THE DISTRICT MUNICIPALITY OF MUSKOKA

ADMINISTRATION POLICY

Name: Video Surveillance		**Policy Number:** AD-014-2019
Administrative Approval Date:	**Council Approval Date:** December 16, 2019	**By-Law Reference**:
Supersedes: New	**Most Recent Amendment Date:** November 4, 2019	**Effective Date:** December 16, 2019

1. POLICY

1.1 The District Municipality of Muskoka (the "District") recognizes the delicate balance between an individual's right to be free from invasion of privacy and the need to protect the safety and security of District employees, the public, and District-owned or operated assets.

1.2 The District may use video surveillance systems in District-owned or operated properties and facilities to deter and detect unauthorized, illegal or inappropriate behaviour.

1.3 This policy does not require or guarantee that a camera or recording equipment will be recording or monitored in real time at all times or that all areas of the facilities or premises will be covered by the video surveillance system.

1.4 Staff involved in any aspect of the operation of video surveillance systems will be trained on this policy and their legislated obligations in performing their duties and functions related to the operation of the video surveillance systems.

2. PURPOSE

To establish procedures for the installation and use of video surveillance systems and to ensure that the personal information of individuals captured by such systems is collected, used and disclosed in accordance with the *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56, as amended (MFIPPA) and any other applicable laws.

3. APPLICATION

3.1 This policy applies to all District employees, as well as contracted service providers and their employees who may work with or operate video surveillance systems.

3.2 This policy applies to video surveillance systems installed or proposed to be installed at District-owned or operated properties or facilities.

3.3 This policy does not apply to covert surveillance used as an investigation tool for law enforcement purposes or in contemplation of litigation.

4. LEGISLATIVE AUTHORITY

4.1 The District shall collect, use, disclose and store personal information in carrying out its video surveillance program strictly in accordance with MFIPPA and other applicable guides and laws.

4.2 The collection, use, and disclosure of video records and this policy shall comply with other related District policies, including but not limited to:

4.2.1 The Records Retention By-law (2016-37), Schedule "A" Records Retention Program policy (AD-008), and Schedule "B" Records Retention Schedule, as amended;

4.2.2 Corporate Records and Information Management Program (AD-009); and

4.2.3 Municipal Freedom of Information and Protection of Privacy (MFIPPA) policy (AD-012).

4.3 The objectives and use of video surveillance systems will be consistent with the Information Privacy Commission's (IPC) *Guidelines for the Use of Video Surveillance*.

4.4 This policy may be amended from time-to-time as required under the authority of the Chief Administrative Officer (CAO).

5. DEFINITIONS

5.1 Authorized User – District employees and the employees of a contracted service provider who have been approved by the CAO, relevant Commissioner or designate to operate video surveillance systems and who have received training consistent with the requirements of this policy.

5.2 Commissioner – members of the District Strategic Leadership Team (DSLT) including departmental Commissioners, the District Solicitor, and the Director, Human Resources.

5.3 Freedom of Information (FOI) Coordinator – the person appointed by by-law who is responsible for the administration of applicable privacy legislation in the District.

5.4 Incident – an event or occurrence involving the safety or security of people, premises or assets of a District-owned or operated property or facility.

5.5 Personal Information (as collected by the District pursuant to this policy) – recorded information about an identifiable individual, including, but not limited to information relating to an individual's race, colour, national or ethnic origin, sex, or age. If the video surveillance system displays such characteristics of an identifiable individual or the activities in which he or she is engaged, its contents will be considered "personal information".

5.6 Privacy Impact Assessment (PIA) – a risk management tool that helps to identify the effects of a proposed video surveillance system on the privacy of an individual(s) and the safeguards or strategies that may be utilized to eliminate the adverse outcomes of those effects or reduce them to a reasonable level.

5.7 Record – a document made or received in the regular course of business and kept for administrative or operational purposes, regardless of media, including but not limited to correspondence, memoranda, plans, maps, drawings, graphic works, photographs,

film, microfilm, microfiche, sound records, videotapes, machine readable records including email and databases, and any other documentary material regardless of physical form or characteristics, and including "official records" and "transitory records". For the purposes of this policy, video recordings are considered a record and are managed according to the provisions of the Corporate Records and Information Management Program (AD-009), the Records Retention Program (AD-008) and the Records Retention By-law and Schedule (2016-37) as amended.

5.8 Storage device – a videotape, computer disk or drive, computer chip or other device or means used to store the recorded data or visual, audio or other images captured by a video surveillance system.

5.9 Video surveillance system – electronic or digital video recording devices, including cameras, monitors, and storage devices that enable continuous or periodic video recording, observing or monitoring individuals and property in or around District-owned or operated facilities.

6. RESPONSIBILITIES

6.1 The CAO or designate is responsible for:
- **6.1.1** Ensuring overall compliance with this policy and related legislation or by-laws;
- **6.1.2** Acting upon reported breaches of the policy; and
- **6.1.3** Ensuring regular audits of video surveillance systems are conducted to ensure that on-going need for a system is assessed and that privacy risks are mitigated.

6.2 The FOI Coordinator or designate shall be responsible for the following:
- **6.2.1** Implementing, administering and evaluating this policy and any related procedures;
- **6.2.2** Working with the Director/Manager to complete a PIA (Appendix A) for existing and proposed video surveillance systems and recommending approval or rejection based on the information provided;
- **6.2.3** Maintaining a record to identify the location of all video surveillance systems, including the locations of cameras and storage devices, at each site such as floor plans, site plans and equipment inventories;
- **6.2.4** Working in conjunction with the Director/Manager to prepare and ensure signs are posted notifying the public that video surveillance systems are in use;
- **6.2.5** Ensuring that information obtained through video surveillance is used exclusively for lawful purposes and in compliance with this policy, MFIPPA and other applicable legislation, regulations, and by-laws;
- **6.2.6** Identifying and/or providing training for Authorized Users on this policy and their responsibilities under MFIPPA;
- **6.2.7** Ensuring any recorded information being kept for a specific purpose is being adequately stored;
- **6.2.8** Responding to questions and requests for information regarding video surveillance records;
- **6.2.9** Recording and responding to MFIPPA requests for disclosure of video surveillance records;
- **6.2.10** Working with the Director/Manager to investigate in the event of an improper disclosure of personal information and implement any recommendations that result;
- **6.2.11** Responding to privacy complaints or requests for information received through the Office of the Information Privacy Commissioner (IPC) as required; and

6.2.12 Conducting periodic internal audits to ensure compliance with this policy and applicable privacy laws.

6.3 The CAO or Commissioner or designate responsible for a facility in which a video surveillance system is installed is responsible for:

6.3.1 Ensuring compliance with this policy;

6.3.2 Ensuring that a video surveillance system is justified for a particular facility or location (through the completion of a PIA) and providing approval to install a video surveillance system for that facility once satisfied that the undertaking is necessary and the privacy risks have been mitigated;

6.3.3 Determining and documenting the authorized user(s) for a particular video surveillance system and ensuring that they are trained on its use and their responsibilities under this policy;

6.3.4 Ensuring that information obtained is used exclusively for lawful purposes and in compliance with this policy and other applicable legislation, regulations, and by-laws; and

6.3.5 Assisting the FOI Coordinator in investigating and responding to potential privacy breaches.

6.4 Director/Manager or designate shall be responsible for:

6.4.1 Working with the FOI Coordinator to complete a PIA for existing and proposed video surveillance systems;

6.4.2 Working with ITS department for the procurement of suitable equipment;

6.4.3 Installation, maintenance and day-to-day operation of any video surveillance system in their area of responsibility;

6.4.4 Providing the FOI Coordinator with a record to identify the location of all video surveillance systems, including the locations of cameras and storage devices, at each site such as floor plans, site plans and equipment inventories;

6.4.5 Ensuring signs are posted notifying the public that a video surveillance system is in use;

6.4.6 Taking all reasonable efforts to ensure that video surveillance equipment is securely stored and that unauthorized individuals are prohibited from reviewing or accessing footage captured by the video surveillance system;

6.4.7 Developing site specific procedures for the operation of the video surveillance system at each facility;

6.4.8 Training authorized users on site specific procedures;

6.4.9 Conducting regular reviews of video surveillance equipment and practices to ensure compliance with this policy and related procedures; and

6.4.10 Reporting any breaches of the policy or improper disclosure of personal information to the CAO or relevant Commissioner and the FOI Coordinator.

6.5 The Director, Information Technology Services (ITS) is responsible for defining the specifications of the equipment and ensuring standardization and compatibility with network requirements.

6.6 Authorized Users are responsible for:

6.6.1 Participating in training and adhering to this policy, related policies and procedures, and privacy legislation, including signing an Authorized User Confidentiality and Compliance Agreement (Appendix B);

6.6.2 Not accessing or using information contained in the video surveillance system, its components, files, or databases for personal reasons;

6.6.3 Not disposing of, destroying, erasing or altering any record without proper authorization and without following the procedures established in this policy and the District's Records Retention Program policy; and

6.6.4 Reporting to the Director/Manager any suspected violations of this policy or any suspected problems with a video surveillance system.

7. ADMINISTRATION

7.1 Approval for Installation of Video Surveillance Systems:

7.1.1 Video surveillance systems shall be installed in identified public or common areas only where video surveillance is justified on the basis of information provided in the PIA.

7.1.2 The CAO or Commissioner responsible for the facility, in conjunction with the FOI Coordinator, or designate may authorize the installation or change of a video surveillance system.

7.2 Public Notification:

7.2.1 The Director/Manager shall ensure that appropriate signs notifying the public of the video surveillance system are prominently posted with a clear, language-neutral graphical depiction of the use of video surveillance at the entrances, interior of buildings and/or perimeter of surveillance areas.

7.2.2 Signs shall satisfy the notification requirements under Section 29(2) of the MFIPPA (see Appendix C for an example).

7.2.3 This policy shall be posted on the District's website.

7.3 Camera Placement and Monitoring Equipment:

7.3.1 Where possible, all cameras that are adjustable or moveable will be restricted to prohibit the viewing of locations not intended to be monitored.

7.3.2 Video surveillance systems shall not be installed in areas where the public and employees have a high expectation of privacy such as changing rooms or washrooms.

7.3.3 Unless otherwise specified, video surveillance systems may operate 24 hours per day and may be activated by motion or sound detection.

7.3.4 Monitoring equipment shall be located away from the public, in restricted access areas, or in locked rooms with keyed access, or locked storage unit.

7.3.5 The Director/Manager shall provide the FOI Coordinator with a record that identifies the location of all video surveillance systems, including the locations of cameras and storage devices, at each site such as floor plans, site plans and equipment inventories.

7.4 Use of Personal Information Collected:

7.4.1 The personal information collected from the video surveillance system will be used only for the purpose for which it was obtained pursuant to this policy and as identified in the PIA.

7.4.2 Without limiting the generality of the foregoing, the personal information collected may be used by the District or law enforcement agencies to:

- Assist in investigating criminal activity or breaches of District by-laws;
- Assess the effectiveness of safety and security measures taken at a particular property or facility;
- Investigate an incident involving the safety or security of people or District-owned or operated properties or facilities.

7.5 Requests for Disclosure:

7.5.1 General Prohibition – no person shall disclose a video surveillance record that contains personal information to any individual or organization except as permitted through MFIPPA.

7.5.2 Public requests for disclosure – all such requests for video records will follow the process outlined in MFIPPA and the District's MFIPPA policy.

7.5.3 Internal requests for disclosure – District employees may request access to a video recording if it is necessary for the performance of their duties in the discharge of their functions. Such requests must be submitted to the Director/Manager responsible for the video surveillance system.

7.5.4 Law enforcement requests for disclosure – the District may disclose a copy of a video recording to a law enforcement agency where there are reasonable grounds to believe that an unlawful activity has occurred and been captured by the video surveillance system in accordance with section 32(g) of MFIPPA (refer to Appendix D – Law Enforcement Officer's Request Form).

7.6 Storage and Retention of Records – Video records will be retained according to the District's Records Retention Program policy (AD-008) and the Records Retention By-law (2016-38) and Records Retention Schedule, as amended.

7.7 Unauthorized Disclosure:

7.7.1 The District shall ensure that unauthorized disclosures are addressed in a timely and effective manner.

7.7.2 Any District employee having knowledge or suspicion of an unauthorized disclosure of a record or unauthorized access must immediately inform the FOI Coordinator of the breach.

7.7.3 The FOI Coordinator, or designate, shall investigate the alleged breach, in consultation with the appropriate Director/Manager and/or CAO/Commissioner or designate and determine whether or not a violation of this policy and MFIPPA has occurred.

7.7.4 Where it is determined that a breach has occurred, the FOI Coordinator shall follow the procedures outlined in the District's MFIPPA policy.

7.8 Training for Authorized Users – regular training and orientation programs for authorized users shall include a review of this policy, any related procedures, and applicable privacy laws.

7.9 Contracted Service Providers – when the day-to-day operation of a District-owned facility is contracted to an external service provider and the service provider's responsibilities include video surveillance, then this policy shall be referenced in their contractual agreement with the District and:

7.9.1 Authorized contract staff shall comply with the appropriate staff responsibilities as outlined in this policy.

7.9.2 When a contracted service provider fails to comply with this policy, it shall be considered in breach of contract leading to penalties up to and including contract termination.

7.10 Audits of Video Surveillance Policy and Practices

7.10.1 The FOI Coordinator, or designate, will ensure that the use and security of its video surveillance program and equipment is subject to regular audits, at least once a year, to address compliance with this policy and applicable laws. Such audits will include:

- Consideration of the on-going need for video surveillance and if its use can be restricted;
- Ensuring that video images are being properly retained and stored and security measures are being followed; and
- Ensuring that videos are being deleted in accordance with the Records Retention By-law and Retention Schedule, as amended;

7.10.2 The FOI Coordinator will address any recommendations from the audit with the Director/Manager and/or CAO or relevant Commissioner.

7.10.3 Audit records shall be maintained by the FOI Coordinator consistent with the District's Corporate Records and Information Management Program (AD-009).

7.10.4 District staff and contracted service providers will be made aware that their activities are subject to an audit and that they may be called upon to justify their surveillance.

7.11 Any requests or concerns related to the District's handling of personal information collected through video surveillance can be directed to the FOI Coordinator.

Appendices and Forms

- Appendix A System Privacy Impact Assessment (PIA)
- Appendix B Authorized User Confidentiality and Compliance Agreement
- Appendix C Example of Video Surveillance Signage
- Appendix D Law Enforcement Officer's Request Form

Related Policies/Procedures:

- AD-008 Records Retention Program Policy (Schedule "A" to By-law 2016-37)
- AD-009 Corporate Records and Information Management Program
- AD-012 Municipal Freedom of Information and Protection of Privacy (MFIPPA)

Reference: (approval and amendment details, legal references)

- Records Retention By-law (2016-37) and Schedule "B" Records Retention Schedule
- *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA)
- *Guideline for Using Video Surveillance Cameras in Public Places* – Information and Privacy Commissioner of Ontario

ADMINISTRATION POLICY – APPENDIX A

Name: Video Surveillance: System Privacy Impact Assessment (PIA)	**Policy Number:** AD-014-2019 Appendix A

Facility Name	
Address	
Location of surveillance system	
New or Existing system?	
Requestor	
Division	
Date	

1. Please describe the video surveillance system (VSS) to be utilized and how its set-up adheres to the District's Video Surveillance policy. Attach floor/site plan with camera and equipment locations.

2. Provide justification for the use of a VSS at this particular facility or property including verifiable, specific reports of incidents of crime or significant safety concerns.

3. Video surveillance should only be considered after other measures of deterrence or detection have been considered and rejected as unworkable. Have the following security measures been considered and rejected as unworkable or less effective?

	Security Measure	Yes	No	Comments
A	Security Procedures			
B	Panic Alarms			
C	Door Locking Hardware			
D	Alarm System			
E	Access Control System			
F	Signage			
G	Security Officer / Officer Patrols			
H	Lighting			
I	Other – please specify			

4. An assessment should be conducted on the effects that the proposed VSS may have on personal privacy and the ways in which any adverse effects can be mitigated. Have the following effects and mitigation strategies been considered?

	Effects and Mitigation Strategies	Yes	No	Comments
A	Is the VSS proposed to be located in an area that will minimize property intrusion?			
B	Is the VSS proposed to be located in a location where the public and/or employees have a higher expectation of privacy (i.e. washroom or change room, etc.)?			
C	Is the location of the proposed VSS visible?			
D	Can the scope of the video surveillance be restricted to the recognized problem area?			
E	Is space allocated for adequate signage notifying the public of a VSS in use?			

5. The proposed design and operation of a VSS should minimize privacy intrusion. Have the following design and operation factors been considered for the proposed facility?

	Measures to mitigate privacy impact	Yes	No	Comments
A	Can the proposed VSS be restricted through hardware or software to ensure that it cannot be adjusted or manipulated to overlook spaces not contemplated in the PIA?			
B	Is the storage device going to be located in a strictly controlled access area?			
C	Can the storage device be installed in such a way that it will be hidden from public view?			
D	Are there other measures in place to mitigate privacy impact?			

6. Administration – please provide the following information related to this initiative:

   a. Who will be authorized to access video surveillance equipment (staff positions and/or potential vendors)?

   b. Where are recordings proposed to be stored? (e.g. network server on site, third party servers, on cloud, within or outside of Ontario or Canada)

   c. What security measures will be put in place to protect where the recordings are stored? (i.e. locked server room, logins/passwords, etc.)

   d. Does the system have the ability to be altered to protect the privacy of other individuals (i.e. blurring faces/license plates)?

   e. Does the system have the ability to audit who accessed it, when and what they did? (e.g. what video they reviewed, did they copy the video?)

f. Will the proposed VSS will be linked to other databases (e.g. FOB/Key access systems, Resident databases etc.)?

7. Prior to installing a VSS and where feasible to do so, the District should identify those individuals who reasonably may be affected by the VSS and consult with them on the system's necessity and impact.

	Stakeholder	**Particular Interest**	**Comment/Concerns**
A			
B			
C			
D			

PIA Recommendations:

Indicate recommendations for changes and/or approval.

Completed by (Print)			
Job Title			
Signature		Date	
Commissioner Authorization		Date	
FOI Coordinator Authorization		Date	

ADMINISTRATON POLICY – APPENDIX B

Name:	**Policy Number:**
Video Surveillance: Authorized User Confidentiality and Compliance Agreement	AD-014-2019 Appendix B

UNDERTAKING OF CONFIDENTIALITY AND COMPLIANCE WITH THE DISTRICT'S VIDEO SURVEILLANCE POLICY

I, (print name) _____, a District of Muskoka (employee, service provider or authorized consultant) understand that for the purposes of carrying out my duties on behalf of the District, I may have access from time-to-time to information from the District's video surveillance system in the execution of those duties, including surveillance video record(s) and digital video recorder(s) and related equipment.

I acknowledge and agree that:

1. All information belongs to the District of Muskoka.
2. The information shall be under the District's control and is subject to the *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56 (MFIPPA).
3. MFIPPA contains provisions that regulate and prohibit the disclosure of personal information. All video surveillance recordings ("information") will be considered personal, as defined in and protected by MFIPPA. The disclosure of any information (personal or otherwise) shall be only in accordance with this Undertaking and the District's Video Surveillance Policy (the Policy), as amended from time-to-time.

I further acknowledge and agree that:

4. I have reviewed and agree to comply with all aspects of the Policy.
5. All information is confidential and I will not access, copy, disclose or provide to any person, or otherwise deal with or use any information, including without limitation any details relating to information (whether personal or otherwise), except as specifically authorized by the District and in accordance with the Policy.
6. I will not use or refer to any information for any purpose other than as specifically authorized by the District as set out in the Policy.

To ensure that confidentiality is maintained, I agree to store any information that I have access to in a manner as directed by the District and in accordance with the Policy. I further agree not to destroy or remove any information from the District's premises except as specifically authorized by the District and in accordance with the Policy. I will not leave any information unsecured and will take all measures reasonably necessary to ensure that persons not authorized to view or access the information are not in any manner provided with such opportunities.

I will report any unauthorized access, copying, disclosure or other dealing or use of the information, of which I become aware, immediately to my supervisor, and will, at their request, cooperate fully with the District, the Office of the Information and Privacy Commissioner or any other investigative body in the investigation of same.

I acknowledge that failure to comply with this Undertaking or with the Policy and any related procedures may result in disciplinary action being taken or termination of my contract, as may be applicable, as well as civil or criminal liability.

Name (print)	
Job Title	
Signature	
Company Name	
Date	

THE DISTRICT MUNICIPALITY OF MUSKOKA

ADMINISTRATION POLICY – APPENDIX C

Name: Video Surveillance: Example of Video Surveillance Signage	**Policy Number:** AD-014-2019 Appendix C

ATTENTION

VIDEO CAMERA IN USE

Video Surveillance Cameras are in Use on this Property

Personal information collected by the Video Surveillance Cameras at this site is collected under the authority of The District Municipality of Muskoka and the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA). This information is used for the purpose of promoting public safety and reducing crime at this site.

The ***Video Surveillance*** policy can be accessed on the District's website www.muskoka.on.ca

Questions regarding the collection, use and disclosure of images recorded by the video surveillance system or the completed forms may be directed to:

Freedom of Information Coordinator,
70 Pine Street,
Bracebridge, ON, P1L 1N3,
Or by emailing clerk@muskoka.on.ca
Or by calling 705-645-2231

ADMINISTRATION POLICY – APPENDIX D

Name: Video Surveillance: Law Enforcement Officer's Request Form	**Policy Number:** AD-014-2019 Appendix D

RELEASE OF RECORD TO LAW ENFORCEMENT AGENCY UNDER SECTION 32 (G) OF THE MUNICIPAL FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

Section 32 (g) of the *Municipal Freedom of Information and Protection of Privacy Act (*MFIPPA) permits the disclosure of personal information by the District of Muskoka (the District) to a law enforcement agency in Canada for the purpose of aiding an investigation undertaken with a view to a law enforcement proceeding. Please refer to the District's Video Surveillance policy.

To ensure that personal information is only released in appropriate circumstances, this Law Enforcement Officer's Request form must be completed prior to any disclosures of District records containing personal information to law enforcement agencies.

It should be noted that:

- The law enforcement officer(s) should identify, in detail, the record requested, including the location of the video surveillance equipment, to ensure that only the specific record required for the investigation is disclosed.
- In the event that a specific record cannot be identified, and the law enforcement officer is requesting to search through a large volume of records or to gain access to a District controlled information system, the District's Freedom of Information Officer (FIO) should be contacted for further direction.
- If the law enforcement officer is presenting a subpoena, the FIO must be notified prior to any disclosure of records.

The following record is being requested under Section 32(g) of MFIPPA, which provides for the disclosure of records containing personal information for the purpose of aiding a law enforcement investigation.

This section to be completed by District Staff	
Record Requested	
Video Surveillance Camera Location	
Description of Record	

Name: Video Surveillance	**Policy Number:** AD-014-2019

This section to be completed by the attending Law Enforcement Officer	
Record Description	
Subject Name	
Occurrence / Investigation Number	
Warrant or Apprehension Number	
View Original Record	☐ Yes ☐ No
Copy Requested	☐ Yes ☐ No

I, _____ (print Officer's name) request the above personal information to aid an investigation undertaken by _____ (print Law Enforcement Agency) with view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result.

Signature of Law Enforcement Officer			
Badge / Identification Number		Date	
Signature of Authorized Staff Member		Date	

Questions regarding the collection, use and disclosure of images recorded by the video surveillance system or the completed forms may be directed to:

Freedom of Information Coordinator,
70 Pine Street,
Bracebridge, ON, P1L 1N3,
Or by emailing clerk@muskoka.on.ca
Or by calling 705-645-2231