Section	Integrated Video and Evidence Program	Current Approval Date
Subject	Digital Evidence Management System (DEMS) Standard	Month, Day, Year

PURPOSE

This Standard, along with the Audio and Video Recording Policy, the Digital Evidence Management System (DEMS) Procedure Guide, and the Information Sharing Standard, outlines the principles and requirements for the secure use of DEMS by all Metrolinx employees who are authorized to access the system.

Metrolinx shall utilize DEMS to establish the secure management of digital evidence. This enterprise platform enables the efficient collection, organization, analysis, and sharing of digital evidence including Body-Worn Camera footage, In-Vehicle Dash Camera recordings, CCTV footage, audio files, and Drone footage within a centralized, cloud-based environment. The system supports evidence integrity and supports collaboration throughout its lifecycle. Authorized Officers, including Customer Protection Officers (CPOs), Revenue Protection Officers (RPOs), and Station Safety Ambassadors (SSAs), are equipped with integrated hardware, software, and mobile tools to securely upload, tag, catalogue, and store digital evidence in accordance with Metrolinx-approved protocols. Why do we need this policy? A brief statement about the intended purpose of this policy, why it is being put in place, and how it is connected to Metrolinx's mission, vision, and values.

SCOPE & APPLICATION

This Standard applies to all Metrolinx employees who have access to the DEMS system, including full-time, part-time, probationary, and fixed-term employees who utilize DEMS to support CPS operations.

DEMS must be used to securely store, organize, and if applicable, share digital evidence as a result of a safety incident, investigative matter, or enforcement action in accordance with this Standard and the DEMS Procedure Guide.

DIGITAL EVIDENCE MANAGEMENT SYSTEM (DEMS) FUNCTIONALITY REQUIREMENTS

Functional requirements for DEMS must support the secure, efficient, and lawful collection, storage, management, and dissemination of digital evidence throughout the evidence collection process. The system must facilitate seamless ingestion of various digital evidence formats including audio, video, photographs, and documents from multiple sources such as Body-Worn Cameras, In-Vehicle Dash Cameras, Drones, CCTV, mobile devices, and third-party platforms. It should maintain chain of custody tracking with detailed audit logs to maintain the integrity and admissibility of evidence in court, complying with Ontario's legal and privacy regulations, including the Freedom of Information and Protection of Privacy Act (FIPPA) and applicable standards from the Ministry of the Solicitor General. Role-based access controls must be implemented to restrict data access based on user permissions, and the system must support secure sharing with prosecutors, defense counsel, and other authorized stakeholders.

Additionally, DEMS will integrate, where technically feasible, with existing law enforcement and justice systems, support advanced search and tagging capabilities, and provide evidence lifecycle management features, including retention schedules and secure disposition when appropriate.

DIGITAL EVIDENCE MANAGEMENT SYSTEM (DEMS) NON-FUNCTIONALITY REQUIREMENTS

Non-functional requirements for DEMS focus on supporting the system's reliability, security, scalability, and compliance with both federal and provincial standards. The system must exhibit high availability to support 24/7 access for CPS employees and judicial personnel. Security is paramount; thus, DEMS must incorporate strong encryption protocols for data protection, enforce strict access controls and, multi-factor authentication where technically feasible, and intrusion detection systems, aligning with relevant federal and provincial guidelines. The platform must be scalable to accommodate growing volumes of digital evidence without degradation in performance and must support concurrent access by multiple users.

Usability is also critical, as the DEMS interface should be intuitive and responsive, maintaining accessibility in accordance with the Accessibility for Ontarians with Disabilities Act (AODA). The system must support disaster recovery and data redundancy measures, including backups, recovery time objectives, and recovery point objectives that meet Metrolinx standards as outlined in the Metrolinx Information Security Policy. Additionally, DEMS should undergo regular performance, security, and compliance audits to maintain that it continues to meet evolving Metrolinx legal, technological, and operational requirements.

DIGITAL EVIDENCE MANAGEMENT SYSTEM (DEMS) SECURITY STANDARDS

Security standards for DEMS must align with provincial and federal guidelines to support the protection, confidentiality, and integrity of sensitive information. All data must be protected using advanced encryption protocols which are continuously monitored by the Metrolinx Innovation & Information Technology (I&IT) business unit. The system will implement robust identity and access management measures, including multi-factor authentication (MFA), role-based access controls, and strict user provisioning and de-provisioning processes. Audit logging shall be tamper-proof, comprehensive, and regularly reviewed to support accountability and support for investigations.

To protect against data breaches and unauthorized access, DEMS shall include built-in intrusion detection and prevention systems, which are further supported by regular vulnerability assessments, and penetration testing as set in the Metrolinx Information Security Policy. Furthermore, DEMS shall be compliant with the Freedom of Information and Protection of Privacy Act (FIPPA), and relevant portions of the Criminal Code of Canada and the Canadian Charter of Rights and Freedoms concerning lawful access, privacy, and disclosure of digital evidence, as well as Metrolinx internal policies such as the Metrolinx Information Security Policy and the Metrolinx Enterprise Data Governance and Management Policy.

DATA MANAGEMENT

Data management for DEMS must support the accurate, secure, and efficient handling of digital evidence throughout its entire lifecycle, from collection to final disposition. The system shall support the ingestion of diverse file types including video, audio, documents, and images while preserving metadata such as timestamps, device identifiers, and source information to maintain evidentiary value. All data will be classified, indexed, and stored in a manner that enables efficient retrieval and search capabilities, supporting filters such as case number, incident type, Authorized Officer name, and date range. DEMS must enforce strict chain of custody controls, automatically logging all user actions including uploads, views, edits, transfers, and dispositions, in tamper-proof audit trails.

Data retention must comply with the Metrolinx Record Retention Schedule. The system will also support version control, evidence tagging, and linkage of multiple pieces of evidence to a single case file. Interoperability with other justice and law enforcement systems, where technically feasible, is essential to facilitate seamless data flow. Additionally, DEMS must support robust backup and disaster recovery mechanisms, maintaining data resilience and availability in the event of system failures or security incidents as per requirements outlined in the contract with the DEMS provider.

PRIVACY CONSIDERATIONS

Privacy considerations for DEMS are paramount, given the sensitive and often personal nature of the digital evidence it handles. The system must comply with the Freedom of Information and Protection of Privacy Act (FIPPA), maintaining that the collection, use, disclosure, and retention of personal information are lawful, necessary, and proportionate. Privacy by Design principles, as endorsed by the Information and Privacy Commissioner of Ontario, must be embedded into the system architecture from the outset. This includes data minimization, default privacy settings, user access limitations, and end-to-end encryption.

Access to digital evidence shall be strictly role-based, with audit trails capturing all user interactions to support accountability and transparency. Features such as facial blurring and other redaction tools shall be utilized to protect the identities of individuals who are not directly involved in investigations or prosecutions. DEMS must also provide mechanisms to support individuals' rights to access their personal information or request corrections under FIPPA, while maintaining the integrity of evidence for legal proceedings. Regular privacy impact assessments (PIAs) shall be conducted to evaluate and mitigate privacy risks as the system evolves or expands in functionality.

REVIEW AND USE OF DIGITAL EVIDENCE MANAGEMENT SYSTEM (DEMS) MATERIALS

The review and use of material stored within DEMS must support the secure, efficient, and legally compliant handling of digital materials and comply with federal and provincial information sharing laws. Authorized users such as Authorized Officers, CPS investigators, CPS SOC Team, law enforcement agencies and Prosecutors must be able to securely access and review digital evidence within the system using a role-based access model that supports

that only relevant personnel can view or modify specific files. DEMS offers tools for detailed review, including video playback with frame-by-frame analysis, audio enhancement options, document annotation, and metadata inspection. Information within DEMS shall be easily searchable by key fields such as case number, date, file type, or involved parties, allowing for efficient retrieval during investigations or court preparation. Prosecutors must be able to compile disclosure packages directly within the system and securely share them with defense counsel, if required. DEMS shall also support evidence presentation in court, with export options that preserve the chain of custody and integrity of the digital files. Detailed audit logs will track every access, view, comment, or modification, supporting a transparent review history that can be verified, if challenged in court. In addition, any use of sensitive/personal information must align with Metrolinx policies, privacy legislation, and judicial directives, such as, the redaction of third-party personal data not essential to the case.

PUBLIC RELEASE OF DEMS MATERIAL

Public access to information in DEMS must comply with provincial and federal privacy laws. While the public generally cannot access digital evidence directly, access may be granted through formal Freedom of Information (FOI) requests governed under FIPPA. DEMS must support these requests with features such as redaction, metadata suppression, and secure, time-limited viewing links. When evidence is presented in open court, it may become public record, thus DEMS must enable lawful extraction and sharing while protecting sensitive information such as the identities of victims, minors, vulnerable persons, or third parties.

The system must also log all access events, maintaining a complete record of who accessed what information, when, and under what authorization. These access events will be audited to verify that only authorized personnel have accessed the records for the purpose of performing their duties. Privacy-by-design principles must be maintained during any public-facing use of evidence, and system administrators must have oversight tools to review and approve all public disclosures in a manner which does not compromise legal integrity, privacy rights, or ongoing investigations.

DISPOSITION OF MATERIAL STORED IN THE DIGITAL EVIDENCE MANAGEMENT SYSTEM (DEMS)

The disposition of material from within DEMS must be governed by strict legal, procedural, and technological controls to maintain compliance with evidentiary, privacy, and records management requirements. Disposition processes shall align with Metrolinx's Records and Information Management (RIM) Policy, Disposition Process, applicable legislation, including the Archives and Recordkeeping Act, and the Metrolinx's Records Retention Schedule. Evidence must not be deleted arbitrarily or prematurely, especially if it may be subject to ongoing investigations, court proceedings, and/or disclosure obligations. All evidence captured in DEMS will be retained and deleted in accordance with the Metrolinx Records Retention Schedule.

Permissions in DEMS must allow only authorized personnel, typically evidence custodians or system administrators, to initiate disposition, and only after confirming that legal and operational retention criteria have been met. Any disposition of data shall align with the appropriate record series within the Metrolinx Record Retention Schedule. Prior to disposition, the system will trigger a review of workflows and require multiple levels of approval to prevent accidental or unauthorized loss of data. All disposition actions must be logged in tamper-proof audit trails, documenting who initiated the disposition, when it occurred, the rationale, and which files were affected. In cases involving public complaints, civil litigation, or internal investigations, DEMS shall also support legal holds to prevent automatic or scheduled disposition. When evidence is lawfully deleted, the system shall maintain complete and secure erasure of the data from both primary and backup storage environments to meet privacy and data protection standards. Overall, disposition shall be handled as a tightly controlled process that balances the need for responsible data lifecycle management with the legal obligation to preserve and protect digital evidence.

TRAINING REQUIREMENTS

The successful implementation of DEMS requires comprehensive training to support that all Authorized Officers, as well as relevant managers, investigators, and administrative staff, understand the operational, legal, and ethical responsibilities of DEMS use.

In-person training is mandatory for all personnel who utilize DEMS and its associated data. This includes detailed instructions on the technical aspects of DEMS and will be supported by the DEMS Procedure Guide.

Refresher training shall be delivered regularly to reinforce policy, standards, procedures and adapt to changes in legislation, technology, or operational requirements. All training will emphasize the ethical responsibilities of using DEMS, focusing on security, data integrity, transparency, professionalism, and maintaining public trust.

LEGAL AND COMPLIANCE REQUIREMENTS

Legal and compliance requirements for DEMS are critical to supporting that digital evidence is handled in a manner that upholds the rule of law, respects individual privacy rights, and maintains evidentiary integrity for use in judicial proceedings. DEMS must comply with the Freedom of Information and Protection of Privacy Act (FIPPA) which governs the collection, use, retention, and disclosure of personal information by public bodies. It must also align with the Criminal Code of Canada and Canadian Charter of Rights and Freedoms, particularly concerning lawful search and seizure, disclosure obligations, and the right to a fair and unbiased trial. The system must support the proper documentation and enforcement of chain of custody procedures to preserve the admissibility of evidence in court.

Data retention and disposal must comply with Metrolinx's Record Retention Schedule, Metrolinx's Records and Information Management (RIM) Policy and Disposition process, and will be carried out securely, consistent in a manner that's appropriate with the sensitivity level of the information. Additionally, DEMS will provide tools to manage disclosure obligations, supporting that relevant evidence is shared with defense counsel in a timely and secure

manner. The system shall undergo regular audits to demonstrate compliance with applicable laws, regulations, and Metrolinx policies such as the Metrolinx Information Security Policy and to support that it is adaptable to future legislative or policy changes affecting digital evidence management in Ontario.

COMPLIANCE AND ACCOUNTABILITY

Compliance and accountability for DEMS is essential to uphold legal requirements, protect individual rights, and maintain public trust in Metrolinx. To maintain ongoing compliance, the system must incorporate robust audit and monitoring capabilities, including immutable logs of all user activity such as uploads, downloads, views, edits, dispositions, and disclosures which can be reviewed during internal audits, legal proceedings, or investigations into misuse compliance checks, Privacy Impact Assessments (PIAs), and Threat Risk Assessments (TRAs) must be conducted to evaluate the system's adherence to legislative and policy standards, particularly when updates or new integrations are implemented in a timely manner. Additionally, training and education programs are mandatory for all users to support that they understand their legal responsibilities and the potential consequences of misuse, such as disciplinary action, civil liability, or criminal prosecution. System administrators have the authority and tools to enforce compliance, investigate irregularities, and support that digital evidence is managed with integrity, transparency, and accountability at all times.

SYSTEM ADMINISTRATION AND MAINTENANCE

System administration and maintenance for DEMS must be designed to support continuous, secure, and efficient system operation, in alignment with Metrolinx cybersecurity controls and applicable provincial and federal governance standards. This includes implementing appropriate access management, encryption, logging, and monitoring practices to safeguard sensitive data and maintain system integrity

Administrative functions must include comprehensive user and access management, enabling system administrators to assign, modify, and revoke access based on clearly defined roles and responsibilities, following the principle of least privilege. Administrators are also responsible for managing system and security configurations, monitoring storage capacity and system health, and supporting optimal system performance as evidence volume increases. These activities must align with Metrolinx cybersecurity policies and standards, including secure configuration, access control enforcement, and continuous monitoring to maintain system integrity, security, and data protection.

Regular system maintenance, such as software patching, vulnerability remediation, database optimization, and system log reviews must follow a documented change management protocol in accordance with Metrolinx's IT Change Management Procedure. Maintenance activities should be scheduled to minimize operational disruption and maintain alignment with Metrolinx's cybersecurity policies and standards

System administrators will have access to advanced monitoring tools that provide real-time alerts for system faults, unauthorized access attempts, or abnormal usage patterns. All administrative actions must be fully logged and auditable to facilitate both internal oversight

and external compliance verification. To maintain alignment with evolving legislative mandates and organizational standards, DEMS must be subject to regular security evaluations. These include Threat Risk Assessments (TRAs), penetration testing, and compatibility assessments.

Additionally, comprehensive documentation, continuous training programs, and robust support mechanisms must be established to support administrators are well-prepared to manage the platform effectively and respond promptly to emerging technical challenges or regulatory updates.

ROLES AND RESPONSIBILITIES

CPS Vice President

The CPS Vice President is responsible for the following:

- Provide oversight and support the consistent application of this Standard.

CPS Director, Professional Standards

The CPS Director, Professional Standards is responsible for the following:

- Support the implementation and compliance with this standard and all associated procedures.
- Communicating and implementing the Standard and associated Procedure Guide to applicable Metrolinx employees.
- Handling and reporting issues of non-compliance pertaining to the use of DEMS.

Authorized Officers

Authorized Officers (Customer Protection Officers, Revenue Protection Officers, and Station Safety Ambassadors) are responsible for the following:

- **Proper Usage**: Operate DEMS in accordance with established protocols and permissions granted based upon the Authorized Officer's respective role and job duties.
- **Digital Evidence Management**: Upload digital photographs, audio recordings, and video recordings in a timely and accurate manner in accordance with CPS Metrolinx data management procedures.
- **Data Integrity**: Maintain the integrity of digital evidence by following proper handling procedures and maintaining that digital photographs, audio recordings, and video recordings are not altered, deleted, or mishandled.

CPS Managers

CPS Mangers are responsible for the following:

- Monitoring CPO/RPO/SSA compliance with DEMS procedures as stated in the DEMS Procedure Guide.

CPS Investigations

The Investigations Team is responsible for the following:

- The coordination and collection of digital evidence requested by law enforcement agencies and supporting compliance with legal, regulatory, and procedural guidelines pertaining to evidence handling.
- **Digital Evidence Management**: Upload digital photographs, audio recordings, and video recordings in DEMS in a timely and accurate manner in accordance with CPS data management directives.
- **Data Integrity**: Maintain the integrity of digital evidence by following proper handling procedures and maintaining that digital photographs, audio recordings, and video recordings are not altered, deleted, or mishandled.

CPS Data & Analytics Team

The CPS Data & Analytics Team is responsible for the following:

- Reporting program performance and statistics (generating reports).
- Approving permissions for DEMS users based upon a role-based access control matrix.

Metrolinx IT Team

The Metrolinx IT Team is responsible for the following:

- Assisting in the technical setup, deployment, data management, and cybersecurity and compliance requirements for the digital evidence program.
- Managing permissions and user accounts while maintaining system integrity and software.
- Liaise with the DEMS service provider in order to provide technical support for the DEMS Platform.

CPS Training and Development

The CPS Training & Development Team is responsible for the following:

- The development and implementation of a robust training program which supports CPS employees are properly trained to access and utilize DEMS and understand the responsibilities each role has with access, control, and safeguarding of digital evidence.

CPS Risk and Audit Team

CPS Risk & Audit is responsible for the following:

- Conduct routine audits as per the Audit Program Standard.
- Developing recommendations to address non-compliance.
- Supporting the development of Corrective Action Plans (CAPS) that will support

that issues of non-compliance are addressed fully.

- Conduct follow-up audits to maintain that the DEMS program adheres to Metrolinx policies, privacy regulations, standards, and IPC guidelines.

ESCALATIONS AND EXCEPTIONS

Any exceptions or instances of non-compliance with this Standard shall be escalated to the Director of Professional Standards. Failure to comply with this Standard or the affiliated job aids may result in disciplinary action, up to and including dismissal.

REFERENCES

Archives and Recordkeeping Act
Audit Program Standard
Audio and Video Recording Policy (CSM-0202-01)
Body Worn Cameras Procedure Guide (CSM-0202-02P)
Closed Circuit Television Standard (CSM-0202-05)
Closed Circuit Television Procedure Guide (CSM-0202-05P)
Critical Cyber Systems Protection Act (CCSPA)
Digital Evidence Management System (DEMS) Procedure Guide (CSM-0202-06P)
Drone Operation and Maintenance Standard (CSM-0202-04)
Drone Operation and Maintenance Procedure Guide (CSM-0202-04P)
Freedom of Information and Protection of Privacy Act
Information Sharing Procedure Guide (CSM-0202-08P)
Information Sharing Standard (CSM-0202-08)
Information Security Policy (CA-0504-02)
IPC Model Governance Framework for Body Worn Camera Programs in Ontario
IT Change Management Procedure (CA-0502-12P)
Metrolinx Enterprise Data Governance and Management Policy (CA-0701-01)
Metrolinx Enterprise Privacy Policy (CA-0901-01)
Metrolinx Records Disposition Process (CA-0402-06P)
Metrolinx Record Retention Schedule
Records and Information Management (RIM) Policy (CA-0402-01)

ADMINISTRATION

Identification Name	Digital Evidence Management System (DEMS) Standard
Approved By	Chief Operating Officer
Owner	Vice President, Customer Protective Services
Monitor	Director, Customer Protective Services Professional Standards
Original Approval Date	
Review Frequency	Annually
Supersedes	N/A

STANDARD HISTORY

Revision / Review Date	Author	Description
December 10, 2025	Customer Protective Services, Professional Standards	New Standard

DEFINITIONS

Accidental: An event which occurs inadvertently, or unexpectedly.

Body Worn Camera (BWC): A device worn by an Officer for the purpose of recording video and audio information.

Chain of Custody: The documented chronological history of evidence, meticulously tracking its possession, control, transfer, analysis, and disposition from the moment of collection to its presentation in legal proceedings.

Closed Circuit Television Camera (CCTV): A system which uses video cameras to transmit a signal to a specific set of monitors or recording devices, rather than broadcasting it openly.

Corrective Action Plans (CAPs): Detailed, structured approach that outlines the steps an organization will take to address and resolve issues identified during an audit or other evaluation process.

Customer Protection Officer (CPO): A person employed by Metrolinx who has been appointed by the Commissioner of the Ontario Provincial Police, and approved by the Solicitor General, as a “Special Constable” in accordance with S. 92 of the Community Safety and Policing Act, with powers and duties as set out in the appointment.

Digital Evidence: Includes, but is not limited to digital photographs, audio recordings, and video recordings captured by Metrolinx personnel in relation to an investigation, Metrolinx system or safety related matter.

Digital Evidence Management System (DEMS): A cloud-based digital evidence management system, which provides secure storage, organization, and sharing of digital evidence.

Manager: An employee who is responsible for directing, supervising, and monitoring the work of Customer Protection Officers, Revenue Protection Officers and Station Safety Ambassadors.

Metadata Tagging: The process of adding descriptive information to digital files and other data to make them easier to find, organize, and manage. These tags act as labels that provide context and meaning about the data, allowing users and systems to better understand and interact with it

Privacy Impact Assessment (PIA): A systematic process for identifying, assessing, and mitigating potential privacy risks associated with a project, program, or system that involves the collection, use, or disclosure of personal information.

Redaction: A process to obscure or remove parts of a record, such as personal information, prior to publication or release.

Revenue Protection Officer (RPO): A person employed by Metrolinx who carries out the responsibilities of carrying out Metrolinx Fare Non-Compliance Interactions in accordance with the proper escalation procedure and engage with passengers and assist with fare-related or general questions.

Station Safety Ambassador (SSA): Uniformed Metrolinx employees responsible for detecting and deterring disorder and protecting the safety and security of customers and employees throughout Metrolinx properties. SSAs are appointed under subsection 21(5) of the Metrolinx Act, 2006 as Provincial Offence Officers for the purposes of administering and enforcing Metrolinx by-laws.

Threat Risk Assessment (TRA): A security evaluation process used to identify, assess, and mitigate cybersecurity threats and risks associated with technology deployments. It supports compliance with Metrolinx Cybersecurity Policies, NIST, and ISO 27001 by analyzing threats, vulnerabilities, and potential impacts, and recommending security controls to protect Metrolinx's systems and data.

Vulnerable Person(s): A person who is believed to be someone in need of special care due to: cognitive, physical, intellectual, or developmental disability; needing protection from themselves or others (e.g. a person experiencing mental health challenges, suicidality, intimate partner violence, human trafficking, etc.); or any other condition/state which may place them at increased risk (e.g. a person perceived to be under-housed/experiencing homelessness, experiencing poverty, experiencing substance use issues, etc.).