If this information is required in an accessible format, please contact 1-800-372-1102 ext. 3702

Durham Region Transit Report

To:	Durham Region Transit Executive Committee
From:	General Manager, Durham Region Transit
Report:	#2024-DRT-14
Date:	September 4, 2024

Subject:

Updated Surveillance System in DRT Vehicles Policy

Recommendation:

That the Transit Executive Committee recommends:

That the revised Surveillance System in DRT Vehicles Policy, effective September 4, 2024, be approved.

Report:

1. Purpose

1.1 This report seeks approval for revisions to DRT's Surveillance System in DRT Vehicles Policy.

2. Background

2.1 Video and audio recording systems were first installed in DRT vehicles with the introduction of the PULSE bus fleet in 2013. The Durham Region Transit Commission approved the original Onboard Security Video Surveillance Policy, on September 5, 2012, and further directed that the DRT's surveillance policy be separate from the Region's facility-related video surveillance policy.

2.2 In 2018, DRT procured the current onboard surveillance system which is installed throughout the DRT fleet.

2.3 During the recent bi-annual review of the Policy, several minor revisions were identified to ensure consistency with corporate record retention policies and to better reflect current operational practices.

3. Previous Reports and Decisions

3.1 #2022-DRT-17 Updated Surveillance System in DRT Vehicles Policy

3.2 #2019-DRT-13 Updated Surveillance System in DRT Vehicles Policy

3.3 #2018-DRT-20 Updated Surveillance System in DRT Vehicles Policy

3.4 #2012-DRT-18 Surveillance System in DRT Vehicles Policy

4. Discussion

4.1 Principles of the original policy remain unchanged, balancing an individual's right to privacy and the need to protect the safety and security of the public transit network and the community, specifically passengers, pedestrians and DRT employees and assets, to investigate personal injury and other legal claims and proceedings, and to investigate and resolve operational matters as they may occur.

4.2 The proposed policy has been revised to be consistent with corporate record retention requirements and other minor changes.

a. Format revisions
b. Revised retention schedule
c. Updated list of designated personnel able to view and/or retrieve Surveillance Recordings

4.3 The recommended policy (Attachment #2) has been reviewed by Legal Services, Labour Relations, and the Access and Privacy Office.

5. Financial

5.1 There are no financial impacts associated with this report.

6. Relationship to Strategic Plan

6.1 This report aligns with/addresses the following strategic goals and priorities in the Durham Region Strategic Plan:

a. Service Excellence

7. Conclusion

7.1 It is recommended that TEC approve the revised Surveillance System in DRT Vehicles (Attachment #2).

8. Attachments

8.1 Attachment #1: Proposed revisions to current policy: Surveillance System in DRT Vehicles, September 7, 2022.

8.2 Attachment #2: Revised policy: Surveillance System in DRT Vehicles, effective date September 4, 2024

Respectfully submitted,

Original Signed by

Bill Holmes
General Manager, DRT

Recommended for Presentation to Committee

Original Signed by

Elaine Baxter-Trahair
Chief Administrative Officer

Policy Manual

Title: Surveillance System in DRT Vehicles	
Issued: September 5, 2012	**Page #: 1 of 13**
Revised: ~~July 1, 2019~~ September 4, 2024	
Approved by: General Manager	

1. Policy Statement

1.1 It is the policy of Durham Region Transit (DRT) to utilize a Surveillance System on transit vehicles to

- Ensure the safety and security of passengers, pedestrians, and DRT employees and assets;
- Investigate personal injury and other legal claims and proceedings; and
- Investigate and resolve Operational Matters.

1.2 DRT recognizes the need to balance an individual's right to privacy and the need to ensure the safety and security of the public transit network and the community. Although a transit bus is a public space, this policy is consistent with the principle of data minimization, which entails limiting the amount of personal information collected and retained to that which is necessary to fulfill the purposes of the lawfully authorized activity. DRT is committed to providing a safe and secure transit system for employees, passengers and pedestrians, and activities and systems that contribute to safety and crime prevention in the community.

1.3 While surveillance systems are installed on vehicles for criminal, safety, security, investigatory, and evidentiary reasons, DRT's Surveillance System is designed to minimize privacy intrusion. Proper surveillance, where deemed necessary, is one of the most effective means of helping to keep the DRT transit system operating in a safe, secure, and privacy protective manner.

1.4 This Policy has been developed to govern the Surveillance System for DRT vehicles, as more particularly set out in Section 2.1, and in accordance with the privacy provisions of the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and the Privacy and Video Surveillance in Mass Transit Systems report (2008) from the Ontario Information and Privacy Commissioner.

2. Definitions

FOI	Freedom of Information
MFIPPA	Municipal Freedom of Information and Protection to Privacy Act
Monitor	Active observation of Surveillance Recordings in real time, or systematic observation of Surveillance Recordings without a reasonable cause
Operational Matter	Incident, event or occurrence in relation to a DRT vehicle or employee
Personal Information	As defined by MFIPPA
Remote Access	Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet)
Surveillance Recordings	Information, including audio and video, recorded by the Surveillance System and stored on a Digital Video Recorder (DVR) or other storage device.
Surveillance Records	Copies of Surveillance Recordings, created for the purpose of: a) complying with any warrant, summons, court order or other legal process that requires disclosure of Surveillance Recordings; b) complying with Freedom of Information requests and MFIPPA; c) supporting investigations of personal injury and other legal claims and proceedings; and d) supporting investigations into Operational Matters.
Surveillance System	The physical or other mechanical or digital components of the Surveillance System installed on the vehicle or in a building, that enable continuous video and audio recording, observing or monitoring of the inside and outside of the vehicle, and for viewing Surveillance Recordings and producing Surveillance Records

2.1 Surveillance System

A. DRT's Surveillance System may include the use of video and audio recording equipment/device.

B. DRT may use its Surveillance System on transit vehicles, including ~~conventional and specialized vehicles~~ **DRT buses** ~~and specialized transit vehicles~~**, contracted service provider vehicles used to deliver DRT services,** and DRT non-revenue vehicles.

C. Surveillance System equipment/devices at facilities will be installed within secure locations

2.2 Application

A. This Policy is implemented by DRT staff. DRT contractors and service providers, and any third party who have responsibilities related to the Surveillance System will be made aware of this Policy, given instruction in meeting the Policy's requirements, and be required to agree in writing to comply with the requirements of this Policy.

B. Surveillance Recordings will be used only for the purposes of detecting, deterring and investigating unlawful and safety/security activities, investigating personal injury and other legal claims and proceedings, and investigating and resolving Operational Matters.

C. DRT staff will not monitor the Surveillance System.

D. Surveillance Recordings will not be used to monitor the performance of employees. Behaviors observed when reviewing Surveillance Recordings while investigating an Operational Matter will be managed according to established labour relations practices, which may include, without limitation, the use and reliance of Surveillance Recordings for employee development and/or discipline.

2.3 Exceptions

This policy does not apply to the following:

a) Covert surveillance used for law enforcement purposes. In those circumstances, either a statutory authority exists and/or the authority for the surveillance is lawfully obtained through a search warrant. Covert surveillance is surveillance conducted using hidden devices. If covert surveillance is not implemented pursuant to the conditions in the preceding paragraph, extra diligence in considering the use of the technology is required.
b) Surveillance System components installed at Regional buildings including transit facilities, which are managed by Facilities Management

3. Roles and Responsibilities

3.1 General Manager, DRT:

The General Manager may delegate responsibilities under this Policy.

a) Review the Policy every two years and forward to the Transit Executive Committee recommendations that will significantly alter the Policy.
b) Receive and review status updates and audit results, and implement the recommendations accordingly.

c) Designate appropriate staff to view Surveillance Recordings and produce Surveillance Records.
d) Review requests for Surveillance Records and where such requests comply with MFIPPA and this Policy, authorize the Administrator to produce a copy of the appropriate Surveillance Recording(s).
e) Immediately contact the Corporate Privacy Office and work with privacy staff to investigate any alleged privacy breach of this Policy.

3.2 Deputy **General** Manager, Business Services

The Deputy General Manager may delegate responsibilities under this Policy.

a) Ensure assigned staff comply with this Policy as it relates to privacy, storage, dissemination, and documentation for disclosure of information.
b) **Manage the administrator requirements of the Surveillance System platform**.
c) In consultation with the appropriate staff, develop training for DRT and contract staff regarding obligations and compliance with the MFIPPA and this Policy.
d) In consultation with the appropriate staff, coordinate technical requirements and activities related to design, functionality, installation, **maintenance**, and upgrades to the Surveillance System.
e) Establish an appropriate employee on- and off-boarding process to ensure activation and deactivation of access to the Surveillance System.
f) Ensure completion of a semi-annual review of user access to ensure only authorized users have access to view Surveillance Recordings.
g) Immediately report all alleged privacy breaches of this Policy to the General Manager and in their absence, the Corporate Privacy Office.

3.3 Deputy General Manager, Operations

The Deputy General Manager may delegate responsibilities under this Policy.

a) Ensure assigned staff comply with this Policy as it relates to privacy, storage, dissemination and documentation for disclosure of information.
b) Approve the locations on vehicles for installation of the Surveillance System in accordance with this Policy.
c) Consult with the Regional Clerk/Director of Legislative Services and /or Legal Services, for any issues related to MFIPPA requests.
d) Support the Deputy General Manager, Business Services, to develop training for DRT and contract staff regarding obligations and compliance with the MFIPPA and this Policy.
e) Immediately report all alleged privacy breaches of this Policy to the General Manager and in their absence, the Corporate Privacy Office.

3.4 Deputy General Manager, Maintenance

The Deputy General Manager may delegate responsibilities under this Policy.

a) Ensure assigned staff comply with this Policy as it relates to privacy, storage, dissemination, and documentation for disclosure of information.
b) Ensure that Surveillance System equipment on DRT vehicles is maintained in a state of good repair.
c) Delegate day-to-day maintenance of the Surveillance System on DRT Vehicles to designated staff, as appropriate.
d) Support the Deputy **General** Manager, Business Services, to develop training for DRT and contract staff regarding obligations and compliance with the MFIPPA and this Policy.
e) Immediately report all alleged privacy breaches of this Policy to the General Manager and in their absence, the Corporate Privacy Office.
f) Manage daily operational requirements for the Surveillance System.
g) Ensure assigned staff comply with this Policy.
h) Ensure records of activities related to accessing Surveillance Recordings are maintained as outlined in this Policy.
i) In consultation with the Deputy General Manager, Business Services, ensure relevant staff are trained in compliance with the MFIPPA and this Policy.

3.5 Supervisors, Operations

a) Report any Surveillance System defects to maintenance staff.
b) Document required information when accessing Surveillance Recordings.
c) Ensure no personal information obtained from Surveillance Recordings are disclosed to anyone without the approval of the applicable Manager.
d) Forward requests for a Surveillance Record to the Deputy General Manager, Operations.

3.6 Administrator

a) When approved by General Manager or designate, create required Surveillance Records.
b) Monitor and track requests and copies of Surveillance Records according to MFIPPA, this Policy, and corporate records management requirements.
c) Oversee all documentation required and generated to implement this Policy.

3.7 Director, Human Resources

a) Provide guidance on use of Surveillance Recordings in investigations where employee information has been captured.

3.8 Access and Privacy Office

a) Administer requirements of MFIPPA.
b) Coordinate with DRT to ensure compliance to MFIPPA and statutory obligations.

c) Respond to any inadvertent disclosures of personal information or any privacy complaints made to the Region or DRT, or Information and Privacy Commissioner (IPC)/Ontario and comply with Orders issued.

d) In consultation with the Deputy General Manager, Business Services, ensure relevant staff are trained in compliance with the MFIPPA and this Policy.

3.9 Corporate Services – Information Technology (CS-IT)

a) Service and support of the computer and Windows operating system used for the Surveillance System.
b) Service and support of the DRT network such as to facilitate remote access, except where the network is a component of the Surveillance System

3.10 Authorized Users, Contracted Service Providers

a) Ensure all relevant staff comply to the requirements of this policy.
b) View Surveillance Recordings **in person at a DRT facility in the presence of a Transit Manager, Operations or designate**, when appropriate to investigate relevant Operational Matters.
c) Ensure any Surveillance System defects are reported to the appropriate designated DRT staff.
~~d) Document required information when accessing Surveillance Recordings.~~
e) Ensure no personal information obtained from Surveillance Recordings are disclosed to anyone without the approval of the applicable **DRT** Manager.
f) Forward requests for a Surveillance Record to the Administrator.
g) Prohibited to disclose, access or use information recorded by the Surveillance System, its components, files, or database for personal reasons, nor disclose, dispose, destroy, erase or alter any record without proper authorization from the Deputy General Manager, Operations, and without following the terms and conditions contained in this Policy.

3.11 Employees of DRT and Contracted Service Providers

a) Prohibited to disclose, access or use information recorded by the Surveillance System, its components, files, or database for personal reasons, nor disclose, dispose, destroy, erase or alter any record without proper authorization from the Deputy General Manager, Operations, and without following the terms and conditions contained in this Policy.

3.12 DRPS

a) DRPS shall comply with the Memorandum of Understanding that provides DRPS access to Surveillance Recordings from DRT vehicles.
b) DRPS employees will submit requests to view Surveillance Recordings to the DRPS video analysis group.

c) DRPS video analysis group will access the Surveillance System to view the appropriate Surveillance Recordings for investigative purposes.
d) Video analysis group will forward requests for a Surveillance Record to the Administrator, to be used strictly for investigative purposes.
e) Provide secure DRPS evidence link to the Administrator to upload Surveillance Recording.

4. Guidelines: Implementation of a Surveillance System

4.1 Designing Installing and Using Surveillance System Equipment

When designing a Surveillance System and installing related equipment, the following must be considered:

a) The ability to adjust cameras will be restricted to designated **business services and** maintenance staff, so that cameras cannot be manipulated to overlook spaces that are not intended to be monitored by the surveillance program.
b) Reception/recording equipment must be in a strictly controlled access area or system. Only staff designated by the appropriate Deputy General Manager will have access to the controlled access area/system and the reception/recording equipment.
c) Every reasonable attempt should be made to ensure Surveillance System equipment is not in a position that enables the public and/or unauthorized staff to view images.
d) Surveillance Recording components and related equipment will be installed at locations set out in Section 2.1 of this Policy, which may be amended from time to time.

4.2 Notice of Use of Video Recording System

a) DRT will post decals, visible to members of the public, at all entrances and/or prominently displayed on the perimeter of the vehicles with a Surveillance System installed.
b) The notification requirements of this decal must inform individuals of the legal authority for the collection of personal information; the principal purpose(s) for which the personal information is intended to be used; and the title, business address, and telephone number of someone who can answer questions about the collection.

4.3 Personnel Authorized to Operate and Maintain Surveillance System Equipment

Only authorized agents or personnel assigned by the General Manager or designate, as specific in Schedule A, will be permitted to operate the Surveillance System, to view Surveillance Recordings, create Surveillance Records and maintain the Surveillance System installed on DRT vehicles. All employees and representatives of third parties with responsibilities outlined in this Policy, will acknowledge in writing that they have received training with respect to their responsibilities and confidentiality obligations, and that they understand those obligations.

4.4 Breach of Policy

The General Manager, Municipal Freedom of Information and Protection of Privacy Coordinator, Director Human Resources, and Legal Services, as needed, will investigate and respond to any breach or alleged breach of this Policy.

5. Surveillance Equipment/Records

5.1 Types of Recording Devices

DRT may use a Digital Video Recorder system (DVR) and may implement technology replacements and/or upgrades, as required.

5.2 Record Identification

All Surveillance Records will be clearly identified (labelled) as to the date and location of origin including being labelled or titled with a unique, sequential number or other verifiable symbol. On a vehicle or in a facility with a DVR that stores recordings/information directly on a hard drive, the computer time and date stamp will be understood to be this identification.

Each user or facility, as applicable, will maintain records of activities related to recording devices and records according to the Region's Records Retention By-law. The activities include information regarding the use, maintenance, access and storage of recorded material.

5.3 Remote Access

DRT may use remote access to retrieve, view, operate, maintain or audit all or part of the Surveillance System. DRT further reserves the right to provide remote access to law enforcement agencies for law enforcement purposes. Any remote access provided to law enforcement agencies will contain a provision allowing DRT to conduct annual audits relating to the use and disclosure of information obtained through the Surveillance System and any such audits will be performed in accordance with this Policy.

Where the Surveillance System does not provide appropriate electronic recording of user activities, physical logbooks will be maintained to record all activities related to Surveillance System devices and records. The activities include all information regarding the use, maintenance and storage of records; and all instances of access to, and use of, recorded material. All entries will include name of authorized agent, date, time and activity. The logbook or electronic alternative must remain in a safe and secure location.

6. Auditing

6.1 DRT will undertake an internal audit every two years to ensure adherence to this Policy. Auditing may include verification that reported incidents were properly recorded; procedures on security; established roles and responsibilities; maintenance, storage, retention and disposal of equipment and recorded information have been followed; and requests for information have been tracked and responded to accordingly.

Any deficiencies, concerns and/or recommendations identified will be resolved.

6.2 General Manager or designate will conduct a bi-annual review of user access to ensure only authorized users have access to view Surveillance Recordings.

7. Access to Surveillance Recordings

7.1 Access

Access to Surveillance Recordings will be restricted to authorized agents specified in Appendix A, to comply with the roles and responsibilities as outlined in this Policy.

7.2 Storage

All storage devices that are not in use must be stored securely in a locked receptacle located in an access-controlled area.

7.3 Viewing Surveillance Recordings

Only authorized personnel or agents listed in Schedule A, are permitted to view and retrieve Surveillance Recordings. Surveillance Recordings will be viewed in a controlled area. Every reasonable attempt will be made to ensure that recordings are not viewable or can be heard by other individuals.

7.4 Access to Information Requests

All requests for Surveillance Records where disclosure may be inconsistent with the principle purposes of the collection will be directed to the Regional Clerk/Director of Legislative Services for processing. A person requesting access to a Surveillance Record is required to follow the requirements of the Region of Durham in making a Freedom of Information (FOI) request (available at www.Durham.ca or by contacting the Regional Clerk/Access and Privacy Office).

DRT will comply with any warrant, summons, court order or other legal process that requires disclosure of surveillance images or information, subject to consultation with the Regional Solicitor and Access and Privacy Office.

7.5 Surveillance Records – Law Enforcement, Security, Safety and Evidentiary Purposes

Release of Surveillance Records must support the purposes of this Policy and requires the approval of the General Manager or designate. The General Manager or designate will consult, as required, with the Region's Access and Privacy Office, Legal Services or Director Human Resources, prior to releasing Surveillance Records.

Requests, including law enforcement agencies or regulatory agencies, will be in writing and must identify the legal authority under which the agency is requesting disclosure unless the agency requests immediate access for reasons including imminent danger, hot pursuit or serious threat to public and/or worker health and safety. In this case, provided the images and information are logged for tracking purposes, the information may be disclosed by the General Manager or designate without a written request.

For each Surveillance Record DRT will record the following information:

a) The date and time of the original, recorded incident including the designated name/number of the applicable hardware, vehicle, property, requester, type of incident and associated tracking numbers.
b) The name of the Administrator creating the record.
c) The time and date the record was sealed.
d) The time and date the sealed record was provided to the requester.
e) The name and signature of an authorized person representing the requester.

DRT will maintain a copy of all Surveillance Records, in accordance with the requirements of this Policy.

7.6 Custody, Control, Retention and Disposal of Video Records/Recordings

DRT retains custody and control of all original Surveillance Recordings. Surveillance Records are subject to the access and privacy requirements of the MFIPPA, which includes but is not limited to the prohibition of DRT employees and contractors from access, or use of information from the Surveillance System, its components, files, or database for personal reasons.

Except for records retained for labour relations, criminal, safety, or security investigations or for evidentiary purposes, Surveillance Recordings will not be available to be used after 72 hours.

Surveillance Recordings **(source/unprocessed footage)** used for operational purposes will be ~~DRT copies of Surveillance Records produced from the Surveillance System will be retained for a~~ **archived by DRT for a period of two (2) years from the date the Surveillance Recording was downloaded**. ~~DRT will retain a copy of all Surveillance Records. DRT copies of Surveillance Records produced from the Surveillance System will be retained for a period of two years from the year the Surveillance Recording was~~

~~produced.~~ **Surveillance Records for potential risk management purposes will be archived by DRT for a period of seven (7) years.**

DRT will take all reasonable efforts to ensure the security of records in its control / custody and ensure their safe and secure disposal. Old storage devices will be disposed in accordance with Regional policy 14.21, System Acquisition, Maintenance, and Disposal, and applicable technology asset disposal processes ensuring personal information is erased prior to disposal and cannot be retrieved or reconstructed. Disposal methods may include, but are not limited to: shredding, burning, melting, overwriting, de-magnetizing, or erasing depending on the type of storage device.

7.7 Unauthorized Access and/or Disclosure (Privacy Breach)

A DRT Employee or contractor who becomes aware of any unauthorized disclosure of a Surveillance Record in contravention of this Policy and/or a potential privacy breach will immediately notify the General Manager through their respective Manager or Deputy General Manager.

Upon confirmation of the existence of a privacy breach, the General Manager will notify the Access and Privacy Office for implementation of the appropriate processes within the Corporate Privacy Breach Management policy.

The Deputy General Manager will inform the General Manager of events that have led up to the privacy breach. The employee or contractor will work with the Deputy General Manager or designate to take all reasonable actions to recover the record and limit the record's disclosure.

DRT will notify, where possible, affected parties whose Personal Information was inappropriately disclosed. The General Manager, in consultation with the Deputy General Manager or designate will investigate the cause of the disclosure with the goal of eliminating potential future occurrences.

A breach of this Policy by an employee of DRT may result in discipline, up to and including dismissal. A breach of this Policy by a third party with responsibilities under this Policy will result in the appropriate and applicable accountability measures.

7.8 Public Inquires about the Policy

An employee receiving an inquiry from the public regarding this Policy will direct the person to www.durhamregiontransit.com for information and to provide feedback.

An employee receiving an inquiry from the public regarding any privacy breaches and/or complaints will direct the individual to the Access and Privacy Office.

7.9 Review of Surveillance System in DRT Vehicles Policy

This Policy will be reviewed every two years by the General Manager who will forward recommendations for update, if any, to the Transit Executive Committee for approval.

8. Reference Sources

a) Municipal Freedom of Information and Protection of Privacy Act;
b) Ontario Information Privacy Commissioner Privacy Investigative Report MC07-68, Privacy and Video Surveillance in Mass Transit Systems, March 3, 2008.
c) Guidelines for the Use of Video Surveillance, October 2015, Information and Privacy Commission of Ontario
d) Region of Durham Policy 14.21, System Acquisition, Maintenance, and Disposal
e) Corporate Privacy Breach Management Policy

SCHEDULE "A" - DESIGNATED PERSONNEL

For this policy, the personnel designated as authorized agents shall be as follows and includes any successor positions and other Regional employees or agents authorized under privacy legislation.

Approve the release of ~~information~~ records for law enforcement or legal proceedings

- General Manager, DRT or designate
- Regional Solicitor

Approved to view ~~information~~ records

- General Manager, DRT or designate
- Director, Human Resources or designate
- Regional Solicitor **or designate**
- Access and Privacy Office designate
- Manager of Contracted Service Provider or designate
- **Manager of Maintenance, DRT or designate**
- Lead Manager of Safety and Training, DRT
- ~~Chairperson, Local 222 or designate, during the course of a grievance procedure for a disciplinary suspension or termination of employment wherein the Surveillance Recording in question is relevant to the grievance in question and is being viewed for the purpose of facilitating a settlement short of labour arbitration. It is understood that DRT will not provide the Chairperson with a copy of the Surveillance Recording and that DRT shall undertake appropriate editing to the Surveillance Recording to ensure the identity of any third-parties is protected prior to the Chairperson's viewing.~~
- **Chairperson, Unifor Local 222 or designate, during the course of an investigation wherein management has determined that if the alleged conduct under investigation is validated a member of Unifor Local 222 would be disciplined, and may be given an opportunity to view the Surveillance Recording at Step 1 of the grievance process.**

Approved to retrieve and view ~~information~~ records

- Deputy General Manager, Operations, DRT **and designate**
- Deputy General Manager, Maintenance, DRT **and designate**
- Deputy General Manager, Business Services, DRT **and designate**
- ~~Manager, Transit Policy and Planning, DRT~~
- Manager**s**, Operations, DRT
- Supervisor**s**, Operations, DRT
- ~~Administrative Assistant to the General Manager, DRT or designate~~

- ~~Program Manager, Technical Solutions, ***DRT*** or designate~~

Approved to create surveillance records

- Administrative Assistant to the General Manager, DRT or designate

Policy Manual

Title: Surveillance System in DRT Vehicles	
Issued: September 5, 2012	**Page #: 1 of 13**
Revised: September 4, 2024	
Approved by: General Manager	

1. Policy Statement

1.1 It is the policy of Durham Region Transit (DRT) to utilize a Surveillance System on transit vehicles to

- Ensure the safety and security of passengers, pedestrians, and DRT employees and assets;
- Investigate personal injury and other legal claims and proceedings; and
- Investigate and resolve Operational Matters.

1.2 DRT recognizes the need to balance an individual's right to privacy and the need to ensure the safety and security of the public transit network and the community. Although a transit bus is a public space, this policy is consistent with the principle of data minimization, which entails limiting the amount of personal information collected and retained to that which is necessary to fulfill the purposes of the lawfully authorized activity. DRT is committed to providing a safe and secure transit system for employees, passengers and pedestrians, and activities and systems that contribute to safety and crime prevention in the community.

1.3 While surveillance systems are installed on vehicles for criminal, safety, security, investigatory, and evidentiary reasons, DRT's Surveillance System is designed to minimize privacy intrusion. Proper surveillance, where deemed necessary, is one of the most effective means of helping to keep the DRT transit system operating in a safe, secure, and privacy protective manner.

1.4 This Policy has been developed to govern the Surveillance System for DRT vehicles, as more particularly set out in Section 2.1, and in accordance with the privacy provisions of the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and the Privacy and Video Surveillance in Mass Transit Systems report (2008) from the Ontario Information and Privacy Commissioner.

2. Definitions

FOI	Freedom of Information
MFIPPA	Municipal Freedom of Information and Protection to Privacy Act
Monitor	Active observation of Surveillance Recordings in real time, or systematic observation of Surveillance Recordings without a reasonable cause
Operational Matter	Incident, event or occurrence in relation to a DRT vehicle or employee
Personal Information	As defined by MFIPPA
Remote Access	Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet)
Surveillance Recordings	Information, including audio and video, recorded by the Surveillance System and stored on a Digital Video Recorder (DVR) or other storage device.
Surveillance Records	Copies of Surveillance Recordings, created for the purpose of: a) complying with any warrant, summons, court order or other legal process that requires disclosure of Surveillance Recordings; b) complying with Freedom of Information requests and MFIPPA; c) supporting investigations of personal injury and other legal claims and proceedings; and d) supporting investigations into Operational Matters.
Surveillance System	The physical or other mechanical or digital components of the Surveillance System installed on the vehicle or in a building, that enable continuous video and audio recording, observing or monitoring of the inside and outside of the vehicle, and for viewing Surveillance Recordings and producing Surveillance Records

2.1 Surveillance System

A. DRT's Surveillance System may include the use of video and audio recording equipment/device.

B. DRT may use its Surveillance System on transit vehicles, including ~~conventional and specialized vehicles~~ **DRT buses** ~~and specialized transit vehicles~~**, contracted service provider vehicles used to deliver DRT services,** and DRT non-revenue vehicles.

C. Surveillance System equipment/devices at facilities will be installed within secure locations

2.2 Application

A. This Policy is implemented by DRT staff. DRT contractors and service providers, and any third party who have responsibilities related to the Surveillance System will be made aware of this Policy, given instruction in meeting the Policy's requirements, and be required to agree in writing to comply with the requirements of this Policy.

B. Surveillance Recordings will be used only for the purposes of detecting, deterring and investigating unlawful and safety/security activities, investigating personal injury and other legal claims and proceedings, and investigating and resolving Operational Matters.

C. DRT staff will not monitor the Surveillance System.

D. Surveillance Recordings will not be used to monitor the performance of employees. Behaviors observed when reviewing Surveillance Recordings while investigating an Operational Matter will be managed according to established labour relations practices, which may include, without limitation, the use and reliance of Surveillance Recordings for employee development and/or discipline.

2.3 Exceptions

This policy does not apply to the following:

a) Covert surveillance used for law enforcement purposes. In those circumstances, either a statutory authority exists and/or the authority for the surveillance is lawfully obtained through a search warrant. Covert surveillance is surveillance conducted using hidden devices. If covert surveillance is not implemented pursuant to the conditions in the preceding paragraph, extra diligence in considering the use of the technology is required.
b) Surveillance System components installed at Regional buildings including transit facilities, which are managed by Facilities Management

3. Roles and Responsibilities

3.1 General Manager, DRT:

The General Manager may delegate responsibilities under this Policy.

a) Review the Policy every two years and forward to the Transit Executive Committee recommendations that will significantly alter the Policy.
b) Receive and review status updates and audit results, and implement the recommendations accordingly.

c) Designate appropriate staff to view Surveillance Recordings and produce Surveillance Records.
d) Review requests for Surveillance Records and where such requests comply with MFIPPA and this Policy, authorize the Administrator to produce a copy of the appropriate Surveillance Recording(s).
e) Immediately contact the Corporate Privacy Office and work with privacy staff to investigate any alleged privacy breach of this Policy.

3.2 Deputy General Manager, Business Services

The Deputy General Manager may delegate responsibilities under this Policy.

a) Ensure assigned staff comply with this Policy as it relates to privacy, storage, dissemination, and documentation for disclosure of information.
b) Manage the administrator requirements of the Surveillance System platform.
c) In consultation with the appropriate staff, develop training for DRT and contract staff regarding obligations and compliance with the MFIPPA and this Policy.
d) In consultation with the appropriate staff, coordinate technical requirements and activities related to design, functionality, installation, maintenance, and upgrades to the Surveillance System.
e) Establish an appropriate employee on- and off-boarding process to ensure activation and deactivation of access to the Surveillance System.
f) Ensure completion of a semi-annual review of user access to ensure only authorized users have access to view Surveillance Recordings.
g) Immediately report all alleged privacy breaches of this Policy to the General Manager and in their absence, the Corporate Privacy Office.

3.3 Deputy General Manager, Operations

The Deputy General Manager may delegate responsibilities under this Policy.

a) Ensure assigned staff comply with this Policy as it relates to privacy, storage, dissemination and documentation for disclosure of information.
b) Approve the locations on vehicles for installation of the Surveillance System in accordance with this Policy.
c) Consult with the Regional Clerk/Director of Legislative Services and /or Legal Services, for any issues related to MFIPPA requests.
d) Support the Deputy General Manager, Business Services, to develop training for DRT and contract staff regarding obligations and compliance with the MFIPPA and this Policy.
e) Immediately report all alleged privacy breaches of this Policy to the General Manager and in their absence, the Corporate Privacy Office.

3.4 Deputy General Manager, Maintenance

The Deputy General Manager may delegate responsibilities under this Policy.

a) Ensure assigned staff comply with this Policy as it relates to privacy, storage, dissemination, and documentation for disclosure of information.
b) Ensure that Surveillance System equipment on DRT vehicles is maintained in a state of good repair.
c) Delegate day-to-day maintenance of the Surveillance System on DRT Vehicles to designated staff, as appropriate.
d) Support the Deputy General Manager, Business Services, to develop training for DRT and contract staff regarding obligations and compliance with the MFIPPA and this Policy.
e) Immediately report all alleged privacy breaches of this Policy to the General Manager and in their absence, the Corporate Privacy Office.
f) Manage daily operational requirements for the Surveillance System.
g) Ensure assigned staff comply with this Policy.
h) Ensure records of activities related to accessing Surveillance Recordings are maintained as outlined in this Policy.
i) In consultation with the Deputy General Manager, Business Services, ensure relevant staff are trained in compliance with the MFIPPA and this Policy.

3.5 Supervisors, Operations

a) Report any Surveillance System defects to maintenance staff.
b) Document required information when accessing Surveillance Recordings.
c) Ensure no personal information obtained from Surveillance Recordings are disclosed to anyone without the approval of the applicable Manager.
d) Forward requests for a Surveillance Record to the Deputy General Manager, Operations.

3.6 Administrator

a) When approved by General Manager or designate, create required Surveillance Records.
b) Monitor and track requests and copies of Surveillance Records according to MFIPPA, this Policy, and corporate records management requirements.
c) Oversee all documentation required and generated to implement this Policy.

3.7 Director, Human Resources

a) Provide guidance on use of Surveillance Recordings in investigations where employee information has been captured.

3.8 Access and Privacy Office

a) Administer requirements of MFIPPA.
b) Coordinate with DRT to ensure compliance to MFIPPA and statutory obligations.

c) Respond to any inadvertent disclosures of personal information or any privacy complaints made to the Region or DRT, or Information and Privacy Commissioner (IPC)/Ontario and comply with Orders issued.
d) In consultation with the Deputy General Manager, Business Services, ensure relevant staff are trained in compliance with the MFIPPA and this Policy.

3.9 Corporate Services – Information Technology (CS-IT)

a) Service and support of the computer and Windows operating system used for the Surveillance System.
b) Service and support of the DRT network such as to facilitate remote access, except where the network is a component of the Surveillance System

3.10 Authorized Users, Contracted Service Providers

a) Ensure all relevant staff comply to the requirements of this policy.
b) View Surveillance Recordings in person at a DRT facility in the presence of a Transit Manager, Operations or designate, when appropriate to investigate relevant Operational Matters.
c) Ensure any Surveillance System defects are reported to the appropriate designated DRT staff.
d) Ensure no personal information obtained from Surveillance Recordings are disclosed to anyone without the approval of the applicable DRT Manager.
e) Forward requests for a Surveillance Record to the Administrator.
f) Prohibited to disclose, access or use information recorded by the Surveillance System, its components, files, or database for personal reasons, nor disclose, dispose, destroy, erase or alter any record without proper authorization from the Deputy General Manager, Operations, and without following the terms and conditions contained in this Policy.

3.11 Employees of DRT and Contracted Service Providers

a) Prohibited to disclose, access or use information recorded by the Surveillance System, its components, files, or database for personal reasons, nor disclose, dispose, destroy, erase or alter any record without proper authorization from the Deputy General Manager, Operations, and without following the terms and conditions contained in this Policy.

3.12 DRPS

a) DRPS shall comply with the Memorandum of Understanding that provides DRPS access to Surveillance Recordings from DRT vehicles.
b) DRPS employees will submit requests to view Surveillance Recordings to the DRPS video analysis group.

c) DRPS video analysis group will access the Surveillance System to view the appropriate Surveillance Recordings for investigative purposes.
d) Video analysis group will forward requests for a Surveillance Record to the Administrator, to be used strictly for investigative purposes.
e) Provide secure DRPS evidence link to the Administrator to upload Surveillance Recording.

4. Guidelines: Implementation of a Surveillance System

4.1 Designing Installing and Using Surveillance System Equipment

When designing a Surveillance System and installing related equipment, the following must be considered:

a) The ability to adjust cameras will be restricted to designated **business services and** maintenance staff, so that cameras cannot be manipulated to overlook spaces that are not intended to be monitored by the surveillance program.
b) Reception/recording equipment must be in a strictly controlled access area or system. Only staff designated by the appropriate Deputy General Manager will have access to the controlled access area/system and the reception/recording equipment.
c) Every reasonable attempt should be made to ensure Surveillance System equipment is not in a position that enables the public and/or unauthorized staff to view images.
d) Surveillance Recording components and related equipment will be installed at locations set out in Section 2.1 of this Policy, which may be amended from time to time.

4.2 Notice of Use of Video Recording System

a) DRT will post decals, visible to members of the public, at all entrances and/or prominently displayed on the perimeter of the vehicles with a Surveillance System installed.
b) The notification requirements of this decal must inform individuals of the legal authority for the collection of personal information; the principal purpose(s) for which the personal information is intended to be used; and the title, business address, and telephone number of someone who can answer questions about the collection.

4.3 Personnel Authorized to Operate and Maintain Surveillance System Equipment

Only authorized agents or personnel assigned by the General Manager or designate, as specific in Schedule A, will be permitted to operate the Surveillance System, to view Surveillance Recordings, create Surveillance Records and maintain the Surveillance System installed on DRT vehicles. All employees and representatives of third parties with responsibilities outlined in this Policy, will acknowledge in writing that they have received training with respect to their responsibilities and confidentiality obligations, and that they understand those obligations.

4.4 Breach of Policy

The General Manager, Municipal Freedom of Information and Protection of Privacy Coordinator, Director Human Resources, and Legal Services, as needed, will investigate and respond to any breach or alleged breach of this Policy.

5. Surveillance Equipment/Records

5.1 Types of Recording Devices

DRT may use a Digital Video Recorder system (DVR) and may implement technology replacements and/or upgrades, as required.

5.2 Record Identification

All Surveillance Records will be clearly identified (labelled) as to the date and location of origin including being labelled or titled with a unique, sequential number or other verifiable symbol. On a vehicle or in a facility with a DVR that stores recordings/information directly on a hard drive, the computer time and date stamp will be understood to be this identification.

Each user or facility, as applicable, will maintain records of activities related to recording devices and records according to the Region's Records Retention By-law. The activities include information regarding the use, maintenance, access and storage of recorded material.

5.3 Remote Access

DRT may use remote access to retrieve, view, operate, maintain or audit all or part of the Surveillance System. DRT further reserves the right to provide remote access to law enforcement agencies for law enforcement purposes. Any remote access provided to law enforcement agencies will contain a provision allowing DRT to conduct annual audits relating to the use and disclosure of information obtained through the Surveillance System and any such audits will be performed in accordance with this Policy.

Where the Surveillance System does not provide appropriate electronic recording of user activities, physical logbooks will be maintained to record all activities related to Surveillance System devices and records. The activities include all information regarding the use, maintenance and storage of records; and all instances of access to, and use of, recorded material. All entries will include name of authorized agent, date, time and activity. The logbook or electronic alternative must remain in a safe and secure location.

6. Auditing

6.1 DRT will undertake an internal audit every two years to ensure adherence to this Policy. Auditing may include verification that reported incidents were properly recorded; procedures on security; established roles and responsibilities; maintenance, storage, retention and disposal of equipment and recorded information have been followed; and requests for information have been tracked and responded to accordingly.

Any deficiencies, concerns and/or recommendations identified will be resolved.

6.2 General Manager or designate will conduct a bi-annual review of user access to ensure only authorized users have access to view Surveillance Recordings.

7. Access to Surveillance Recordings

7.1 Access

Access to Surveillance Recordings will be restricted to authorized agents specified in Appendix A, to comply with the roles and responsibilities as outlined in this Policy.

7.2 Storage

All storage devices that are not in use must be stored securely in a locked receptacle located in an access-controlled area.

7.3 Viewing Surveillance Recordings

Only authorized personnel or agents listed in Schedule A, are permitted to view and retrieve Surveillance Recordings. Surveillance Recordings will be viewed in a controlled area. Every reasonable attempt will be made to ensure that recordings are not viewable or can be heard by other individuals.

7.4 Access to Information Requests

All requests for Surveillance Records where disclosure may be inconsistent with the principle purposes of the collection will be directed to the Regional Clerk/Director of Legislative Services for processing. A person requesting access to a Surveillance Record is required to follow the requirements of the Region of Durham in making a Freedom of Information (FOI) request (available at www.Durham.ca or by contacting the Regional Clerk/Access and Privacy Office).

DRT will comply with any warrant, summons, court order or other legal process that requires disclosure of surveillance images or information, subject to consultation with the Regional Solicitor and Access and Privacy Office.

7.5 Surveillance Records – Law Enforcement, Security, Safety and Evidentiary Purposes

Release of Surveillance Records must support the purposes of this Policy and requires the approval of the General Manager or designate. The General Manager or designate will consult, as required, with the Region's Access and Privacy Office, Legal Services or Director Human Resources, prior to releasing Surveillance Records.

Requests, including law enforcement agencies or regulatory agencies, will be in writing and must identify the legal authority under which the agency is requesting disclosure unless the agency requests immediate access for reasons including imminent danger, hot pursuit or serious threat to public and/or worker health and safety. In this case, provided the images and information are logged for tracking purposes, the information may be disclosed by the General Manager or designate without a written request.

For each Surveillance Record DRT will record the following information:

a) The date and time of the original, recorded incident including the designated name/number of the applicable hardware, vehicle, property, requester, type of incident and associated tracking numbers.
b) The name of the Administrator creating the record.
c) The time and date the record was sealed.
d) The time and date the sealed record was provided to the requester.
e) The name and signature of an authorized person representing the requester.

DRT will maintain a copy of all Surveillance Records, in accordance with the requirements of this Policy.

7.6 Custody, Control, Retention and Disposal of Video Records/Recordings

DRT retains custody and control of all original Surveillance Recordings. Surveillance Records are subject to the access and privacy requirements of the MFIPPA, which includes but is not limited to the prohibition of DRT employees and contractors from access, or use of information from the Surveillance System, its components, files, or database for personal reasons.

Except for records retained for labour relations, criminal, safety, or security investigations or for evidentiary purposes, Surveillance Recordings will not be available to be used after 72 hours.

Surveillance Recordings (source/unprocessed footage) used for operational purposes will be archived by DRT for a period of two (2) years from the date the Surveillance Recording was downloaded. Surveillance Records for potential risk management purposes will be archived by DRT for a period of seven (7) years.

DRT will take all reasonable efforts to ensure the security of records in its control / custody and ensure their safe and secure disposal. Old storage devices will be disposed in accordance with Regional policy 14.21, System Acquisition, Maintenance, and Disposal,

and applicable technology asset disposal processes ensuring personal information is erased prior to disposal and cannot be retrieved or reconstructed. Disposal methods may include, but are not limited to: shredding, burning, melting, overwriting, de-magnetizing, or erasing depending on the type of storage device.

7.7 Unauthorized Access and/or Disclosure (Privacy Breach)

A DRT Employee or contractor who becomes aware of any unauthorized disclosure of a Surveillance Record in contravention of this Policy and/or a potential privacy breach will immediately notify the General Manager through their respective Manager or Deputy General Manager.

Upon confirmation of the existence of a privacy breach, the General Manager will notify the Access and Privacy Office for implementation of the appropriate processes within the Corporate Privacy Breach Management policy.

The Deputy General Manager will inform the General Manager of events that have led up to the privacy breach. The employee or contractor will work with the Deputy General Manager or designate to take all reasonable actions to recover the record and limit the record's disclosure.

DRT will notify, where possible, affected parties whose Personal Information was inappropriately disclosed. The General Manager, in consultation with the Deputy General Manager or designate will investigate the cause of the disclosure with the goal of eliminating potential future occurrences.

A breach of this Policy by an employee of DRT may result in discipline, up to and including dismissal. A breach of this Policy by a third party with responsibilities under this Policy will result in the appropriate and applicable accountability measures.

7.8 Public Inquires about the Policy

An employee receiving an inquiry from the public regarding this Policy will direct the person to www.durhamregiontransit.com for information and to provide feedback.

An employee receiving an inquiry from the public regarding any privacy breaches and/or complaints will direct the individual to the Access and Privacy Office.

7.9 Review of Surveillance System in DRT Vehicles Policy

This Policy will be reviewed every two years by the General Manager who will forward recommendations for update, if any, to the Transit Executive Committee for approval.

8. Reference Sources

a) Municipal Freedom of Information and Protection of Privacy Act;

b) Ontario Information Privacy Commissioner Privacy Investigative Report MC07-68, Privacy and Video Surveillance in Mass Transit Systems, March 3, 2008.
c) Guidelines for the Use of Video Surveillance, October 2015, Information and Privacy Commission of Ontario
d) Region of Durham Policy 14.21, System Acquisition, Maintenance, and Disposal
e) Corporate Privacy Breach Management Policy

SCHEDULE “A” - DESIGNATED PERSONNEL

For this policy, the personnel designated as authorized agents shall be as follows and includes any successor positions and other Regional employees or agents authorized under privacy legislation.

Approve the release of records for law enforcement or legal proceedings

- General Manager, DRT or designate
- Regional Solicitor

Approved to view records

- General Manager, DRT or designate
- Director, Human Resources or designate
- Regional Solicitor or designate
- Access and Privacy Office designate
- Manager of Contracted Service Provider or designate
- Manager of Maintenance, DRT or designate
- Lead Manager of Safety and Training, DRT
- Chairperson, Unifor Local 222 or designate, during the course of an investigation wherein management has determined that if the alleged conduct under investigation is validated a member of Unifor Local 222 would be disciplined, and may be given an opportunity to view the Surveillance Recording at Step 1 of the grievance process.

Approved to retrieve and view records

- Deputy General Manager, Operations, DRT and designate
- Deputy General Manager, Maintenance, DRT and designate
- Deputy General Manager, Business Services, DRT and designate
- Managers, Operations, DRT
- Supervisors, Operations, DRT

Approved to create surveillance records

- Administrative Assistant to the General Manager, DRT or designate