**Valley Waste-Resource Management**
**Authority Approved Policy Statement**

| | |
|---|---|
| **Policy Name** | Video Surveillance Equipment Policy |
| **Policy Number** | AAP-29 |
| **Last Revision Date** | December 22, 2021 |
| **IMSA** | Under authority of Clauses 7(1) |

**Purpose**

To provide procedures for the effective management of video surveillance by the Valley Region Solid Waste-Resource Management Authority that enhances the safety and security of employees, members of the public, and Authority's assets and property, including preventing and deterring crime, identifying suspects, and gathering evidence, while minimizing privacy intrusion.

This Policy has been developed in keeping with the terms and conditions of the Intermunicipal Services Agreement and more specifically applies to Clause 7(1) within the Agreement.

**Definitions**

In this policy,

a. "Access & Privacy Officer" means the responsible officer under Part XX of the MGA, being the General Manager, or his or her delegate;

b. "Authority" means the Valley Region Solid Waste-Resource Management Authority;

c. "Authority property" means any real property or other asset owned or leased, and operated directly by the Authority.

d. "camera system" or "system" means security camera equipment, including cameras, monitors, and associated control and storage equipment that allow for remote viewing of images and/or audio captured within the field of vision of the cameras;

e. "General Manager" means the General Manager as engaged by the Authority to oversee the umbrella of programs and services offered by the Authority;

f. "contractor" means a corporate entity or an individual performing work on behalf of the Authority under contract;

g. "covert video surveillance" means the use of hidden or non-disclosed system(s) for law enforcement purposes, to respond to a specific threat to the safety and security of employees, members of the public, or property, or to assist with internal investigations;

h. "digital recordings" means the images, data, and associated records created and retained as a result of the Authority's use of a camera system;

i. "employee" means any person categorized as permanent, term, full-time, part-time, casual, contract, seasonal, temporary, or student worker in the employ of the Authority, as well as volunteers;

j. "internal investigation" means an investigation undertaken by the Authority where alleged improper conduct by an employee has been identified, including actions or omissions that are in breach of policies, procedures, or work-related instructions;

k. "MGA" means Municipal Government Act;

l. "personal information" has the same meaning as defined in Part XX of the MGA;

m. "secure" means to copy a portion of a digital recording to an external storage device such as a hard drive or flash drive;

**Principles Supporting Policy**

The appropriate use of video surveillance, combined with other safety and security measures, is a necessary and effective means of achieving the enhanced safety and security of employees, members of the public, and the Authority's assets including real property.

The Authority recognizes the need for synergies between an individual's right to privacy and the Authority's duty to promote and maintain safe and secure environments and protect property. Every attempt has been made to ensure that this Policy has been developed in keeping with the Video Surveillance Guidelines as prepared and released by the Office of the Information and Privacy Commissioner of Nova Scotia.

**Responsibility**

The Authority, in consultation with the General Manager will:

- Ensure that the Valley Region Solid Waste-Resource Management Authority has in place a comprehensive Video Surveillance Equipment Policy;

- Review, amend and adopt changes to the Video Surveillance Equipment Policy on a regular and timely basis.

**Policy**
This policy applies to camera systems on all Authority-owned property.

This policy does not apply to covert video surveillance.

Nothing in this policy limits the ability to develop and implement policies relating to the use of digital recordings for the management of employees.

**Installation**
The decision to install a camera system on Authority property shall be made by the General Manager, or at the direction of the Authority.

When considering the installation of a camera system on Authority property, the following criteria shall be considered and documented by the General Manager or delegate:

a) the existence of demonstrated and significant safety or security concerns at the location, or at similar locations to the location, where placement of a camera system is being proposed;

b) what measures, other than the installation of a camera system, are available to address identified safety or security concerns;

c) whether measures other than the installation of a camera system would be effective in addressing the identified safety or security concerns;

d) the effect that the proposed placement of a camera system may have on personal privacy, and the ways in which privacy intrusion can be minimized;

e) the operational requirements of the Authority; and

f) any other criteria deemed relevant by the General Manager.

The General Manager shall recommend whether a full Privacy Impact Assessment is required.

Where circumstances require the immediate installation of a camera system, the General Manager will recommend whether or not a full Privacy Impact Assessment is required as soon as possible after installation as is practicable and adjustments, up to and including removal, will be made if required in respect of the installation once the review is complete.

**Signage**

a) Where a camera system is permanently installed on Authority property, the General Manager shall post signage in a conspicuous place in close proximity to the system, advising employees and members of the public that the area is monitored by a camera system, the authority for doing so, the principle purpose(s) for which the digital recordings is intended to be used, and the telephone number of someone who can answer questions about the collection of digital recordings.

b) Notwithstanding (a), if a sign cannot physically be posted in a conspicuous place in close proximity, it shall be posted in the general vicinity.

c) Where a number of camera systems are placed in a location, it shall be sufficient to display a single sign in a conspicuous place at or near the entry point advising those entering the location that it is being monitored by a camera system.

A camera system shall not be installed in areas where employees or members of the public have a higher expectation of privacy, including within a washroom or change room.

To the extent possible, a camera system shall:

a) be focused on the location identified as having the need for video surveillance, and

b) have the ability to be adjusted or manipulated to restrict overlooking spaces not intended to be monitored.

To the extent possible, video displays of digital recordings should not be located such that the public or unauthorized staff may view the images.

A camera system may operate at any time in a twenty-four-hour period.

The General Manager shall maintain an inventory of all camera systems under their control.

**Use of Digital Recordings**

Digital recordings obtained through a camera system may be used by the Authority to:

a) enhance the safety and security of employees, contractors and members of the public who are on Authority property;

b) safeguard Authority property and other assets;

c) detect and deter criminal activity by providing law enforcement agencies with evidence related to possible unlawful activities;

d) manage risk to the Authority including workplace accidents and/or injuries, incidents, complaints, claims, or potential claims involving the Authority; and

e) undertake internal investigations, as authorized by the General Manager.

The General Manager may secure digital recordings from an identified time and location for any of the purposes set out above.

**Custody and Control of Digital Recordings**

The Authority is responsible for the custody and control of digital recordings applicable to this policy.

Camera system recording equipment shall be located such that only individuals authorized by the General Manager may access the equipment.

All wireless transmissions of digital recordings shall be encrypted.

The General Manager may designate employees or contractors who are authorized to access a camera system and digital recordings for the purpose of:

a) monitoring a given location;
b) retrieving, downloading, viewing, and/or securing a digital recording; and
c) performing maintenance and repairs on the system.

The General Manager shall maintain a list of individuals authorized to access a camera system.

**Third-party Access to Digital Recordings**

Third parties may request access to digital recordings in the following manner:

a) an application pursuant to MGA Part XX;
b) as part of a legal action against the Authority; or
c) by way of a court order or otherwise as provided for by law.

Law enforcement personnel may request access to digital recordings for law enforcement or investigative reasons by contacting the General Manager.

A third party who is given access to digital recordings may be required to acknowledge in writing his or her duties, obligations, and responsibilities with respect to the confidentiality, use, and disclosure of the digital recordings.

Any unauthorized access to digital recordings or camera system shall be reported to the General Manager for investigation.

Any employee who provides digital recordings to unauthorized parties, either as a result of intentional wrongful disclosure or disclosure caused by negligence, may be subject to disciplinary action, up to and including dismissal.

Any contractor who provides digital recordings to unauthorized parties, either as a result of intentional wrongful disclosure or disclosure caused by negligence, may be subject to termination of their contract.

**Retention and Disposal of Digital Recordings**

The Authority may develop retention periods for digital recordings, including the length of time such recordings are to be maintained, and the General Manager may develop different retention periods for those digital recordings that have been secured depending upon the circumstances.

Digital recordings that have been secured in response to a request shall be retained in accordance with the legal and records management requirements of the request.

Where digital recordings that have been secured in response to a request for access or a request to secure are subsequently used to make a decision that directly affects an individual, they shall be retained for a minimum of one year.

Digital recordings for which no request to secure has been received by the General Manager shall not be retained for longer than 60 days. A camera system may record over such existing recordings.

Secured digital recordings shall be disposed of in a manner that ensures that personal information is erased and cannot be retrieved or reconstructed. Disposal methods may include use of Kill-disk, shredding, burning, or erasing depending on the type of storage device.

**Transition**

The guidelines for installation of a camera system do not apply to a camera system installed prior to the adoption of this policy until three years from the coming into force of this policy.

Chair of the Authority Board

Jan 6/22
Date

General Manager

Dec 22/2021
Date