the personal information is intended to be used, and the Privacy Team's contact information in the event of any questions about the collection of personal information.

The public must be notified of the existence, and possible operation, of video monitoring Equipment. Clearly written signs must be prominently displayed at the entrances, on the exterior walls, and/or perimeter of the video monitoring areas, bearing the following wording:

For Safety, Security and Crime Prevention Purposes
THIS AREA MAY BE UNDER VIDEO SURVEILLANCE
Recordings may be used as evidence in a court of law
Questions? Contact the Township of Esquimalt, Privacy Team, foi@esquimalt.ca
250-414-7177 or Municipal Hall, 1229 Esquimalt Road, Esquimalt, BC V9A 3P1
This collection of personal information is authorized under Section 26 (c) of the
Freedom of Information and Protection of Privacy Act.

A sample of a compliant sign is contained in Appendix 1 of this policy.

12. OPERATIONAL LOGS AND AUDITS

The responsible staff, including Third Parties, must maintain a log for the operation of their video surveillance system, showing the dates and times of operation, the location and field of view of the cameras, and the position titles of those that have access to the information.

For each Video Surveillance System that collects or may collect personal information, the log must also record all viewing and / authorized copies (see Section 13) of the Video Surveillance System recordings, the start and end locations viewed in the recording, the date and time of viewing and/or copying, and identify all individuals who have viewed and/or received a copy of the video.

Audits of systems that collect personal information may be conducted by internal audit on a periodic basis to confirm compliance with FIPPA and adherence to this Policy and the associated procedures. Those viewing a Video Surveillance System must be made aware that each system is subject to random auditing and that they may be called upon to justify the method and details of use of the system.

13. ACCESS TO RECORDS AND EQUIPMENT

All requests for access to Records are to be directed to: foi@esquimalt.ca or Corporate Services, Municipal Hall, 1229 Esquimalt Road, Esquimalt, BC V9A 3P1 for response. Such requests must be in writing either in the form of a letter, an email, or on the prescribed form available on the Township's website and must set out the specific date and time of the

incident and Record requested. Only information from the specified date and time will be accessed, reviewed and captured for distribution as required.

Video Records may be disclosed to police, law enforcement agencies, or other appropriate authorities only when the authorities are known and recognized as authorities of the Township, the Province, or the Federal Government. Official documentation and authorizing statutes must be provided and carefully reviewed before Records are sought and/or disclosed or otherwise distributed.

14. USE, ACCESS AND DISCLOSURE

The information recorded by Video Surveillance Systems is subject to FIPPA. Information recorded by the Video Surveillance System may only be used, disclosed, or accessed for the purpose for which it was collected or otherwise authorized by law.

Information may be released to the public through the formal access to Records (FOI) process, or as otherwise required by law. Administration of FOI requests is the responsibility of the Corporate Services Department of the Township of Esquimalt and must be directed there.

Only the Corporate Officer, or a staff person delegated by the Corporate Officer, may be authorized to disclose information recorded by the Video Surveillance System. To enable a proper audit trail, logs must be kept of any such instance of disclosure.

Access requests that are not compliant with FIPPA must be forwarded to the Corporate Services Department.

Unauthorized access to, use, or disclosure of personal information from a Video Surveillance System is a breach and will be investigated (see Section 17).

If the Corporate Officer provides access to any Record, the following information, as relevant, will be recorded:

1. the date and time of the original recorded incident including the designated name/number of the applicable camera and storage device if applicable;
2. the time and date the copy of the original Record was prepared and sealed;
3. the time and date the sealed copy of the Record was provided to the applicant;
4. the case file number of the Law Enforcement Officer's investigation, if applicable;
5. a description of the circumstances and legal authority justifying the disclosure;
6. the amount of the Record involved; and
7. the means used to provide access to the Record.

15. DATA SHARING

The Township may enter into agreements to share live feeds of Video Surveillance System Video with other government agencies, with prior approval of the Corporate Officer, or their designate, if it is a condition of such an agreement that the other governmental agency is not permitted to record the Video Surveillance System video.

16. RECORDS MANAGEMENT

Records created by Video Surveillance Systems are not only subject to FIPPA, but also the Township Records Management Policy (ADMIN-42) and the Records Classification and Retention Schedule which prescribes retention periods.

All video surveillance recordings must be retained for a period of no longer than 30 days and destroyed at the end of this retention period unless:

1. The recorded information reveals an incident that contains personal information about an individual and the Township or a Third Party uses this information to make a decision that directly affects the individual, in which case the video surveillance Records must be retained for one year after the decision is made in accordance with FIPPA.
2. A request is made by the Township's Legal Counsel or Risk Manager to preserve the Recorded information on the basis that the Recorded information is relevant to contemplated or current litigation, in which case the video surveillance Records must be retained until:
   (i) 10 days after the expiry of the applicable limitation period for the commencement of a legal action where a legal action is contemplated but no legal action is commenced;
   (ii) 10 days after the expiry of the applicable appeal period where a legal action has been commenced, the matter has been adjudicated upon by the Court, or an administrative tribunal and no appeal has been filed; or
   (iii) 10 days after the settlement or other resolution of the litigation.
3. The responsible Department requires the video surveillance recordings to be preserved for an additional period to complete the business purpose for which the video surveillance recordings were created. In such a case, the interested party must make a written request to the Corporate Officer setting out the basis on which an extension is required. Upon receipt of the request, the Corporate Officer may decline or grant the request for an extension to a fixed date.

Where the Records Classification and Retention Schedule and the above listed exemptions conflict, the records will be retained for the longer period.

17. UNAUTHORIZED ACCESS OR USE (PRIVACY BREACH)

Complaints about an information breach must be made to the Corporate Officer. The Corporate Officer is responsible for reporting information breaches to the CAO. The Corporate Officer, or their delegate, must carry out an investigation. The CAO is responsible for the initiation of discipline or legal action for a breach.

Staff who become aware of any unauthorized access to or disclosure of a Record in contravention of this Policy and/or a potential privacy breach are to immediately notify the Corporate Officer, who will ensure that the following procedures are immediately completed:

1. Upon confirmation of a privacy breach, in accordance with the requirements of FIPPA, the Corporate Officer shall notify the OIPC of the details of the breach.
2. Together with the IT Manager, the Corporate Officer shall take reasonable steps to mitigate the extent of the privacy breach and review the adequacy of privacy protection measures included in the Video Surveillance System and the existing Policy.
3. The Corporate Officer shall inform the CAO of any alleged privacy breach.
4. The IT Manager shall take all reasonable actions to recover the Record and limit any further unauthorized disclosure.
5. The IT Manager shall thoroughly investigate the cause of the unauthorized access or disclosure and take reasonable steps to eliminate potential future re-occurrences.
6. The Corporate Officer will notify affected parties whose personal information was inappropriately disclosed.

Intentional wrongful disclosure or disclosure resulting from negligence by staff may result in disciplinary action up to and including dismissal. Intentional wrongful disclosure or disclosure resulting from negligence by Third Parties may result in the termination of their contract.

18. INQUIRIES RELATED TO POLICY

All inquiries regarding this Policy shall be directed to the Corporate Officer.

19. REVIEW OF POLICY

This Policy shall be reviewed annually by the Corporate Officer who will forward recommendations for update, if any to the CAO for approval.

Appendix 1 – Sample Notice of Video Surveillance

For Safety, Security and Crime Prevention Purposes
THIS AREA MAY BE UNDER VIDEO SURVEILLANCE
Recordings may be used as evidence in a court of law
Questions? Contact the Township of Esquimalt, Privacy Team at foi@esquimalt.ca
250-414-7177 or Municipal Hall, 1229 Esquimalt Road, Esquimalt, BC V9A 3P1
This collection of personal information is authorized under Section 26 (c) of the *Freedom of Information and Protection of Privacy Act*.