Sécurité organisationnelle
Services de protection des clients

Section	Programme intégré de vidéos et de preuve	Date d'approbation actuelle
Objet	Norme sur le Système de gestion des preuves numériques (SGPN)	Jour mois année

OBJET

Cette norme, ainsi que la Politique sur l'enregistrement audio et vidéo, le Guide de la procédure du Système de gestion des preuves numériques (SGPN) et la Norme d'échange de renseignements, énonce les principes et les exigences pour l'utilisation sécuritaire du SGPN par tous les employés de Metrolinx qui sont autorisés à avoir accès au système.

Metrolinx doit utiliser le SGPN pour établir la gestion sécurisée des preuves numériques. Ce quai commercial permet la collecte, l'organisation, l'analyse et l'échange efficaces des preuves numériques, y compris les images des caméras corporelles, les enregistrements des caméras-témoins de circulation à l'intérieur du véhicule, les images du système de télévision en circuit fermé (TVCF), les fichiers audio et les images de drones, au sein d'un environnement infonuagique centralisé. Le système prend en charge l'intégrité des preuves et soutient la collaboration tout au long de son cycle de vie.
Les agents autorisés, y compris les agents de protection des clients (APC), les agents de protection des revenus (APR) et les ambassadeurs de la sécurité en gare (ASG), sont équipés de matériel, de logiciels et d'outils mobiles intégrés pour télécharger, étiqueter, cataloguer et stocker en toute sécurité les preuves numériques, conformément aux protocoles approuvés par Metrolinx. Pourquoi avons-nous besoin de cette politique? Une brève déclaration sur l'objectif de cette politique, la raison pour laquelle elle est mise en place, et la façon dont elle est liée à la mission, à la vision et aux valeurs de Metrolinx.

PORTÉE ET APPLICATION

La présente norme s'applique à tous les employés de Metrolinx qui ont accès au SGPN, y compris les employés à temps plein, les employés à temps partiel, les employés probatoires et les employés occupant un emploi à durée déterminée qui utilisent le SGPN pour soutenir les opérations des Services de protection des consommateurs (SPC).

Le SGPN doit être utilisé pour stocker, organiser et, le cas échéant, échanger en toute sécurité les preuves numériques découlant d'un incident de sécurité, d'une question visée par une enquête ou d'une mesure d'application de la loi, conformément à la présente norme et au Guide de la procédure du SGPN.

EXIGENCES EN MATIÈRE DE FONCTIONNALITÉ DU SYSTÈME DE GESTION DES PREUVES NUMÉRIQUES (SGPN)

Les exigences fonctionnelles pour le SGPN doivent appuyer la collecte efficace, légale et en toute sécurité des preuves numériques, ainsi que le stockage, la gestion et la diffusion de

preuves numériques tout au long du processus de collecte de preuves. Le système doit faciliter l'ingestion sans heurte de divers formats de preuves numériques, y compris l'audio, la vidéo, les photographies et les documents provenant de multiples sources telles que les caméras corporelles, les caméras-témoins de circulation à l'intérieur du véhicule, les drones, le système de TVCF, les appareils mobiles et les quais tiers. Il devrait assurer un suivi de la chaîne de possession à l'aide de journaux d'audit détaillés afin d'assurer l'intégrité et l'admissibilité des éléments de preuve devant le tribunal, en conformité avec les règlements juridiques et sur la protection de la vie privée de l'Ontario, y compris la *Loi sur l'accès à l'information et la protection de la vie privée* (*LAIPVP*) et les normes applicables du ministère du Solliciteur général. Des contrôles d'accès fondés sur les rôles doivent être mis en œuvre pour restreindre l'accès aux données en fonction des autorisations d'utilisateur et le système doit prendre en charge l'échange en toute sécurité avec les procureurs, les avocats de la défense et d'autres intervenants autorisés.

De plus, le SGPN s'intégrera, dans la mesure du possible sur le plan technique, aux systèmes existants d'application de la loi et de justice, prendra en charge les capacités de pointe en matière de recherche et de balisage et il offrira des fonctionnalités de gestion du cycle de vie des preuves, y compris les calendriers de conservation et l'élimination en toute sécurité, le cas échéant.

EXIGENCES EN MATIÈRE DE NON-FONCTIONNALITÉ DU SYSTÈME DE GESTION DES PREUVES NUMÉRIQUES (SGPN)

Les exigences non fonctionnelles pour le SGPN sont axées sur le soutien de la fiabilité, de la sécurité, de l'évolutivité et de la conformité du système avec les normes fédérales et provinciales. Le système doit présenter une disponibilité élevée pour appuyer un accès 24 heures sur 24, 7 jours sur 7 pour les employés des SPC et le personnel judiciaire. La sécurité est primordiale; ainsi, le SGPN doit intégrer de solides protocoles de chiffrement pour la protection des données, appliquer des contrôles d'accès stricts et l'authentification multifacteur, dans la mesure du possible sur le plan technologique, ainsi que des systèmes de détection d'intrusion, en conformité avec les lignes directrices fédérales et provinciales pertinentes. Le quai doit être évolutif pour répondre aux volumes croissants de preuves numériques sans dégradation du rendement et doit prendre en charge l'accès simultané par plusieurs utilisateurs.

L'utilisabilité est également essentielle, car l'interface du SGPN doit être intuitive et réactive, tout en assurant l'accessibilité conformément à la *Loi sur l'accessibilité pour les personnes handicapées de l'Ontario* (*LAPHO*).
Le système doit prendre en charge la reprise après sinistre et les mesures de redondance des données, y compris les sauvegardes, les objectifs de temps de récupération et les objectifs de récupération qui respectent les normes de Metrolinx telles qu'elles sont décrites dans la politique de sécurité de l'information de Metrolinx. De plus, le SGPN devrait faire l'objet d'audits réguliers du rendement, de sécurité et de conformité afin de s'assurer qu'il continue de répondre aux exigences légales, technologiques et opérationnelles de Metrolinx en constante évolution.

NORMES DE SÉCURITÉ DU SYSTÈME DE GESTION DES PREUVES NUMÉRIQUES (SGPN)

Les normes de sécurité pour le SGPN doivent être conformes aux lignes directrices provinciales et fédérales afin de soutenir la protection, la confidentialité et l'intégrité des renseignements de nature délicate. Toutes les données doivent être protégées à l'aide de protocoles de chiffrement de pointe qui sont continuellement surveillés par l'unité commerciale Innovation et Technologie de l'information (I et TI) de Metrolinx. Le système mettra en œuvre des mesures robustes de gestion de l'identité et de l'accès, y compris l'authentification multifacteur (AMF), les contrôles d'accès fondés sur les rôles et des processus stricts d'autorisations ou de résiliations d'accès des utilisateurs. L'enregistrement des audits doit être inviolable, complet et régulièrement examiné afin de soutenir la responsabilité et d'appuyer les enquêtes.

Afin de se protéger contre les violations des données et l'accès non autorisé, le SGPN doit inclure des systèmes intégrés de détection et de prévention des intrusions, qui sont en outre appuyés par des évaluations régulières de la vulnérabilité et des essais de pénétration tels qu'ils sont définis dans la politique de sécurité de l'information de Metrolinx.
De plus, le SGPN doit être conforme à la *Loi sur l'accès à l'information et la protection de la vie privée (LAIPVP)*, ainsi qu'aux parties pertinentes du *Code criminel* du Canada et de la *Charte canadienne des droits et libertés* concernant l'accès légal, la vie privée et la divulgation des preuves numériques, ainsi qu'aux politiques internes de Metrolinx telles que la politique de sécurité de l'information et la politique de gouvernance et de gestion des données d'entreprise de Metrolinx.

GESTION DES DONNÉES

La gestion des données pour le SGPN doit appuyer le traitement précis, sécurisé et efficace des preuves numériques tout au long de leur cycle de vie, de la collecte à l'élimination finale. Le système doit prendre en charge l'ingestion de divers types de fichiers, y compris la vidéo, l'audio, les documents et les images, tout en préservant les métadonnées telles que les horodatages, les identifiants d'appareil et les renseignements sources afin d'assurer la valeur probante. Toutes les données seront classifiées, indexées et stockées de manière à permettre des capacités de récupération et de recherche efficaces, en appuyant des filtres tels que le numéro de cas, le type d'incident, le nom de l'agent autorisé et la période. Le SGPN doit appliquer des contrôles stricts de la chaîne de possession, enregistrant automatiquement toutes les mesures prises par les utilisateurs, y compris les téléchargements, les consultations, les modifications, les transferts et les éliminations, dans des pistes d'audit inviolables.

La conservation des données doit respecter le calendrier de conservation des documents de Metrolinx. Le système prendra également en charge le contrôle des versions, le balisage des preuves et la liaison de plusieurs éléments de preuve à un seul dossier. L'interopérabilité avec d'autres systèmes de justice et d'application de la loi, dans la mesure du possible sur le plan technique, est essentielle pour faciliter un flux de données sans heurts. De plus, le SGPN doit prendre en charge des mécanismes de sauvegarde et de récupération en cas de sinistre robustes, assurant la résilience et la disponibilité des données en cas de pannes du

système ou d'incidents de sécurité conformément aux exigences énoncées dans le contrat conclu avec le fournisseur du SGPN.

CONSIDÉRATIONS LIÉES À LA PROTECTION DE LA VIE PRIVÉE

Les considérations liées à la protection de la vie privée pour le SGPN sont primordiales, compte tenu de la nature délicate et souvent personnelle des preuves numériques qu'il traite. Le système doit se conformer à la *Loi sur l'accès à l'information et la protection de la vie privée* (*LAIPVP*), en veillant à ce que la collecte, l'utilisation, la divulgation et la conservation des renseignements personnels soient légales, nécessaires et proportionnées. Les principes de conception en matière de protection de la vie privée, tels qu'approuvés par le Commissaire à l'information et à la protection de la vie privée (CIPVP) de l'Ontario, doivent être intégrés à l'architecture du système dès le départ. Cela inclut la minimisation des données, les paramètres de confidentialité par défaut, les limitations d'accès des utilisateurs et le chiffrement de bout en bout.

L'accès aux preuves numériques doit être strictement fondé sur les rôles, avec des pistes d'audit qui saisissent toutes les interactions des utilisateurs pour appuyer la responsabilité et la transparence. Des fonctionnalités telles que le flou du visage et d'autres outils de caviardage doivent être utilisés pour protéger l'identité des personnes qui ne participent pas directement aux les enquêtes ou aux poursuites. Le SGPN doit également fournir des mécanismes pour appuyer les droits des personnes d'accéder à leurs renseignements personnels ou de demander des corrections en vertu de *LAIPVP*, tout en assurant l'intégrité de la preuve pour les procédures judiciaires. Des évaluations des facteurs relatifs à la vie privée (EFVP) régulière doivent être effectuées pour évaluer et atténuer les risques liés à la protection de la vie privée à mesure que le système évolue ou étend sa fonctionnalité.

EXAMEN ET UTILISATION DES DOCUMENTS DU SYSTÈME DE GESTION DES PREUVES NUMÉRIQUES (SGPN)

L'examen et l'utilisation de documents stockés dans le SGPN doivent appuyer la manipulation sécurisée, efficace et conforme à la loi des documents numériques et respecter les lois fédérales et provinciales en matière d'échange de renseignements. Les utilisateurs autorisés, tels que les agents autorisés, les enquêteurs des SPC, l'équipe de la Section des opérations criminelles (SOC) des SPC, les organismes d'application de la loi et les procureurs doivent pouvoir accéder et examiner en toute sécurité les preuves numériques au sein du système en utilisant un modèle d'accès fondé sur les rôles qui appuient le principe selon lequel seulement le personnel pertinent peut consulter ou modifier des fichiers particuliers. Le SGPN offre des outils pour un examen détaillé, y compris la lecture vidéo avec analyse image par image, des options d'amélioration audio, l'annotation de documents et l'inspection des métadonnées. Les renseignements dans le SGPN doivent être facilement interrogeables par des champs clés tels que le numéro de dossier, la date, le type de dossier ou les parties concernées, permettant une récupération efficace au cours des enquêtes ou de la préparation d'un tribunal. Les procureurs doivent être en mesure de compiler les dossiers de divulgation directement dans le système et de les partager en toute sécurité avec un avocat de la défense, le cas échéant. Le SGPN doit également prendre en charge la présentation de

preuves au tribunal, avec des options d'exportation qui préservent la chaîne de possession et l'intégrité des dossiers numériques. Les journaux d'audit détaillés suivront chaque accès, consultation, commentaire ou modification, appuyant un historique d'examen transparent qui peut être vérifié, en cas de contestation devant un tribunal. De plus, toute utilisation de renseignements personnels et de nature délicate doit être conforme aux politiques de Metrolinx, aux lois en matière de protection de la vie privée et aux directives judiciaires, telles que le caviardage de données personnelles de tiers non essentielles à l'affaire.

PUBLICATION DES DOCUMENTS DU SGPN

L'accès du public aux renseignements dans le SGPN doit respecter les lois provinciales et fédérales en matière de protection de la vie privée. Même si le public ne peut généralement pas avoir accès directement aux preuves numériques, l'accès peut être accordé au moyen d'une demande officielle d'accès à l'information (AI) régie par la *LAIPVP*. Le SGPN doit prendre en charge ces demandes à l'aide de fonctionnalités telles que le caviardage, la suppression des métadonnées et des liens d'affichage sécurisés et limités dans le temps. Lorsque des éléments de preuve sont présentés en audience publique, ils peuvent devenir un document public et le SGPN doit donc permettre une extraction et un échange légaux tout en protégeant les renseignements de nature délicate, tels que l'identité des victimes, des mineurs, des personnes vulnérables ou des tiers.

Le système doit également enregistrer tous les événements d'accès, en tenant à jour un registre complet des personnes qui ont accédé à quels renseignements, quand et en vertu de quelle autorisation. Ces événements d'accès feront l'objet d'un audit afin de vérifier que seuls les membres du personnel autorisé a eu accès aux documents dans le but d'exercer leurs fonctions. Les principes de confidentialité dès la conception doivent être respectés lors de toute utilisation publique des preuves et les administrateurs du système doivent disposer d'outils de supervision pour examiner et approuver toutes les divulgations publiques d'une manière qui ne compromet pas l'intégrité juridique, les droits à la vie privée ou les enquêtes en cours.

ÉLIMINATION DES DOCUMENTS STOCKÉS DANS LE SYSTÈME DE GESTION DES PREUVES NUMÉRIQUES (SGPN)

L'élimination des documents provenant de SGPN doit être régie par des contrôles juridiques, procéduraux et technologiques stricts afin d'assurer le respect des exigences en matière de preuve, de protection de la vie privée et de gestion des documents. Les processus d'élimination doivent être conformes à la politique de gestion des dossiers et de l'information (GDI) de Metrolinx, au processus d'élimination, aux lois applicables, y compris la *Loi sur les archives et la conservation des documents*, ainsi qu'au calendrier de conservation des documents de Metrolinx.
Les preuves ne doivent pas être supprimées de manière arbitraire ou prématurée, surtout si elles peuvent faire l'objet d'enquêtes en cours, de procédures judiciaires et/ou d'obligations de divulgation. Toutes les preuves saisies dans le SGPN seront conservées et supprimées conformément au calendrier de conservation des documents de Metrolinx.

Les autorisations dans le SGPN doivent permettre uniquement aux membres du personnel autorisés, généralement aux gardiens de preuves ou aux administrateurs du système, d'amorcer l'élimination, et ce, uniquement après avoir confirmé que les critères juridiques et opérationnels de conservation ont été satisfaits. Toute élimination des données doit être conforme à la série de documents appropriée dans le calendrier de conservation des documents de Metrolinx. Avant l'élimination, le système déclenchera un examen des flux de travail et exigera plusieurs niveaux d'approbation afin de prévenir la perte accidentelle ou non autorisée de données. Toutes les mesures d'élimination doivent être consignées dans des pistes d'audit inviolables, consignant qui a lancé l'élimination, quand elle a eu lieu, la justification, et les fichiers touchés. Dans les cas concernant des plaintes publiques, des litiges civils ou des enquêtes internes, le SGPN doit également prendre en charge les mesures de conservation légales afin d'empêcher l'élimination automatique ou prévue. Lorsque des preuves sont légalement supprimées, le système doit assurer un effacement complet et sécurisé des données à la fois des environnements de stockage principaux et de sauvegarde afin de respecter les normes de confidentialité et de protection des données. En général, l'élimination doit être gérée comme un processus étroitement contrôlé qui établit un équilibre entre la nécessité d'une gestion responsable du cycle de vie des données et l'obligation légale de préserver et de protéger les preuves numériques.

EXIGENCES EN MATIÈRE DE FORMATION

Le succès de la mise en œuvre du SGPN nécessite une formation exhaustive afin de s'assurer que tous les agents autorisés, ainsi que les gestionnaires, les enquêteurs et le personnel administratif concernés comprennent les responsabilités opérationnelles, juridiques et éthiques de l'utilisation du SGPN.

La formation en personne est obligatoire pour tous les membres du personnel qui utilisent le SGPN et ses données connexes. Cela comprend des instructions détaillées sur les aspects techniques du SGPN et sera appuyé par le Guide de la procédure du SGPN.

La formation de recyclage doit être offerte régulièrement afin de renforcer les politiques, les normes, les procédures et de s'adapter aux modifications législatives, à la technologie ou aux exigences opérationnelles. Toute formation mettra l'accent sur les responsabilités éthiques d'utiliser le SGPN, en se concentrant sur la sécurité, l'intégrité des données, la transparence, le professionnalisme et le maintien de la confiance du public.

EXIGENCES LÉGALES ET DE CONFORMITÉ

Les exigences légales et de conformité pour le SGPN sont essentielles pour s'assurer que les preuves numériques sont traitées d'une manière qui respecte la primauté du droit, les droits à la protection de la vie privée des personnes et qui assure l'intégrité des preuves pour une utilisation dans les procédures judiciaires. Le SGPN doit se conformer à la *Loi sur l'accès à l'information et la protection de la vie privée* (*LAIPVP*) qui régit la collecte, l'utilisation, la conservation et la divulgation des renseignements personnels par les organismes publics. Il doit également être conforme au *Code criminel* du Canada et à la *Charte canadienne des droits et libertés*, plus particulièrement en ce qui concerne les fouilles, les perquisitions et les saisies légales, les obligations de divulgation et le droit à un procès équitable et impartial. Le

système doit prendre en charge les documents appropriés et l'application des procédures de la chaîne de possession afin de préserver l'admissibilité des preuves au tribunal.

La conservation et l'élimination des données doivent respecter le calendrier de conservation des documents de Metrolinx, la politique de gestion des dossiers et de l'information (GDI) de Metrolinx, et seront effectuées en toute sécurité, conformément au niveau de sensibilité des renseignements. De plus, le SGPN fournira des outils pour gérer les obligations de divulgation, en veillant à ce que les preuves pertinentes soient communiquées à l'avocat de la défense en temps opportun et en toute sécurité.

Le système doit faire l'objet d'audits réguliers pour démontrer sa conformité aux lois, aux règlements et aux politiques de Metrolinx applicables, telles que la politique de sécurité de l'information de Metrolinx et pour soutenir son adaptabilité aux modifications législatives ou politiques futures touchant la gestion des preuves numériques en Ontario.

CONFORMITÉ ET RESPONSABILISATION

La conformité et la responsabilisation pour le SGPN sont essentielles pour respecter les exigences légales, protéger les droits des personnes et maintenir la confiance du public envers Metrolinx. Afin d'assurer une conformité continue, le système doit intégrer des capacités robustes d'audit et de surveillance, y compris des journaux immuables de toutes les activités des utilisateurs, telles que les téléversements, les téléchargements, les consultations, les modifications, les éliminations et les divulgations, qui peuvent être examinés au cours d'audits internes, de procédures judiciaires ou d'enquêtes sur les contrôles de conformité. Des évaluations des facteurs relatifs à la vie privée (EFVP) et des évaluations de la menace et des risques (EMR) doivent être effectuées pour évaluer le respect du système des normes législatives et politiques, plus particulièrement lorsque des mises à jour ou de nouvelles intégrations sont mises en œuvre en temps opportun. De plus, les programmes de formation et d'éducation sont obligatoires pour tous les utilisateurs afin de s'assurer qu'ils comprennent leurs responsabilités légales et les conséquences possibles d'une mauvaise utilisation, telles qu'une mesure disciplinaire, la responsabilité civile ou les poursuites pénales. Les administrateurs du système ont le pouvoir et les outils nécessaires pour faire respecter la conformité, enquêter sur les irrégularités et veiller à ce que les preuves numériques soient gérées avec intégrité, transparence et de manière responsable en tout temps.

ADMINISTRATION ET ENTRETIEN DES SYSTÈMES

L'administration et l'entretien des systèmes pour le SGPN doivent être conçus de manière à prendre en charge une opération de système continue, sécurisée et efficace, en conformité avec les contrôles de cybersécurité de Metrolinx et les normes de gouvernance provinciales et fédérales applicables. Cela comprend la mise en œuvre d'une gestion appropriée des accès, du chiffrage, de l'enregistrement et des pratiques de surveillance pour protéger les données de nature délicate et assurer l'intégrité du système

Les fonctions administratives doivent inclure une gestion exhaustive des utilisateurs et des accès, permettant aux administrateurs du système d'attribuer, de modifier et de révoquer l'accès en fonction des rôles et des responsabilités clairement définis, conformément au

principe du moindre privilège. Les administrateurs sont également chargés de la gestion des configurations du système et des configurations de sécurité, de la surveillance de la capacité de stockage et de la santé du système, ainsi que du soutien au rendement optimal du système à mesure que le nombre de preuves augmente. Ces activités doivent être conformes aux politiques et aux normes de cybersécurité de Metrolinx, y compris la configuration en toute sécurité, l'application du contrôle d'accès et la surveillance continue afin d'assurer l'intégrité, la sécurité et la protection des données du système.

L'entretien régulier du système, tel que la correction de logiciels, la remédiation de la vulnérabilité, l'optimisation des bases de données et les examens des journaux de systèmes, doit suivre un protocole consigné de gestion du changement, conformément à la procédure de gestion des changements informatiques de Metrolinx. Les activités d'entretien devraient être planifiées afin de réduire au minimum les perturbations opérationnelles et d'assurer l'harmonisation avec les politiques et les normes de cybersécurité de Metrolinx

Les administrateurs du système auront accès à des outils de surveillance de pointe qui fournissent des alertes en temps réel pour les défaillances du système, les tentatives d'accès non autorisées ou les modèles d'utilisation anormale. Toutes les mesures administratives doivent être entièrement consignées et vérifiables afin de faciliter la surveillance interne et externe de la conformité. Afin d'assurer l'harmonisation avec l'évolution des mandats législatifs et des normes organisationnelles, le SGPN doit faire l'objet d'évaluations régulières de sécurité. Ces évaluations comprennent les évaluations de la menace et des risques (ERM), les essais de pénétration et les évaluations de la compatibilité.

De plus, une documentation exhaustive, des programmes de formation continus et des mécanismes de soutien solides doivent être mis en place pour que les administrateurs soient bien préparés à gérer le quai de manière efficace et à répondre rapidement aux défis techniques émergents ou aux mises à jour réglementaires.

RÔLES ET RESPONSABILITÉS

Vice-président des SPC

Le vice-président des SPC est responsable des éléments suivants :

- Assurer une surveillance et soutenir l'application cohérente de la présente norme.

Directeur des SPC, Normes professionnelles

Le directeur des SPC, Normes professionnelles, est responsable des éléments suivants :

- Soutenir la mise en œuvre et la conformité avec la présente norme et toutes les procédures connexes.
- Communiquer et mettre en œuvre le norme et le Guide de la procédure connexe auprès des employés concernés de Metrolinx.
- Gestion et signalement des problèmes de non-conformité liés à l'utilisation du SGPN.

Agents autorisés

Les agents autorisés (agents de protection des clients, agents de protection des revenus et ambassadeurs de la sécurité en gare) sont responsables des éléments suivants :

- **Utilisation appropriée** : Exploiter le SGPN conformément aux protocoles et aux autorisations établis en fonction du rôle respectif et des tâches respectives de l'agent autorisé.
- **Gestion des preuves numériques** : Télécharger des photographies numériques, des enregistrements audio et des enregistrements vidéo de manière rapide et précise conformément aux procédures de gestion des données des SPC de Metrolinx.
- **Intégrité des données** : Assurer l'intégrité des preuves numériques en suivant les procédures appropriées de manipulation et en veillant à ce que les photographies numériques, les enregistrements audio et les enregistrements vidéo ne soient pas modifiés, supprimés ou mal manipulés.

Gestionnaires des SPC

Les gestionnaires des SPC sont responsables des éléments suivants :

- Surveiller la conformité des APC, des APR et des ASG aux procédures du SGPN, telles qu'elles sont indiquées dans le Guide de la procédure du SGPN.

Enquêtes des SPC

L'équipe des enquêtes est responsable des éléments suivants :

- La coordination et la collecte des preuves numériques demandées par les organismes d'application de la loi et le soutien à la conformité avec les lignes directrices juridiques, réglementaires et procédurales relatives au traitement des preuves.
- **Gestion des preuves numériques** : Télécharger des photographies numériques, des enregistrements audio et des enregistrements vidéo dans le SGPN de manière rapide et précise conformément aux directives de gestion des données des SPC.
- **Intégrité des données** : Assurer l'intégrité des preuves numériques en suivant les procédures appropriées de manipulation et en veillant à ce que les photographies numériques, les enregistrements audio et les enregistrements vidéo ne soient pas modifiés, supprimés ou mal manipulés.

Équipe des données et d'analyse des SPC

L'équipe des données et d'analyse des SPC est responsable des éléments suivants :

- Rendre compte du rendement du programme et des statistiques (génération de rapports).
- Approuver des autorisations pour les utilisateurs du SGPN en fonction d'une matrice de contrôle d'accès fondée sur les rôles.

Équipe informatique de Metrolinx

L'équipe informatique de Metrolinx est responsable des éléments suivants :

- Aider à l'installation technique, au déploiement, à la gestion des données et aux exigences de cybersécurité et de conformité pour le programme de preuves numériques.
- Gérer les autorisations et les comptes des utilisateurs tout en assurant l'intégrité du système et les logiciels.
- Assurer la liaison avec le fournisseur de services du SGPN afin d'offrir un soutien technique pour le quai du SGPN.

Formation et perfectionnement des SPC

L'équipe de formation et de perfectionnement des SPC est responsable des éléments suivants :

- Élaborer et mettre en œuvre un programme de formation rigoureux qui appuie les employés des SPC afin qu'ils suivent une formation appropriée pour avoir accès au SGPN et pour l'utiliser et comprendre les responsabilités de chaque rôle en matière d'accès, de contrôle et de protection des preuves numériques.

Équipe de risque et d'audit des SPC

L'équipe de risque et d'audit des SPC est responsable des éléments suivants :

- Effectuer des vérifications de routine conformément à la Norme du programme de vérification.
- Élaborer des recommandations pour remédier à la non-conformité.
- Appuyer l'élaboration de plans d'action corrective (PAC) qui permettront de veiller à ce que les problèmes de non-conformité soient pleinement réglés.
- Effectuer des audits de suivi pour s'assurer que le programme du SGPN respecte les politiques de Metrolinx, les règlements, les normes et les lignes directrices du CIPVP en matière de protection de la vie privée.

ESCALADES ET EXCEPTIONS

Toutes les exceptions ou cas de non-conformité à la présente norme doivent être signalés au directeur des normes professionnelles. Le non-respect de la présente norme ou des outils de travail connexes peut entraîner des mesures disciplinaires, pouvant aller jusqu'au congédiement.

RÉFÉRENCES

Loi sur les archives et la conservation des documents
Norme du programme de vérification
Politique audiovisuelle et vidéo (MCS-0202-01)
Guide de la procédure sur les caméras corporelles (MCS-0202-02P) Norme sur la télévision en circuit fermé (MCS-0202-05)
Guide de la procédure de télévision en circuit fermé (MCS-0202-05P) *Loi sur la protection des cybersystèmes essentiels* (*LPCE*)
Guide de la procédure du système de gestion des preuves numériques (SGPN) (MCS-0202-06P) Norme d'exploitation et d'entretien des drones (MCS-0202-04)
Guide de la procédure d'exploitation et d'entretien des drones (MCS-0202-04P)
Loi sur l'accès à l'information et la protection de la vie privée Guide de la procédure d'échange de renseignements (MCS-0202-08P) Norme d'échange de renseignements (MCS-0202-08) Politique de sécurité de l'information (CA-0504-02)
Cadre de gouvernance du modèle du CIPVP pour les programmes de caméras corporelles en Ontario Procédure de gestion des changements informatiques (CA-0502-12P)
Politique de gouvernance et de gestion des données d'entreprise de Metrolinx (CA-0701-01) Politique sur la protection de la vie privée de Metrolinx (CA-0901-01)
Processus d'élimination de documents de Metrolinx (CA-0402-06P) Calendrier de conservation des documents de Metrolinx
Politique de gestion des documents et de l'information (GDI) (CA-0402-01)

ADMINISTRATION

Nom d'identification	Norme sur le Système de gestion des preuves numériques (SGPN)
Approuvé par	Chef de l'exploitation
Propriétaire	Vice-président, Services de protection des clients
Témoin	Directeur, Normes professionnelles des services de protection des clients
Date d'approbation initiale	
Fréquence de révision	Annuellement
Remplace	S.O.

HISTORIQUE DE LA NORME

Date de révision et d'examen	Auteur	Description
Le 10 décembre 2025	Services de protection des clients, normes professionnelles	Nouvelle norme

DÉFINITIONS

Accidentel : Un événement qui se produit involontairement ou de manière inattendue.

Caméra corporelle (CC) : Un appareil porté par un agent dans le but d'enregistrer des renseignements vidéo et audio.

Chaîne de possession : L'historique chronologique consigné de la preuve, suivant méticuleusement sa possession, son contrôle, son transfert, son analyse et son élimination depuis le moment de la collecte jusqu'à sa présentation dans le cadre de procédures judiciaires.

Système de télévision en circuit fermé (TVCF) : Un système qui utilise des caméras vidéo pour transmettre un signal à un ensemble particulier de moniteurs ou d'appareils d'enregistrement, plutôt que de le diffuser ouvertement.

Plans d'action corrective (PAC) : Approche détaillée et structurée qui décrit les étapes qu'une organisation suivra pour traiter et régler les problèmes cernés au cours d'un audit ou d'un autre processus d'évaluation.

Agent de protection de la clientèle (APC) : Une personne employée par Metrolinx qui a été nommée par le commissaire de la Police provinciale de l'Ontario, et approuvée par le Solliciteur général, à titre de « constable spécial », conformément à l'article 92 de la *Loi de 2019 sur la sécurité communautaire et les services policiers*, avec les pouvoirs et fonctions énoncés dans la nomination.

Preuve numérique : Comprend, sans toutefois s'y limiter, des photographies, des enregistrements audio et des enregistrements vidéo numériques saisis par les membres du personnel de Metrolinx en lien avec une enquête, le système Metrolinx ou une question liée à la sécurité.

Système de gestion des preuves numériques (SGPN) : Un système de gestion des preuves numériques infonuagique, qui offre un stockage, une organisation et un échange de preuves numériques en toute sécurité.

Gestionnaire : Un employé chargé de diriger, de superviser et de surveiller le travail des agents de protection des clients, des agents de protection des revenus et des ambassadeurs de la sécurité en gare.

Balisage des métadonnées : Le processus d'ajout de renseignements descriptifs aux fichiers numériques et à d'autres données pour les rendre plus faciles à trouver, à organiser et à gérer. Ces balises agissent comme des étiquettes qui fournissent un contexte et une signification sur les données, permettant aux utilisateurs et aux systèmes de mieux les comprendre et d'interagir avec elles.

Évaluation des facteurs relatifs à la vie privée (EFVP) : Un processus systématique pour déterminer, évaluer et atténuer les risques possibles associés à un projet, à un programme ou à un système concernant la collecte, l'utilisation ou la divulgation de renseignements personnels.

Caviardage : Un processus visant à dissimuler ou à supprimer des parties d'un document, telles que des renseignements personnels, avant la publication.

Agent de protection des revenus (APR) : Une personne employée par Metrolinx qui assume les responsabilités liées à l'exécution des interactions de non-conformité sur les tarifs de Metrolinx, conformément à la procédure d'escalade appropriée, interagit avec les passagers et aide à répondre aux questions liées aux tarifs ou aux questions générales.

Ambassadeur de la sécurité en gare (ASG) : Les employés de Metrolinx en uniforme qui sont chargés de détecter et de dissuader les troubles et de protéger la sûreté et la sécurité des clients et des employés dans toutes les propriétés de Metrolinx. Les ASG sont nommés en vertu du paragraphe 21(5) de la *Loi de 2006 sur le Metrolinx* en tant qu'agents des infractions provinciales afin d'appliquer et d'exécuter les règlements administratifs de Metrolinx.

Évaluation de la menace et des risques (EMR) : Un processus d'évaluation de la sécurité utilisé pour cerner, évaluer et atténuer les menaces liés à la cybersécurité et les risques associés aux déploiements technologiques. Elle appuie la conformité aux politiques de cybersécurité de Metrolinx, aux normes et de la technologie (NIST) et à l'ISO 27001 en analysant les menaces, les vulnérabilités et les répercussions possibles et en recommandant des contrôles de sécurité pour protéger les systèmes et les données de Metrolinx.

Personne(s) vulnérable(s) : Une personne considérée comme ayant besoin de soins particuliers en raison d'une : déficience cognitive, physique, intellectuelle ou développementale; nécessitant une protection contre elle-même ou autrui (par exemple, une

personne confrontée à des problèmes de santé mentale, à des tendances suicidaires, à la violence conjugale, à la traite de personne, etc.); ou toute autre condition/état pouvant la placer à un risque accru (par exemple, une personne perçue comme étant en situation d'insuffisance de logement/sans-abri, vivant dans la pauvreté, ayant des problèmes liés à la consommation de substances, etc.).