Municipality of Dysart et al
Policies and Procedures Manual

Video Surveillance Policy

Policy No. 59

Purpose

The Municipality of Dysart et al is committed to public safety, crime prevention, and stewardship of publicly owned assets. Where warranted, Dysart may use video surveillance systems in Dysart-owned or operated buildings and open spaces to deter and detect crime and anti-social behavior such as theft, vandalism, and unauthorized entry.

Dysart shall maintain control of and responsibility for its video surveillance system at all times.

Guiding Principles

When conducting video surveillance of the public, the Municipality of Dysart et al will:

- collect data only when authorized by a statute, required by law enforcement, or when necessary to the proper administration of a lawfully authorized activity;
- minimize the amount of data collected;
- retain data for no longer than required;
- only use data for the purpose for which it was collected;
- take all reasonable measures to prevent unauthorized access to collected data and inadvertent destruction of, or damage to, collected data;
- notify individuals, through the use of signage, when video surveillance is in use;
- not disclose collected data unless disclosure is:
    - with consent from the individuals whose personal information appears in the images;
    - in response to a Freedom of Information request;
    - or requested by law enforcement to aid an investigation.

Definitions

Act(s) means the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).

Authorized staff refers to employees of the Municipality of Dysart et al or to a Municipality of Dysart et al contractor who are specifically authorized by Municipality of Dysart et al to operate the video surveillance system for a particular facility and to perform the duty, responsibility or action described in this policy.

Disclosure refers to the release of relevant information. Disclosure includes viewing recordings or recorded images, as well as making copies of recordings or images.

Freedom of Information Request is a formal request for access to records made under the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).

Personal Information as defined by MFIPPA means recorded information about an identifiable individual including:

- Information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation, or marital or family status of the individual;
- Information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to the financial transactions in which the individual has been involved;
- Any identifying number, symbol, or other particular assigned to the individual;
- The address, telephone number, fingerprints or blood type of the individual;
- The personal opinions or views of the individual except if they relate to another individual;
- Correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence;
- The views or opinions of another individual about the individual, and
- The individual's name if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

Record means any record of information, however recorded, whether in printed form, on film, by electronic means or otherwise, and includes: a photograph, a film, a microfilm, a videotape, a machine-readable record, and any record that is capable of being produced from a machine-readable record.

Retention Period is the period of time during which specific records series must be kept before records in that records series may be disposed of.

Video Surveillance means a video, physical or other mechanical, electronic, digital or wireless surveillance system or device that enables continuous or periodic video or image recording, observing or monitoring of information about individuals in open, public spaces. In this policy, the term video surveillance system includes an audio device, thermal imaging technology or any other component associated with capturing the image of an individual.

Procedures

Authority

Video security surveillance systems are a resource used by Dysart at selected sites within the management jurisdiction of Municipality of Dysart et al for the purpose of increasing the safety and security of residents, staff and members of the public, to protect public safety, our corporate assets and property and to detect and deter criminal activity and vandalism.

Municipality of Dysart et al is authorized to conduct video surveillance under Section 28(2) of the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) or Section 38(2) of the Freedom of Information and Protection of Privacy Act (FIPPA), as applicable. Dysart recognizes that video surveillance technology has the potential for infringing upon an individual's right to privacy and although video surveillance technology may be required for legitimate operational purposes, its use must be in accordance with the provisions of MFIPPA or FIPPA, as applicable, and any other applicable privacy laws.

Compliance

Municipality of Dysart et al collection and storage of, and access to, information recorded from video surveillance shall conform to published guidelines and specific direction as may be provided by the Information and Privacy Commissioner of Ontario (IPC) from time to time.

Public Consultation

Dysart acknowledges the importance of public consultation when new or additional video surveillance systems are considered for Dysart owned buildings and property. The extent of public consultation may vary depending on the extent of public access.

When new or additional video surveillance installations are being considered for open public spaces, Dysart shall consult with relevant stakeholders and the public to determine the necessity and acceptability.

When new or additional video surveillance systems are being considered for Dysart-owned or operated buildings to which the public are invited, such as a library branch, notice shall be provided at the site with an opportunity for public feedback.

When new or additional systems are contemplated inside Dysart buildings or parking lots where there may be a high risk to staff or clients, consultation shall not be required.

Roles and Responsibilities

Dysart Council
Dysart Council shall be responsible for authorizing the installation of video surveillance systems.

Dysart CAO
Dysart CAO shall be responsible for implementation, administration and evaluation of Dysart's Video Surveillance Policy and Procedures.

The CAO shall also be responsible for ensuring that information obtained through video surveillance is used exclusively for lawful purposes.

Dysart CAO, and the County of Haliburton Director of IT
The CAO, and the Director of IT shall be responsible for granting authorized access to employees or contractors operating on behalf of Municipality of Dysart et al.

The Director of IT shall also ensure that video surveillance systems are deployed with proper security measures including strong authentication and access, controls, audit logging, and encryption.

Facility Manager
The Department Head responsible for each Dysart-owned or operated site with a video surveillance system (the "Facility Manager") shall ensure that the site complies with this policy, as well as any site-specific policies that may be required.

Authorized Staff
Staff with authorized access to the monitoring equipment and recorded information shall be trained in its use in accordance with this policy. Authorized staff shall sign a written confidentiality agreement regarding their duties under the Policy and the Acts. Breaches of the policy may result in disciplinary action in accordance with Dysart's Code of Conduct.

Location and Use of Surveillance Equipment

Video Surveillance Cameras
Dysart shall install video surveillance cameras in identified public areas only where video surveillance is a necessary and viable detection or deterrence activity.

Dysart may install visible and/or hidden surveillance cameras, but Dysart shall not install equipment inside areas where the public and employees have a higher expectation of privacy (e.g. change rooms and washrooms).

Where cameras are not visible, Dysart shall ensure that appropriate signs are installed in accordance with this policy.

Video Surveillance Equipment
Dysart shall ensure that video monitors are accessed only by authorized Dysart staff or authorized Contract Service Provider's staff, and are not located in a position that enables public viewing. Dysart shall encourage that monitors are turned off except when needed to ensure the system is operating or to view the video recording devices.

Dysart shall ensure that video recording equipment is located away from the public, in restricted access areas, preferably in locked rooms with keyed access.

All storage devices used in the recycling rotation, awaiting review by police, or in storage post police review shall be stored in a locked cabinet at all sites, with access restricted to authorized staff.

Strong authentication and access controls as well as audit logging will be implemented to prevent unauthorized access to video surveillance equipment.

Where possible, all video surveillance data shall be encrypted whether in storage or in transit.

Location Record
Dysart shall ensure that maps and floor plans are prepared to identify the location of all video surveillance equipment at each of the respective sites. Dysart's Clerk shall have copies of all such maps and plans, and each Facility Manager/Coordinator shall have a copy for their site.

Hours of Operation

The majority of the video surveillance systems shall operate 24 hours per day during the season the facility is open. Personal information shall be accessed only in response to an incident.

Retention and Destruction
Since short retention periods minimize risk of improper use and disclosure, Dysart shall ensure that there is a standard retention period at all sites.

Video recording shall be deleted in rotation in a seven (7) day, one (1) week cycle. If the video data has been used or disclosed, it must be retained for a minimum of 1 year.

Dysart will take reasonable measures to protect against inadvertent destruction or damage of surveillance video.

Data storage devices no longer in use, will be securely disposed of in a manner that overwrites data in such a way that it cannot be retrieved. Devices that are no longer

functional or that cannot otherwise be securely wiped, will be physically destroyed in a manner that renders the data unrecoverable.

Access to, and Disclosure of, Recorded Information

Accessing Recorded Video
Dysart shall ensure that surveillance video only be viewed by staff on a need-to-know basis, in order to limit the number of people who have access to surveillance video.

Authorized staff shall only view surveillance video for the purpose for which it was collected. For example, if the purpose of video surveillance is to deter and identify individuals involved in crime or vandalism, authorized staff shall:

- review surveillance video only if there is reasonable cause to believe that a crime or an act of anti-social behavior has been or is in the process of being committed;
- and only access data related to these specific incidents.

Only staff involved in the investigation of these incidents shall view video surveillance.

Disclosure to Law Enforcement Agencies
Disclosure of video surveillance should be made to a law enforcement agency only upon the presentation by the authorities of a warrant or court order for the same and upon completion of a form setting out the name of the individual(s) who took the storage device, under what legal authority, the date and whether the storage device will be returned or destroyed after its use by the authorities.

Dysart has the discretion to disclose information to a law enforcement agency in Canada without a court order, to aid an investigation.

Dysart may disclose personal information to a law enforcement agency on its initiative, where it has a reasonable basis to believe that an offence has occurred. However, it should disclose only the information that appears to be relevant and necessary for a potential investigation.

If staff has reason to believe that the video contains personal information for law enforcement or public safety purposes, they shall notify the law enforcement agency and immediately contact IT who shall copy the video from the hard drive, to another storage medium and set aside in a clearly marked manner in the locked storage cabinet until retrieved by the law enforcement agency.

Disclosure for Health and Safety Reasons
Dysart may disclose personal information in compelling circumstances affecting the health or safety of an individual. This includes disclosure to a law enforcement agency, whether in response to a request or on Dysart's initiative.

Before disclosing personal information to a law enforcement agency for health or safety reasons, Dysart must be satisfied that:

- there are compelling concerns about an individual's health or safety, having considered:
    - the likelihood of the harm occurring
    - the severity of the harm
        - how soon the harm might occur, and
- the disclosure is reasonably likely to reduce the risk of harm to the individual

Dysart will limit the disclosure to the information relevant to reducing the risk.

If disclosing information under for Health and Safety reasons, Dysart must make reasonable efforts to notify individuals, in writing, that their information was disclosed.

Access Log
Dysart shall provide each site with a video surveillance system with an electronic Access Log file. Access to the Access Log file(s) shall be restricted to authorized personnel only.

The Access Log shall be used to record the date, time, purpose and name of authorized staff person reviewing video.

When a video is viewed or removed for law enforcement purposes, the log entry shall include the date, time, name and contact information of the law enforcement officer.

The Access Log shall also be used to track requests for personal information including the date, time, name and contact information.

Inadvertent Disclosures
Dysart shall ensure that inadvertent disclosures are addressed in a timely and effective way. Staff shall immediately report the incident to their Facility Manager, who shall immediately notify the Clerk. The Clerk shall attempt to retrieve the personal information that has been inappropriately disclosed, commence an investigation and notify the Information and Privacy Commission.

Public Notification & Access to Information

Signage
Dysart shall ensure that the public is notified about the presence of video surveillance equipment by prominently posting signs at the perimeter of surveillance areas.

Signs shall be of consistent size and format and convey the following information: indicate video surveillance in use; identify legal authority for collection of personal information (section 28 (2) of the Act); and provide title, address and telephone number of contact person who can answer questions about the system. (see appendix attached)

Other Promotion
Dysart shall also ensure that information regarding this policy is readily available at all sites with video surveillance systems and on Dysart's website.

Personal Access to Information
Dysart recognizes that an individual whose personal information has been collected by a video surveillance system has a right to access his or her personal information under the Act. Such requests will be directed in a timely manner to Dysart Clerk.

Annual Audit and Evaluation

Dysart CAO and Clerk shall conduct an annual review of Dysart's Video Surveillance Policy/ System to ensure that:

- Video surveillance continues to be justified and, if so, whether its use can be restricted;
- Reported incidents and police contact are properly recorded in the logbooks;
- Used videos are being properly retained;
- Video is being deleted in accordance with time frames and security measures are being followed; and
- Any formal or informal information requests from public have been tracked.

Policy Review

Dysart shall periodically review the Video Surveillance Policy pending the outcome of the annual audit and evaluation or at any time Dysart is considering changing or adding new video surveillance systems.