TRANSIT POLICE

EVIDENCE (AND DIGITAL EVIDENCE MANAGEMENT SYSTEM)

Effective Date: May 9, 2005
Revised Date: March 28, 2023
Reviewed Date:
Review Frequency: Annual
Office of Primary Responsibility: Deputy Chief Officer Operations

TABLE OF CONTENTS (with Quick Links)[1]

[1] Use **CTRL + HOME** to return to the Table of Contents from anywhere in this document.

POLICY

Definitions

Axon ® "Capture App" ("Capture App") – The Transit Police's designated mobile device application used to:

(1) Capture photographs, audio statements and video, and any other digital evidence, related to police investigations for upload to Transit Police's digital evidence management system; and

(2) Invite members of the public to submit photographic, video, audio and documentary evidence of an incident via a link shared through the "Capture App".

Axon ® FIPPA S.15 - Harm to Law Enforcement – Web-based application containing Transit Police's instance of the DEMS environment and all evidence uploaded through "Capture App" or "Upload XT".

Axon ® "Upload XT" ("Upload XT") – Transit Police's designated Windows-based desktop application used to easily upload non-"Capture App" generated digital evidence to the Transit Police FIPPA S.15 - Harm to Law Enforcement site.

BCPPS – BC Provincial Policing Standards.

Court Liaison –Transit Police Personnel assigned to the Court Liaison Unit (i.e., Court Liaison Officer, Court Clerk) to perform Court notifications and help facilitate Court related matters.

DEMS – Per Ministerial Order No. M389/2021, the information management system provided by PRIMECORP (Police Records Information Management Environment Incorporated) required to be used by law enforcement services as a digital evidence management system to capture, collect, upload, manage, share and disclose digital evidence.

DEMS Administrator – The Transit Police position designated by the Manager Information Management Section to administer the DEMS in accordance with the law, BCPPS, the Transit Police DEMS Governance Committee, the Provincial DEMS Governance

Committee, associated MOUs and Transit Police policy and procedures, and to provide DEMS technical/training support to Transit Police Personnel.

Digital Evidence – Includes, but is not limited to, digital photographs, audio recordings and video recordings captured or obtained by Transit Police during a police investigation.

DWG/eIM Naming Conventions – Disclosure Workflow Guidelines/electronic Information Management Naming Conventions as prescribed by the Memorandum of Understanding on Disclosure Between British Columbia Police Agencies and the British Columbia Prosecution Service; Ministry of Attorney General, Criminal Justice Branch; and the Public Prosecution Service of Canada, British Columbia Region.

Evidence – Any items seized or acquired by a Member during the course of an investigation or for the purposes of an investigation or court proceeding, including any original paper documents. Evidence can be physical (e.g. knife) or digital (e.g. digital photo of a knife).

Exhibit Custodian – The Transit Police Personnel designated by position to maintain property control for the Transit Police. This position has Special Provincial Constable status.

Exhibit Room – A secured facility used by the Transit Police Exhibit Custodian to store all property collected by Members.

JPD – Jurisdictional Police Department.

Member – Refers to a Designated Constable (all ranks), the Chief Officer or a Deputy Chief Officer, and a Designated Law Enforcement Officer of the Transit Police.

Metro Vancouver Transit Police ("Transit Police") – The operating name for the South Coast British Columbia Transportation Authority Police Service (Designated Policing Unit and Designated Law Enforcement Unit).

Police-Crown MOU – The Memorandum of Understanding on Disclosure Between British Columbia Police Agencies and the British Columbia Prosecution Service; Ministry of Attorney General, Criminal Justice Branch; and the Public Prosecution Service of Canada, British Columbia Region that governs the obligations of the parties in relation to disclosing materials for use in a trial.

RMS – The approved Records Management System, records management policy and procedures used by Transit Police.

Temporary Exhibit Locker – A designated secure temporary storage location for Members to secure property that will be collected by the Exhibit Custodian.

Transit Police and Jurisdictional Police Memorandum of Understanding ("TP-JPD MOU") – The TP-JPD MOU establishes the operational and procedural protocols between Transit Police and Jurisdictional Police with respect to policing and law enforcement within the Transportation Service Region.

Transit Police Personnel – Members and civilian professionals who work for the Transit Police. For the purpose of this policy, this includes persons contracted to work with or for TransLink Security Management Limited.

Transitory Area – For the purposes of this policy; the designated temporary digital storage location [redacted] FIPPA S.15 - Harm to Law) used by Members to view or process evidence (i.e. transcription, redaction, drafting, etc.) prior to uploading into the DEMS or the RMS.

Authority

1. Certain authorities and powers are granted to peace officers from both statute (e.g., *Criminal Code* and *Police Act*) and common law in order to seize or otherwise acquire evidentiary items in the course of carrying out their duties. Members will collect and process evidence in a manner that is consistent with statute, the law, BCPPS, PRIME policy and Transit Police policies.

General

2. All evidence arising from investigations will be:

    (1) Acquired, handled and disposed of in a manner that complies with legal requirements, Transit Police protocols, policy and best practices; and

    (2) Processed in a manner that:
        a. Identifies and records each item of evidence;
        b. Lists the source of the item or items;
        c. Ensures the preservation of the condition of the evidence;
        d. Names the person collecting the item or items;
        e. Provides continuity of possession by recording each time a transfer of possession takes place; and
        f. Meets the requirements of the investigation and prosecution of the case.

3. All evidence submitted to a laboratory for examination will include prior possession information, including:

    (1) Name of the Member last having custody of the item;

    (2) Date and time of submission or mailing and method used for transmission;

    (3) Date and time of receipt in the laboratory; and

    (4) Name and signature of the person in the laboratory receiving the evidence.

4. All evidence submitted to a forensic laboratory for examination will be done so in a timely manner and guided by the conditions relative to the investigation.
[BCPPS Addendum 1 - D8.1 and D8.2]

PROCEDURES

PART A - Physical Evidence

5. All physical evidence will be seized or otherwise collected (e.g., found, acquired through surrender, etc.) and processed in accordance with the relevant provisions of Transit Police policy chapters OD130 – Seizure and OF020 – Exhibit/Property Control.

PART B - Digital Evidence

Limitations on the Use of the DEMS

6. Unless otherwise directed, Members will not upload evidence classified as Protected Level "C" (i.e., informants, witness protection and national security) to the DEMS.

7. While Transit Police specialized units may follow some Major Case Management ("MCM") practices in their files, Transit Police does not meet the requirements of an MCM agency as defined in BCPPS 5.2.1; therefore, all Members and sections of the Transit Police will utilize the DEMS to manage their digital evidence.

Requirement to Use the DEMS

8. As per the *Information Management Systems (Digital Evidence Management System) Regulation* (the "*Regulation*") under the authority of the *Police Act*, Transit Police, as a law enforcement service specified in the Schedule of the *Regulation*, must use Axon's ® DEMS system.

9. Members will be issued a Transit Police approved mobile device with Axon's ® "Capture App" installed and must use the "Capture App" to collect digital evidence (i.e., digital photographs, audio statements and video) in the field. Additionally, Members will consider utilizing the "Community Request" component of the "Capture App" to invite members of the public/businesses to submit digital evidence, photographs, video, or documents to the Member's DEMS file.

    (1) A reminder that Transit Police Personnel must promptly report to their Supervisor if their issued mobile device is lost, stolen or damaged. The Supervisor will then provide written notification to the Transit Police designated Telecommunications Coordinator of same and ensure all necessary reports are completed [refer to Transit Police Policy AG010 – Property Management]. Prompt action by Transit Police Personnel in such situations is required so that Transit Police IT can disable the Mobile Device and allow for the implementation of security protocols.

10. There may be instances where Members will be unable to collect evidence from a citizen/business either via the "Community Request public portal" or by utilizing the "Community Individual Request" feature (e.g., file size is too large or inability to zip file). In such cases, Members will utilize a Transit Police authorized portable drive to obtain the evidence, following all of the procedures outlined in the processing of digital evidence from a portable drive [refer to Transit Police SOP73 – Use of Portable

Drives]. If the file size of the evidence is still too large to download, Members will contact the DEMS Administrator for guidance.

11. All digital evidence, collected from any source and in any form, is to be uploaded to the DEMS as soon as practicable, but no later than the end of the Member's shift, unless otherwise authorized by a Supervisor.

"Capture App" Failure

12. In the event the "Capture App" fails due to a technical issue, Members will utilize the following options as a secure back up:

    (1) Photographs/video will be obtained using the secure "work" side of the Member's issued mobile device. All photographs and video taken will be stored in a secure gallery on the "work" side of the mobile device and can be uploaded to the DEMS utilizing the import feature within the "Capture App" or via "import evidence" feature of FIPPA S.15 - Harm to Law Enforcement

    (2) Audio statements will be taken on a Transit Police issued digital audio recorder and uploaded to the DEMS, utilizing the "import evidence" feature of FIPPA S.15 - Harm to Law Enforcement

DEMS Protocols

13. Members will follow the procedures within this policy and other supplemental user guides (where issued) for the collection and processing of digital evidence using the DEMS.

14. Supervisors and Readers, with authorization from the Manager Information Management Section ("Manager IMS") or Staff Sergeant and higher rank, are authorized to "Restrict" access to an entire case file or individual piece(s) of evidence in the DEMS. Members wishing to utilize the restrict feature in the DEMS will submit a request to their Supervisor to approve the use of this feature and to make a case file or individual piece(s) of evidence restricted.

15. Before restricting access to an entire case file, or individual piece(s) of evidence, the Supervisor must ensure that the report meets at least one of the following criteria:
    a. Evidence being restricted is "hold back" evidence;
    b. Evidence contains sensitive or confidential information; or
    c. A Major Crime, as defined in BCPPS 5.2.1, is involved.[2]

[2] According to the Standard, investigations where major case management is automatically required include: (a) Homicides, as defined in s. 222(4) of the *Criminal Code*; (b) Missing persons, if foul play is suspected; (c) Found remains, if homicide is suspected; (d) Sexual assaults that are suspected to be serial or predatory in nature; (e) Criminal investigations of: (i) workplace deaths or serious injury, or (ii) mass casualties and injuries; and (f) Non-familial abductions. Major case management is also required for any other investigation, including a type or category of investigation, or a particular investigation, which the chief constable, chief officer, or commissioner, or a delegate thereof, has determined, with due regard to the factors listed in Standard (3) of BCPPS 5.2.1 Threshold and Reporting, requires major case management.

16. Any evidence related to a "Private" file in PRIME will be assigned a "Restricted" access class in the DEMS [for more information on "Private" and "Invisible" files refer to Transit Police Policy AF130 – Making Records Private or Invisible].

Restricting Access to Evidence - Identified Sensitive Documents

17. From time to time, Members deal with documents that require a higher level of protection. While most documents will be uploaded to the RMS and saved as an attachment, sensitive documents will be uploaded to the DEMS. Transit Police has identified the following documents as requiring added levels of security/access:

Medical Documents

(1) Members will save medical documents in PDF format and upload them to the DEMS. Once uploaded to the DEMS, the investigating Member will contact the DEMS Administrator and their Supervisor, either of whom may restrict the piece(s) of evidence.

Applications for Judicial Authorizations Nourished by Confidential Informant Information

(2) Any applications for judicial authorizations that are nourished by Confidential Informant information need to have the highest level of protection applied to protect the integrity of the source and the information provided. The following procedures will be followed:

a. The Lead Investigator/Affiant will complete the affidavits related to the application for judicial authorization, taking care to not use language that could identify their source;
b. When the document is saved in the Transitory Area during the drafting process, in Word format, a password will be applied to it;
c. This document password will be shared with only those Members who need access to the document (e.g., Lead Investigator, Supervisor and Source Coordinator); and
d. Once the drafting process is completed, the document will be saved in PDF format and have a password applied to it, prior to being uploaded to the DEMS. The Lead Investigator will contact the DEMS Administrator or their Supervisor to have the piece(s) of evidence restricted.

NOTE: There may be other sensitive documents that need this level of protection and it may be that the process of restriction could vary from document to document. The Deputy Chief Officer Operations or delegate may add additional classes of sensitive documents to this list.

Transitory Area

18. Members and authorized civilian personnel may download evidence to the designated Transitory Area on a short-term, temporary basis, only for the purposes of viewing or processing evidence, or drafting documents, prior to uploading to the RMS or the DEMS. Examples of when temporary downloading for viewing and processing may be required include:

(1) The file format is not supported by the DEMS;

(2) Drafting of an Information to Obtain is required;

(3) The evidence must be processed in another software program, such as for vetting and redaction or other purposes; and

(4) Evidence is received on an external storage device that needs to be copied from the device and saved to the Transitory Area, prior to upload to the DEMS.

19. Members and authorized civilian personnel will delete any draft documents or evidence from the Transitory Area once they have finished viewing or processing it.

20. To maintain the security of evidence files and to ensure that the Transitory Area is only used to store evidence temporarily while being viewed or processed, files will be frequently purged from the Transitory Area Disclosure, Downloads, and Uploads folders on a scheduled basis. The 'Working Documents Drafts' folder will be backed up and only purged upon confirmation that the documents are no longer in draft format and have been uploaded to the appropriate repository (DEMS or RMS). The file purge schedule will be as authorized by the Deputy Chief Officer Administrative Services, in consultation with the Manager IMS and DEMS Administrator, and may be adjusted from time to time.

All DEMS Evidence Requires a GO Number

21. A PRIME GO number is required every time the "Capture App", "Upload XT", or the "import evidence" feature of [redacted] is used to collect evidence. The evidence collected is associated to the PRIME GO number within the DEMS.

Special Study Flag

22. All Members who have captured digital evidence associated to their files must apply the Digital Evidence "DE" Special Study Flag on the front page of their PRIME GO.

(1) Authorized civilian personnel or a Supervisor may apply the Special Study Flag if the Member has omitted it.

Audio Statement

23. Members will utilize the "audio" component of the "Capture App" to obtain all witness statements in the field, unless circumstances present themselves that preclude the Member from doing so. For more on this, refer to Transit Police policy chapters OD140 – Statements and OD240 – Suspect Interviewing – Patrol Based Investigations, and SOP17 Transcription and Back-Up Audio Recordings. (The management of statements will be done from within the DEMS environment in [redacted])

(1) Members are reminded to ensure that the environment they are taking the statement in is suitable for doing so, free of background noise and eavesdropping.

Video Component

24. Members will utilize the "video" component of the "Capture App" in any situation where they are capturing video in the field for evidentiary purposes. In the event that the Member is interrupted during the video, they may wish to start over and delete the first video prior to upload to [redacted]. The following are examples of where it would be appropriate to use the "video" component of the "Capture App":
    a. Pre/post search of a residence when executing a search warrant;
    b. Pre/post search of a vehicle at roadside;
    c. Capturing video of a larger scene to augment digital photos already taken; and
    d. In exigent circumstances, to conduct a non-custodial interview in the field.

"Community Request" Component

25. Whenever possible, Members will utilize the "Community Request" function of the "Capture App" to obtain digital evidence (such as photographs and video) from members of the public. Members will send a request to the member of the public, which is valid for 10 days. Members should have an awareness of the size limitation for the "Capture App", which is currently set at 16 GB and will be adjusted from time to time. This limit will be sufficient in most instances. In the event a member of the public's evidence exceeds the capacity of the "Community Request" function, only then would Members consider utilizing MoveIt, an external storage device, or other designated tool.

Public Portals

26. The DEMS allows for Transit Police to stand up a "Public Portal", creating a unique uniform resource locator ("URL") that can be shared with the public to enable large numbers of citizens to send digital evidence directly to police. "Public Portals" are not stood up often due to the resources required to triage and analyze the influx of such a significant amount of digital evidence. Typically, a "Public Portal" is stood up where there has been a significant criminal event involving a large number of offenders and/or crime scenes (e.g., a riot, and police wish to solicit relevant video and photo evidence that has been captured on mobile devices or CCTV cameras).

27. When a "Public Portal" is determined to be necessary, the investigating section's Supervisor will seek authorization from their Inspector to ensure that a plan and sufficient resources are in place to manage the incoming evidence. Investigators will liaise with Media Relations Section to develop the communication that will invite members of the public to upload digital evidence.

    (1) The Watch Commander or Section Supervisor will be responsible for creating the "Public Portal", ensuring that they add the investigative file number (e.g., GV-2023-12345) at the end of the URL. The Supervisor will assign the Portal Owner as the Investigating Member.

Digital Evidence Pertaining to Violation Tickets ("VTs")

28. Members will utilize the "Capture App" when gathering digital evidence related to VTs. Where a VT is issued and the circumstances are such that a PRIME GO has been

created, the digital evidence will be uploaded with the PRIME GO number associated to the call for service or created by the Member based on the circumstances.

29. Where there is no requirement for a GO to be created, Members will use the bulk GO for that month to upload their digital evidence associated to the VT issuance. Members uploading digital evidence to the bulk file will follow the process outlined in the DEMS Handbook, ensuring they apply the appropriate naming convention to their evidence in the bulk file.

Other Storage Location

30. Members will not store digital evidence in any location other than within the DEMS system, such as personal H: drives.

Deleting Evidence

31. Members will have the latitude to determine what the best evidence is and which evidence is to be committed to FIPPA S.15 - Harm to Law Enforcement. Members are able to review their digital evidence in the "Capture App" and decide whether it is appropriate for them to ***"delete prior to upload"***. This functionality allows the Member to eliminate the need to manage unnecessary evidence after upload and avoid inappropriate evidence from being uploaded to the DEMS. If a Member is uncertain whether it is appropriate for them to delete something from the "Capture App", they are to consult with a Supervisor. Following are some examples of when it may be appropriate for Members to delete files prior to upload:
    a. Digital image is blurry;
    b. Duplicate digital image is taken;
    c. Thumb in the picture;
    d. Member interrupted during a video.

    (1) Members are not to delete evidence prior to upload for purpose of avoiding allegations of misconduct or impropriety.

32. Generally, once evidence is uploaded to the DEMS, it becomes disclosable and should not be deleted. It is recognized that there are some situations where it would be appropriate to delete evidence from a case file, such as when a Member inadvertently uploads an exact duplicate copy of evidence from an external source utilizing the import feature in FIPPA S.15 - Harm to Law Enforcement. The following procedures will be followed in the event a Member believes that evidence that should be deleted from their case file:

    (1) The Member must have their Supervisor review the circumstances and agree that the evidence is not required;

    (2) The Supervisor will forward correspondence/E-mail to the DEMS Administrator at FIPPA S.15 - Harm to Law Enforcement, articulating the rationale for deleting the evidence; and

(3) Upon receipt of correspondence/E-mail) from the Supervisor, the DEMS Administrator will delete the identified evidence, making robust notes in the "Notes" area, explaining why the evidence was deleted.

33. The DEMS Administrator and the Manager IMS are the only Transit Police Personnel authorized to delete evidence from the DEMS [FIPPA S.15 - Harm to Law Enforcement]), unless otherwise so determined by the Deputy Chief Officer Administrative Services. Transit Police recognizes that application of the DEMS in the policing environment is predicated on controlling access to digital evidence and the creation and maintenance of an audit trail; therefore, the permission to delete must be restricted.

Purging and Retention

34. Purging and retention will be in accordance with purging and retention in the RMS.

Viewing DEMS Evidence Internally and Externally

35. Transit Police will have a "presumptive viewing" model within their own instance of the DEMS, which means that all authorized (licensed) Transit Police Personnel will be able to view all Transit Police uploaded evidence within the DEMS without any additional permissions, with the exception of "Restricted Access" evidence. However, Transit Police Personnel will refrain from viewing evidence in the DEMS unless:

(1) They have a valid investigative reason for needing to view the evidence; or

(2) They are required to access the evidence in order to fulfill their job function (i.e. Court Liaison).

36. Transit Police Personnel are advised that the DEMS maintains a robust audit trail and it will document the date, time, location (IP Address) of all evidence that is viewed and who viewed it. Transit Police Personnel are reminded of their obligations set out in Transit Police Form AZ1350 – Handling of Designated and Classified Information and that any breach of the specified requirements may result in the immediate revocation of access to any Designated and Classified Information; to discipline, up to and including termination of employment; and to criminal charges.

External Sharing

37. Unless otherwise directed by the Chief Officer, Transit Police will continue to follow the current process for sharing information with JPDs, in accordance with the TP-JPD MOU.

Reassigning Evidence and Case Files within the DEMS

38. As part of file management, Supervisors will be responsible for managing both the investigative file in PRIME and the digital evidence within the DEMS. There will be times where a Supervisor may need to re-assign an investigative file to another Investigator (i.e., transfer, resignation or extended absence of a Member). In such cases, the re-assignment of the PRIME file will trigger the re-assignment of the DEMS evidence if the file is open and being actively investigated. Supervisors will also ensure that access to any password-protected documents previously

managed by a departing Member has been transferred to another Member. For more guidance on Members terminating employment, refer to s. 47 of this policy.

Sharing Digital Evidence Obtained Outside of "Capture App"

39. Members are advised that it is not best practice to take a photograph of paused video and upload the photograph to the DEMS. However, it is recognized that there may be exigent circumstances, in the interest of public or officer safety, where it is appropriate to capture a digital photo of a paused video. In such cases, and after consultation with a Supervisor, Members will be permitted to share an image with other authorized police personnel, prior to receiving the video evidence into the DEMS through established processes. *(E.g., a suspect has stabbed someone and fled via the SkyTrain; Members could obtain a still image of the suspect from a paused video and, due to the threat to public and officer safety, then push the image out via E-mail to officers responding to the call)*

    (1) In such exigent circumstances, the Members will be required to make a note in their notebook that the image was shared out via E-mail and then upload the image to [redacted] as soon as practicable thereafter, but no later than the end of their shift.

Application of DWG/eIM Naming Conventions

40. Members and authorized civilian staff will be responsible for applying and reviewing the DWG/eIM naming conventions to their evidence uploaded to [redacted], regardless of whether it is uploaded from the "Capture App", "Upload XT", or the "import" feature of [redacted][3]

41. Supervisors will be responsible for ensuring that their Members are applying the required naming conventions.

42. The DEMS Administrator will perform regular auditing of the system to ensure that Members and authorized civilian personnel are applying the naming conventions and, where required, and notify the Member's Supervisor in writing to request that any required work be completed.

Roles and Responsibilities

43. The Manager IMS will provide oversight for the ongoing delivery and maintenance of the DEMS within Transit Police.

44. The DEMS Administrator will be the point of contact for Transit Police Personnel who require assistance with using the DEMS. The DEMS Administrator role will also include, but is not limited to, providing quality assurance in monitoring adherence to the DEMS evidence management requirements, including naming conventions.

[3] Application of the DWG/eIM compliant naming conventions is critical to ensure that the required information management standard is maintained according to the syntax laid out in the Police-Crown MOU.

(1) The PRIME Administrator is authorized to perform the duties of the DEMS Administrator when the DEMS Administrator is on leave or as otherwise assigned by the Manager IMS for off-duty support or coverage.

45. The Operations Communications Centre ("OCC") Manager or delegate and the Exhibit Custodian will use "Upload XT" to upload into the DEMS any digital evidence that they manage within their respective areas.

    (1) The OCC Manager or delegate will upload audio from the OCC operational channels or taped telephone lines.[4]

    (2) The Exhibit Custodian will utilize "Upload XT" to upload TransLink subsidiary video received via "MoveIt" or other designated mechanisms.

46. Court Liaison will ensure that:

    (1) All sensitive attachments and transcripts that go to BC Prosecution Service ("BCPS") are added to the DEMS, in order to provide BCPS with the required evidence for disclosure; and

    (2) All electronically disclosed evidence and related aspects of a Report to Crown Counsel ("RTCC") that are being disclosed through the DEMS adhere to the DWG/eIM naming conventions, according to the Police-Crown MOU.

    (3) All digital evidence pertinent to a Public Prosecution Service of Canada ("PPSC") file is to be stored in the DEMS, where the disclosure package will be assembled in the DEMS, after which it will be downloaded by Court Liaison and sent to PPSC through non-DEMS mechanisms.

Members Terminating Employment

47. All Members terminating employment or going on extended leave must notify the DEMS Administrator who, in conjunction with the Member's Supervisor, will ensure that all evidence on the Member's "Capture App" is uploaded to the DEMS prior to the Member departing the agency or beginning extended leave.

Audit and Monitoring

48. The DEMS maintains an audit log of system access and user activity, including files uploaded, viewed, edited, deleted and shared. The DEMS audit log is retained in perpetuity.

49. The DEMS Administrator or their back-up is the only user role who will have responsibility for managing access to the audit log when access is required. All requests for access to the audit log must be submitted to the DEMS Administrator in writing, articulating their justification (use FIPPA S.15 - Harm to Law Enforcement). Scenarios when an audit trail would be accessed include:

[4] In the future, the OCC Manager or delegate will also be responsible for uploading data from "Next Gen 9-1-1" sources.

(1) Professional Standards Unit investigation (including Office of the Police Complaints Commissioner investigations);

(2) Request from a court in order to examine continuity of evidence;

(3) DEMS Administrator system auditing, bug identification and resolution, and resolution of system issues;

(4) Upon request of a Transit Police Manager at Inspector rank or higher, with cause;

(5) Upon request of the Manager IMS;

(6) As required by the Senior Manager Risk, Emergency Planning and Analytics when conducting audits at the Direction of the Deputy Chief Officer Administrative Services; or

(7) As otherwise directed by the Deputy Chief Officer Administrative Services.

50. The authorized 'access list' to the DEMS audit log may be amended by the Deputy Chief Officer Administrative Services. Any access changes will be documented in writing.

Training

51. Members and authorized civilian personnel will receive training on the policy and procedures for using the DEMS, including the use of the "Capture App" to gather digital evidence, the application of DWG/eIM naming conventions, and the associated disclosure requirements, prior to receiving authorization to use it.

52. Members and authorized civilian personnel may also receive periodic refresher training, as deemed necessary by the Deputy Chief Officer Administrative Services.

Support

53. Transit Police Personnel needing assistance or having questions regarding the DEMS, this policy or any digital evidence gathering process/procedure are to E-mail FIPPA S.15 - Harm to Law Enforcement

54. Transit Police Personnel needing assistance or having questions regarding the DWG/eIM naming conventions are to E-mail FIPPA S.15 - Harm to Law Enforcement

55. Transit Police will establish an internal DEMS governance committee, with membership as so determined by the Chief Officer.

56. The Chief Officer will nominate one or more Transit Police Personnel to the province's DEMS Governance Committee.

References:
BC Police Act, RSBC 1966, c. 367

BC Police Agencies-BC Prosecution Service-Public Prosecution Service of Canada Memorandum of Understanding ("Police-Crown MOU")
Criminal Code of Canada [RSC 1985, c. C-46]
Canada Evidence Act, RSC 1985, c. c-5
BC Regulation 309/21 Information Management Systems (Digital Evidence Management System) Regulation
Transit Police - Jurisdictional Police Memorandum of Understanding (2020)
Transit Police Policy AF130 – Making Records Private or Invisible
Transit Police Policy OD130 – Seizure
Transit Police Policy OD240 – Suspect Interviewing – Patrol Based Investigations
Transit Police Policy OF020 – Exhibit/Property Control
Transit Police SOP17 – Transcription and Back-Up Audio Recordings
Transit Police SOP18 – Digital Imaging Request – TransLink Subsidiaries
Transit Police SOP61 – Mobile Communication Devices
Transit Police SOP73 – Use of Portable Devices