

Section	Integrated Video and Evidence Program	Current Approval Date
Subject	Audio and Video Recording Policy	

PURPOSE

Metrolinx is dedicated to safeguarding its employees, customers, and the communities it serves. Audio and Video Recording (AVR) Systems play a critical role in this commitment by enhancing incident response, monitoring essential infrastructure, protecting public safety, and deterring unlawful activity. All use of AVR Systems shall comply with applicable Metrolinx Policies and Standards.

This policy outlines the framework for the responsible deployment and use of Audio and Video Recording Systems, such as Closed-Circuit Television (CCTV), Body-Worn Cameras (BWCs), In-Vehicle Dash Cameras, Drones, and audio and video recording devices on buses and coaches, excluding in-cab locomotive voice and video recorders (LVVR). It maintains such use is carried out in accordance with Provincial privacy legislation and balances operational requirements with individuals' reasonable expectations of privacy.

POLICY STATEMENT

Metrolinx uses Audio and Video Recording Systems to monitor and protect people, property, and infrastructure. These systems are deployed using an evidence-based approach and only where justified by clear operational needs, safety considerations, or security risks. Their use must align with privacy requirements as set out in the *Freedom of Information and Protection of Privacy Act* (FIPPA), and Metrolinx's Enterprise Privacy Policy (CA-0901-01).

Audio and Video Recording Systems support:

- Deterrence and investigation of criminal activity
- Monitoring of safety and security incidents
- Evidence for insurance claims and legal proceedings
- Enhanced situational awareness for customer service and enforcement personnel
- Operational awareness and decision-making.

The deployment of these systems will be limited to areas where there is a reduced reasonable expectation of privacy and must never infringe on spaces with a heightened reasonable expectation of privacy, such as washrooms or changerooms. In exigent circumstances with approval, Metrolinx may utilize BWCs in areas such as a washroom (i.e. attending an assault or an overdose call for service).

SCOPE & APPLICATION

This policy applies to all Audio and Video Recording Systems under Metrolinx's control, subject to contractual agreements, including but not limited to In-Vehicle Dash Cameras, Body-Worn Cameras, Closed-Circuit Television Cameras (CCTV), Drone Cameras and/or audio and video recording devices used for operational and safety purposes, excluding in-cab locomotive voice and video recorders (LVVR). This policy is applicable to all Metrolinx

employees including probationary, full-time, part-time as well as both casual and contract employees and any contractor performing work on behalf of Metrolinx.

GUIDING PRINCIPLES FOR USE

Metrolinx property, including critical infrastructure, may be monitored using Audio and Video Recording Systems for the safety, security and protection of Metrolinx staff, visitors, and customers as well as for the prevention, detection, and prosecution of criminal activity and/or security threats and for operational reasons.

Audio and Video Recording Systems may be used by Metrolinx to support various organizational needs including but not limited to the basis of operational requirements, safety and security concerns, insurance claims, assisting in active investigations, prosecution and litigation of an offence, enhanced situational awareness for customer service and enforcement personnel, or as a result of specific reports of incidents of crime. Metrolinx may use Audio and Video Recording Systems 24 hours a day, 7-days a week due to the nature of Metrolinx operations.

Audio and Video Recording Systems shall only be implemented where:

- A defined operational or security risk exists.
- Other less intrusive alternatives have been considered and found inadequate/insufficient.
- A Privacy Impact Assessment (PIA) has been conducted to identify and mitigate risks.
- Installation and operation follow design principles that reduce privacy intrusion while achieving security objectives.

Recording shall never occur in high-privacy areas (e.g., washrooms, changerooms) except under exigent circumstances with Manager approval.

Every reasonable attempt must be made to maintain that Audio and Video Recording Systems and equipment are not stored in an area that would allow for unauthorized viewing of data and/or materials.

NOTICE OF USE OF AUDIO AND VIDEO RECORDING SYSTEMS

In order to provide notice to individuals that audio/video is in use on Metrolinx property, Metrolinx will provide clear and visible notification of active surveillance. Sample signage as shown in *Appendix A* may be posted at the following locations:

- At entrances to GO and UP Express facilities
- Onboard buses and coaches
- In Metrolinx vehicles equipped with In-Vehicle Dash Cameras
- Around rail and bus platforms, parking lots, and station waiting areas
- On all Metrolinx Body-Worn Cameras

Signage utilized by Metrolinx shall convey the following information to Metrolinx customers: AVR systems may capture audio and visual information during interactions in the course of operations. Your personal information, which may include images, video, and/or audio, is collected under the authority of the *Metrolinx Act* and the Metrolinx Audio & Video Policy for the purpose of maintaining passenger safety and security. Your personal information is managed in accordance with the Freedom of Information and Protection of Privacy Act (FIPPA). If you have questions, please contact Metrolinx Enterprise Security at EnterpriseSecurity@metrolinx.com.

Metrolinx Authorized Officers equipped with Body-Worn Cameras will also be required to verbally communicate the use of a Body-Worn Camera wherever practicable.

ROLES AND RESPONSIBILITIES

This section lists all the accountabilities, responsibilities and duties that are required to implement this policy.

Freedom of Information (FOI) Office:

- Manage and process requests received under the *Freedom of Information and Protection of Privacy Act* (FIPPA) for access to audio/video recordings.
- Coordinate with relevant program areas for record retrieval and redaction.
- Liaise with the Information and Privacy Commissioner (IPC) on appeals, as required.

Privacy Office:

- Provide privacy guidance on FIPPA obligations as they relate to audio and video recordings.
- Provide privacy advisory and operational support, as needed.
- Respond to privacy complaints and assist in IPC investigations.
- Conduct Privacy Impact Assessments (PIAs) for new technologies and initiatives.
- Support any layouts, modifications, relocations, or removals of CCTV cameras.

Customer Protective Services (CPS) – Enterprise Security/Security Operations Centre:

- Assist in conducting PIAs, as required for new systems.
- Manage law enforcement requests for audio and video recordings.
- Manage internal Metrolinx requests for audio and video recordings to be viewed and/or retained as per Metrolinx policies.
- Manage and maintain user groups and access controls for Metrolinx internal video management system.
- Support both internal and external investigations and audits regarding Audio and Video Recording Systems.
- Approve any layouts, modifications, relocations, or removals of CCTV cameras.

Records and Information Management (RIM) Office:

- Conduct recordkeeping impact assessments, as required.
- Align record retention schedule with internal Metrolinx and applicable Ontario Public Service (OPS) directives and legislative recordkeeping requirements.
- Provide guidance pertaining to supporting appropriate storage and disposition of records.

Innovation & Information Technology (I&IT) Division:

- Review new system designs for alignment with internal Metrolinx security, applicable Ontario Public Service (OPS) directives and legislative requirements.
- Provide technical maintenance, support and training for Audio and Video Recording Systems, where appropriate as required.
- Implement adequate cybersecurity controls to protect Audio and Video Recording Systems, as required.
- Work collaboratively with the Metrolinx Privacy Office and Metrolinx Cybersecurity Team to support privacy and cyber breach responses.

Customer and Transit Operations Business Unit:

- Maintain that Audio and Video Recording Systems on Metrolinx assets such as buses, and coaches are maintained and kept in a state of good repair.
- Maintain that training is provided to all staff members on access and handling procedure related to Audio and Video Recording Systems.
- Immediately report breaches of IT security and/or privacy to the Customer Protective Service Enterprise Security Team, Metrolinx Cybersecurity team, and the Metrolinx Privacy Office.

Contractors:

- All contractors who have access to Metrolinx Audio and Video Recording Systems must adhere to this policy and must not disclose, modify/edit, access or use information contained in any Metrolinx Audio or Video Recording System, its components, files, or database for personal reasons nor disclose, dispose, destroy, erase or alter any record without proper authorization and without following the terms and conditions contained in this policy and procedures.
- Immediately report security or privacy breaches to their supervisor and to their Metrolinx main point of contact who shall then notify the Metrolinx Privacy Office and/or Cybersecurity team.

Metrolinx Employees

- All Metrolinx employees who have access to Audio and Video Recording Systems must adhere to this policy and must not disclose, modify/edit, access or use information contained in any Metrolinx Audio or Video Recording System, its components, files, or database for personal reasons nor disclose, dispose, destroy, erase or alter any record without proper authorization and without following the terms and conditions contained in this policy and procedures.

- Immediately report any security/privacy breach to their supervisor and the Metrolinx Privacy Office and/or Cybersecurity team.

RECORDS MANAGEMENT

Metrolinx utilizes recording devices as part of its Audio and Video Recording Systems. In general, recordings are retained for up to five (5) days as per Provincial mandates. However, certain types of footage may be retained for longer periods due to operational, safety, security, or legal requirements. Recordings that are needed for investigations or legal proceedings may also be preserved beyond this timeframe, in accordance with the Metrolinx Record Retention Schedule.

Any business or operational images and/or recordings captured on a secondary Metrolinx device such as a mobile phone or video capture software on a computer, laptop, or mobile device are only permitted under exigent circumstances, including during a fatality or a critical incident that may pose significant reputational, safety, financial, or operational risk to Metrolinx, or when explicitly authorized by a Metrolinx Director or above.

The recordings or images captured can only be shared with authorization by a Network Operations Director, an Incident Control Manager (ICM), a Regional Control Manager (RCM), a Customer Protective Services Director, the Vice President for Customer Protective Services, or the Vice President for Network Operations. Sharing shall be done through the secure Digital Evidence Management System (DEMS) employed by Metrolinx both internally with persons actively managing the incident and/or the accountable executive of the business unit involved. Externally, it may be shared as per Metrolinx processes with, but not limited to Law Enforcement Agencies, other transit agencies, the Office of the Coroner, the Ministry of Transportation, or other regulatory bodies.

Metrolinx will take all reasonable efforts to maintain that all audio and video recordings will remain safeguarded and controlled at all times, including by applying access controls and encryption.

Metrolinx will take all reasonable efforts to maintain the security of the records in its control and the safe and secure disposal of these records. Storage devices must be disposed of in accordance with applicable technology asset disposal processes and procedures maintaining that personal information is erased prior to disposal and cannot be retrieved or reconstructed. Cloud based storage systems which are utilized shall require that the data be permanently and irretrievably deleted to maintain proper destruction.

ACCESS TO VIDEO RECORDS

Access to video recording records shall be restricted to authorized personnel to carry out their assigned roles and responsibilities.

Requests for records from other transit agencies, the Office of the Coroner, the Ministry of Transportation, or other regulatory bodies shall be handled by Customer Protective Services Enterprise Security. Only authorized personnel will be able to view and share records.

In the event that a Metrolinx site/facility is shared with a partner agency, Metrolinx shall include contractual terms in the applicable legal agreements which define the ownership, access, and responsibilities in accordance with FIPPA where applicable.

ACCESS TO VIDEO RECORDS (PUBLIC REQUESTS)

Any individual can request in writing, access to an audio/video recording via the Metrolinx FOI Office, pursuant to FIPPA. Once received, all FOI requests will be reviewed and assessed individually by the FOI Office in accordance with FIPPA. In order to make a request, the individual must:

1. Provide sufficient detail (approximate date, time, and location, if known, of the incident) to enable an authorized employee, upon reasonable effort, to identify the record; and
2. At the time of making the request, pay the prescribed fees as provided under the *Freedom of Information and Protection of Privacy Act* (FIPPA).

Metrolinx employees receiving inquiries from the public regarding Metrolinx Audio and Video Recording Systems shall direct inquiries to Metrolinx Enterprise Security.

They can be contacted by email at EnterpriseSecurity@metrolinx.com or by mail addressed to Metrolinx Enterprise Security at 277 Front Street West Toronto, Ontario, M5V 2X4.

ACCESS TO VIDEO RECORDS (INTERNAL REQUESTS)

Any internal access to audio and video recordings shall be restricted to authorized staff performing their assigned roles (e.g. to support legal and/or insurance claims) and shall follow the processes outlined in the Information Sharing Standard.

ACCESS TO VIDEO RECORDS (LAW ENFORCEMENT)

Requests for records from law enforcement agencies to aid in an investigation shall be handled by CPS Enterprise Security in accordance with the requirements outlined in the Information Sharing Standard and supporting Procedure Guide. Only authorized personnel will be able to view and share video recordings. Video recordings shared with law enforcement agencies shall be shared in accordance with FIPPA.

Metrolinx may also permit and facilitate the viewing of footage by law enforcement agencies, while Metrolinx retains custody of the footage.

REVIEW AND MONITORING

The Metrolinx Audio and Video Recording Policy will be reviewed every two (2) years to maintain compliance with legislative requirements and alignment with Metrolinx objectives.

ESCALATIONS AND EXCEPTIONS

Metrolinx employees who become aware of any unauthorized access, use, disclosure, or tampering of an audio or video record in contravention of this Policy, or who suspect a potential IT security or privacy breach, shall immediately notify the Metrolinx Privacy Office through their respective Director, or designate.

The Metrolinx Privacy Office shall report confirmed privacy breaches to the Information and Privacy Commissioner of Ontario (IPC) in accordance with applicable legislation, IPC guidelines, and the Enterprise Privacy Policy. The Metrolinx Privacy Office shall also notify affected individuals when required under applicable legislation and regulations. Failure to comply with this Policy may result in disciplinary action for Metrolinx employees, up to and including termination of employment. Contractors found to be in breach of this Policy may be subject to contract review, suspension, or termination, and may be deemed ineligible for future engagements with Metrolinx.

REFERENCES

Archives and Recordkeeping Act, 2006, S.O. 2006, C. 34, Schedule A

CCTV Code of Practice, Revised Edition 2008, Information Commissioner's Office Closed Circuit Television Reference Manual for Security Applications, 2008, Transport Canada

Freedom of Information and Protection of Privacy Act, R.R.O. 1990, Regulation 459 as Amended.

Freedom of Information and Protection of Privacy Act, R.R.O. 1990, Regulation 460

Guidelines for Using Video Surveillance Cameras in Public Places, Office of the Information and Privacy Commissioner of Ontario. 2007.

Metrolinx Enterprise Privacy Policy (CA-0901-01)

Metrolinx I & IT Hardware Asset Disposal Policy (CA-0502-09)

Metrolinx Personal Information Collection, Use and Disclosure Procedures (CA-0406-02)

Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report, Privacy Investigation Report MC07-68, March 2008, Information and Privacy Commissioner of Ontario

Railway Safety Act 2018, C.10, S. 65

APPENDIX

Appendix A: Sample Corporate Audio and Video Recording Signage

ADMINISTRATION

Identification Name	Audio & Video Recording Policy
Approved By	Chief Operating Officer
Owner	Vice President, Customer Protective Services
Monitor	Director, Corporate Resilience, Customer Protective Services Director, Professional Standards, Customer Protective Services
Original Approval Date	
Review Frequency	2 years
Supersedes	CCTV and AV Policy CA-0405-10

POLICY HISTORY

Revision / Review Date	Author	Description
	Customer Protective Services	Policy revised to include Body-Worn Cameras, Drones, and In-Vehicle dash cameras, renamed and new policy number assigned. Replaces CA-0405-10 CCTV and AV Policy
April 2015	System Safety, Safety & Security	Initial Release as CCTV and AV Policy CA-0405-10
January 25, 2006	System Safety	Original Policy

LIST OF ACRONYMS

AVR	Audio and Video Recording
CCTV	Closed-Circuit Television
CPS	Customer Protective Services
FIPPA	<i>Freedom of Information and Protection of Privacy Act</i>
FOI	Freedom of Information
ICM	Incident Control Manager
IPC	Information and Privacy Commissioner of Ontario
LVVR	Locomotive Voice and Video Recorder
NOC	Network Operations Centre
RCM	Regional Control Manager

DEFINITIONS

Audio Recording: A recording of audible components, including any metadata for analytics.

Audio Recording System: Any electronic device and its components which are equipped to capture sound.

Authorized Officer: Is an individual who has been formally granted the authority to act on behalf of Metrolinx as a Customer Protection Officer, Revenue Protection Officer, or a Station Safety Ambassador.

Body-Worn Camera: Wearable device that can record videos, audio, and capture pictures of people or places.

Contractor: Individuals or a company which undertakes a contract to provide materials, labour, or a service.

Critical Infrastructure: Refers to processes, systems, facilities, technologies, networks, assets, and services essential to the health, safety, security, and/or economic well-being of Metrolinx the Agency.

Cybersecurity Breach: Any event or activity that compromises the confidentiality, integrity, or availability of vendor's and Metrolinx's data or systems, including unauthorized access, malicious activities, or system disruptions.

Employees: Any employee of Metrolinx, whether full or part-time, whether employed for an indefinite or a fixed or otherwise limited term and includes individuals either seconded to Metrolinx from another employer or on a leave of absence from another employer.

Enhanced Situational Awareness: The improved ability of Authorized Officers to perceive, understand, and assess an incident or environment in real-time.

Exigent Circumstances: Refers to urgent, emergency situations that require immediate action to protect public safety, prevent harm, or preserve evidence.

In-Vehicle Dash Camera: An onboard camera that records the view either through a vehicle's front and rear windows or both, and potentially the interior of the vehicle.

Locomotive Voice and Video Recorder: A system installed in a locomotive that continuously records audio, video, and operational data in the cab to support safety monitoring, incident investigation, and regulatory compliance in accordance with Transport Canada requirements.

Mobile Device: A piece of portable electronic equipment that can connect to the internet, such as a smartphone or tablet computer.

Privacy Breach: Occurs when personal information is collected, used (including accessed or modified), disclosed, retained, or disposed of in a manner not permitted by law, may be intentional or unintentional, and includes the loss of or failure to protect such information.

Property: A tangible or intangible possession without limitations includes vehicles and property which is owned by an individual or business.

Video Recording: A recording of visual components, including any metadata for analytics.

Video Recording System: Any electronic device and its components that are equipped with a camera capable of recording and storing analog or digital images. Sound may or may not be available.

APPENDIX A

Sample Corporate Audio and Video Recording Signage



Station Signage



Bus Signage



CCTV Signage



Body Worn Camera Sticker