4.8.

PROTECTION DES RENSEIGNEMENTS PERSONNELS (SOCIÉTÉ DE TRANSPORT DE MONTRÉAL)

Le 20 avril 2018

SOMMAIRE DE L'AUDIT

OBJECTIF

Évaluer si les contrôles mis en place permettent d'assurer une sécurité logique et physique des renseignements personnels (RP) détenus par la Société de transport de Montréal (STM) afin d'en limiter les risques de perte de confidentialité, de vol ou d'accès non autorisé.

RÉSULTATS

Globalement, nous pouvons conclure que la STM protège adéquatement les RP amassés dans le cours de ses activités.

En effet, concernant les aspects de gouvernance :

- La STM dispose de politiques corporatives et de gestion adéquates, les responsabilités sont clairement établies et une reddition de comptes est en place;
- Les employés et les gestionnaires sont correctement sensibilisés à l'importance de la protection des RP;
- La STM possède un inventaire des RP répondant aux exigences de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (LAD).

Pour les aspects de conservation et de destruction des RP :

- Un calendrier de conservation a été établi pour les RP présents au sein de dossiers physiques et pour les nouveaux systèmes. Néanmoins, il n'y a pas de règles de conservation pour les cinq systèmes d'information examinés;
- La destruction des RP pour les dossiers physiques est effectuée par une firme externe de manière sécuritaire;
- Aucune destruction des RP n'est prévue pour trois des cinq systèmes d'information évalués.

Pour les mesures de protection :

- Quatre des cinq systèmes audités contiennent des RP réels ailleurs que dans leurs environnements de production;
- Malgré qu'un système présente des lacunes au niveau de la révision des accès, les autres systèmes examinés ont une gestion des accès logiques adéquate;
- Les accès physiques au local des dossiers médicaux sont protégés. Les deux locaux abritant les dossiers d'employés et de candidatures ainsi que les formulaires du transport adapté disposent de serrures à code qui sont moins sécuritaires que des lecteurs de cartes;
- La transmission électronique des RP aux autres organismes de transport est sécuritaire. Par contre, la transmission de dossiers de candidatures à une firme externe n'est pas confidentielle;
- Le processus de gestion des incidents inclut la protection des RP;
- Des tests d'intrusion sont réalisés régulièrement afin de mettre à l'épreuve les systèmes contenant des RP.

En marge de ces résultats, nous avons formulé différentes recommandations aux unités d'affaires de la STM.

Les détails de ces recommandations ainsi que notre conclusion sont décrits dans notre rapport d'audit présenté aux pages suivantes.

Soulignons que les unités d'affaires ont eu l'opportunité de formuler leurs commentaires, lesquels sont reproduits à la suite des recommandations de notre rapport d'audit.

TABLE DES MATIÈRES

LISTE DES SIGLES

ACCÈS
système de gestion des clients du transport adapté

CAI
Commission d'accès à l'information

E-Dotation
système de gestion des candidatures

LAD
Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels

NAS
numéro d'assurance sociale

RP
renseignements personnels

SAP
progiciel de gestion intégré pour, entre autres, les ressources humaines et la paie

SIGESST
système de gestion de la santé et sécurité au travail traitant également les congés de maladie

STM
Société de transport de Montréal

TI
technologies de l'information

VP
système de gestion pour la vente et la perception des cartes OPUS

1. CONTEXTE

De par ses activités, la Société de transport de Montréal (STM) collecte et traite beaucoup de renseignements afférents à la vie privée de ses clients et de ses employés. La STM dessert environ 2,9 millions de clients détenant une carte OPUS enregistrée, 30 000 clients qui utilisent le transport adapté et compte 9 700 employés. Ces renseignements sont nécessaires afin de les servir adéquatement. Les principales activités pour lesquelles la STM collecte des renseignements personnels (RP) sont :

- la constitution des dossiers d'employés et de leurs dossiers médicaux;
- la collecte des coordonnées bancaires des employés pour le traitement de la paie;
- les candidatures aux fins de recrutement;
- l'enregistrement de la carte OPUS (principalement pour les fins du tarif réduit);
- la collecte d'informations médicales pour les usagers du transport adapté.

Au Canada, la vie privée est un droit fondamental qui est protégé de façon globale par des législations tant fédérales que provinciales.

Adoptée le 27 juin 1975, la *Charte des droits et libertés de la personne* du Québec stipule, entre autres, que les libertés et les droits fondamentaux des citoyens sont :

- le droit à la sauvegarde de sa dignité, de son honneur et de sa réputation;
- le droit au respect de sa vie privée.

Le Québec a bâti, au cours des quatre dernières décennies, un modèle législatif incarné par la Commission d'accès à l'information (CAI) du Québec. Elle est chargée de l'application de deux législations :

- Pour le secteur public : *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[1] (LAD);
- Pour le secteur privé : *Loi sur la protection des renseignements personnels dans le secteur privé*[2].

En tant qu'organisme du secteur public, la STM est donc assujettie à la LAD. Cette loi énonce deux droits fondamentaux, soit celui du droit d'accès et celui du droit à la protection des RP.

La LAD s'applique à tous les documents, qu'ils soient sous forme écrite, graphique, sonore, visuelle, informatisée ou autre.

1 RLRQ, chapitre A-2.1.

2 RLRQ, chapitre P-39.1.

Un RP se définit comme[3] :

- tout renseignement qui identifie une personne physique (par opposition à une personne morale);
- un renseignement qui permet l'identification d'un individu (par opposition à des données rendues anonymes);
- un renseignement factuel ou subjectif sur une personne, peu importe sa forme ou son support.

Compte tenu de leur nature, certains RP sont confidentiels. Parmi ceux-ci, nous retrouvons :

- le numéro d'assurance sociale (NAS);
- le numéro d'assurance maladie;
- la date de naissance;
- les coordonnées bancaires;
- les renseignements médicaux;
- le curriculum vitae.

Il existe cependant des RP à caractère public qui ne sont pas confidentiels. En voici quelques exemples :

- Nom, titre, salaire, adresse et numéro de téléphone au travail d'un membre d'un organisme public ou de son conseil d'administration;
- Personnel de direction de la STM.

Toute perte, tout vol ou tout accès non autorisé à des RP confidentiels risquent, en plus d'enfreindre la loi :

- de permettre la divulgation de RP;
- de permettre à une personne malveillante d'usurper des identités;
- de porter atteinte à la sécurité des personnes, compte tenu de la sensibilité de certaines informations détenues;
- de porter atteinte à la réputation de l'organisme;
- d'entraîner une perte de confiance des usagers;
- d'entraîner des poursuites judiciaires.

Dans ce contexte, la STM doit impérativement protéger ses RP afin de diminuer les risques qu'un des événements énoncés ci-dessus survienne.

3 Basé sur le RLRQ, chapitre A-2.1, articles 1 et 54.

2. OBJECTIF DE L'AUDIT ET PORTÉE DES TRAVAUX

En vertu des dispositions de la *Loi sur les cités et villes*, nous avons réalisé une mission d'audit de l'optimisation des ressources portant sur la protection des renseignements personnels au sein de la STM. Nous avons réalisé cette mission conformément à la norme canadienne de mission de certification NCMC 3001, du Manuel de CPA Canada – Certification.

Le présent audit avait pour objectif d'évaluer la présence et l'efficacité des contrôles mis en place permettant d'assurer une sécurité logique et physique sur les RP détenus par la STM afin d'en limiter les risques de perte de confidentialité, de vol ou d'accès non autorisé.

La responsabilité du vérificateur général de la Ville de Montréal consiste à fournir une conclusion sur les objectifs de l'audit. Pour ce faire, nous avons recueilli les éléments probants suffisants et appropriés pour fonder notre conclusion et pour obtenir un niveau d'assurance raisonnable. Notre évaluation est basée sur les critères que nous avons jugés valables dans les circonstances. Ces derniers sont exposés en annexe.

Le vérificateur général de la Ville de Montréal applique la *Norme canadienne de contrôle qualité* (NCCQ 1), du Manuel de CPA Canada – Certification et, en conséquence, maintient un système de contrôle qualité exhaustif qui comprend des politiques et des procédures documentées en ce qui concerne la conformité aux règles de déontologie, aux normes professionnelles et aux exigences légales et réglementaires applicables. De plus, il se conforme aux règles sur l'indépendance et aux autres règles de déontologie du *Code de déontologie des comptables professionnels agréés*, lesquelles reposent sur les principes fondamentaux d'intégrité, de compétence professionnelle et de diligence, de confidentialité et de conduite professionnelle.

L'objet de notre audit a porté sur les RP contenus à l'intérieur des éléments suivants :

- Supports physiques :
  - Les dossiers médicaux des employés;
  - La dotation (les candidatures, les dossiers d'employés);
  - Le transport adapté (le formulaire de demande d'admission au transport adapté, qui inclut des données médicales des clients).
- Systèmes d'information :
  - Progiciel de gestion intégré pour, entre autres, les ressources humaines et la paie (SAP);
  - Système de gestion pour la vente et la perception des cartes OPUS, principalement pour les étudiants et les personnes de 65 ans et plus (VP);
  - Système de gestion des candidatures (E-Dotation);

- Système de gestion de la santé et sécurité au travail traitant également les congés de maladie (SIGESST);
- Système de gestion des clients du transport adapté (ACCÈS).

Nous avons exclu de notre mission les RP amassés dans le cadre d'émission de constats d'infractions de même que dans le cadre de la gestion des régimes de retraite, pour les raisons suivantes :

- Les organismes publics au sens de la LAD ne comprennent pas les tribunaux comme la cour municipale de la Ville de Montréal. Les constats d'infractions émis, selon les règlements 036 et 105 de la STM, sont saisis par des inspecteurs et d'autres employés de l'organisme. Ces constats sont ensuite envoyés vers le système de la cour municipale de la Ville de Montréal. Dans ce cadre, les constats d'infractions judiciaires sont accessibles sans restriction;

- Pour ce qui est des régimes de retraite, leur gestion se fait par un autre organisme que la STM;
- Nous avons également exclu de l'audit les aspects suivants :
  - Les accès logiques aux systèmes SAP et VP;
  - La sécurité physique des salles de serveurs;
  - Le processus de copies de sauvegarde.

Ces éléments sont examinés lors de l'audit des contrôles généraux des technologies de l'information (TI) dans le cadre des états financiers. Pour l'année financière 2017, il a été conclu qu'ils assuraient globalement un environnement de contrôle suffisamment robuste.

Bien que la STM doive se conformer aux lois et aux règlements en vigueur, cet audit ne constitue pas un exercice de conformité à la LAD ni aux autres lois ou normes auxquelles la STM se réfère pour élaborer son processus de protection des RP.

Notre audit a été réalisé de septembre 2017 à mars 2018. Il a consisté à effectuer des entrevues auprès du personnel, à examiner divers documents et à réaliser les sondages que nous avons jugés appropriés en vue d'obtenir l'information probante nécessaire.

À la fin de nos travaux, un projet de rapport d'audit a été présenté, aux fins de discussions, aux gestionnaires concernés au sein de chacune des unités d'affaires auditées. Par la suite, le rapport final a été transmis à la Direction générale de la STM, ainsi qu'à chacune des unités d'affaires concernées, pour l'obtention de plans d'action et d'échéanciers pour leur mise en œuvre. Une copie du rapport final a également été transmise, à titre informatif, au président du conseil d'administration.

3. RÉSULTATS DE L'AUDIT

3.1. GOUVERNANCE

3.1.A. CONTEXTE ET CONSTATATIONS

La gouvernance est formée d'encadrements et de principes de fonctionnement qui sont mis en place par une organisation afin de diffuser ses orientations stratégiques, mettre en place des règles de conduite et favoriser une transparence et une imputabilité dans l'organisation.

Notre premier critère d'audit était à l'effet que la STM devrait élaborer, documenter et communiquer des politiques et des procédures portant sur les RP de même qu'en assigner la responsabilité de leur respect.

La STM se doit également de respecter la LAD. Celle-ci précise, à l'intérieur de trois de ses articles liés aux RP, que :

- *un organisme public doit prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support* [art. 63.1];

- *nul ne peut, au nom d'un organisme public, recueillir un renseignement personnel si cela n'est pas nécessaire à l'exercice des attributions de cet organisme ou à la mise en œuvre d'un programme dont il a la gestion* [art. 64];

- *un organisme public doit établir et maintenir à jour un inventaire de ses fichiers de renseignements personnels* [art. 76].

Pour s'y conformer, la STM a édicté plusieurs encadrements lui permettant de définir certains paramètres de la gestion des RP dans l'organisation.

3.1.1. POLITIQUES

3.1.1.A. CONTEXTE ET CONSTATATIONS

Les encadrements sont des documents qui permettent de déterminer la portée, les exigences de même que les rôles et les responsabilités des diverses unités d'affaires en regard de certains sujets. Ces documents prennent la forme de politiques corporatives et de politiques de gestion dans le cas de la STM.

Au cours de nos travaux d'audit, la STM nous a fourni les politiques pertinentes à la protection des RP, soit une politique corporative et deux politiques de gestion.

La politique corporative intitulée « Sécurité informatique et protection de l'information » établit la position de la STM ainsi que ses orientations stratégiques en matière de sécurité informatique et de protection de l'information. Cette politique, approuvée par le conseil d'administration, définit le cadre général permettant d'assurer une gestion efficace et efficiente des risques liés à la sécurité des systèmes d'information et de traitement des données.

Les principes directeurs contenus dans cette politique voulant que :

- les ressources informatiques et informationnelles soient administrées en accordant une priorité à la sécurité et à la protection de celles-ci;

- l'accès physique et logique au patrimoine informatique et informationnel soit contrôlé de manière à prévenir et à contrer efficacement les intrusions ainsi que l'utilisation non autorisée des équipements, des systèmes et des données constituant ce patrimoine;

- l'accès, la conservation, la communication et la destruction des fichiers et des documents se fassent dans le respect des règles d'éthique de la STM de même que conformément aux lois auxquelles elle est assujettie.

En ce qui concerne les politiques de gestion, soit celle ayant pour titre « Protection de la confidentialité des renseignements personnels » et celle intitulée « Utilisation du patrimoine informatique », elles visent la gestion de l'information et sont approuvées par le directeur général.

La première politique de gestion a pour objet de définir le cadre de gestion qui assure un contrôle efficace des activités entourant les RP. Elle édicte donc les principes de base notamment en matière d'accès, de conservation et de destruction des RP de même qu'en matière de communication à des tiers.

La seconde politique, portant sur l'utilisation du patrimoine informatique, vise à garantir une exploitation efficace, optimale et sécuritaire des équipements et réseaux informatiques de la STM, tout en assurant le respect des individus et la protection des RP qu'elle détient. Elle contient donc des règles et des mesures administratives sur la conservation des informations, sur les méthodes d'accès, sur la communication de l'information de même que sur l'utilisation de l'information et des droits d'accès. Elle définit même des comportements illégaux et inacceptables.

L'examen de ces encadrements nous permet de conclure que ceux-ci sont adéquats. La politique corporative a été émise en 2002 et fait présentement l'objet d'une mise à jour. Les politiques de gestion découlant de cette politique corporative seront abordées et modifiées ultérieurement. Aucune recommandation n'est nécessaire.

3.1.2. PROGRAMME DE SENSIBILISATION

3.1.2.A. CONTEXTE ET CONSTATATIONS

Chacun des employés est une partie prenante au processus de protection des RP. Ainsi, il est essentiel que les encadrements de la STM portant sur la protection des RP, de même que leurs modifications subséquentes soient diffusés auprès de ceux-ci. Au même titre, des mesures particulières de sensibilisation portant sur la vie privée, la confidentialité et la protection des RP doivent être diffusées auprès des employés. Ces mesures doivent aussi être documentées. En outre, la diffusion régulière de telles mesures augmente le niveau de vigilance des individus.

Nous avons analysé le document portant sur une session d'information intitulée « Accès à l'information et protection des renseignements personnels ». Les principaux sujets traités durant cette session étaient :

- la portée de la LAD;
- l'accès aux documents des organismes publics;
- la protection des renseignements personnels;
- l'accès aux renseignements personnels;
- les procédures d'accès à l'information et aux renseignements personnels;
- le rôle de la Commission d'accès à l'information;
- les sanctions.

Cette formation est donnée au moins deux fois par année. Depuis 2013, elle a eu lieu à 19 reprises avec la participation de 177 personnes. Elle est dispensée aux employés ayant les fonctions suivantes : cadres, gestionnaires, chefs de bureau, conseillers, détenteurs de RP, adjointes administratives, employés des renseignements et service à la clientèle.

Une formation intitulée « Ce qu'un gestionnaire d'exploitation devrait savoir au plan légal » est également offerte aux gestionnaires. Celle-ci présente une vue d'ensemble des lois et des règlements qui touchent les activités opérationnelles de la STM. Cette formation inclut un volet sur les concepts d'accès à l'information aux documents détenus par la STM.

De plus, les nouveaux employés doivent signer un document indiquant qu'ils ont pris connaissance de la politique de « Gestion sur l'utilisation du patrimoine informatique » et qu'ils s'engagent à la respecter.

Finalement, afin d'augmenter la vigilance des employés en regard des RP, certaines initiatives ont été instaurées, comme :

- la présentation du code de conduite de la STM aux nouveaux employés de la Division Planification et acquisition de talents lors de leur embauche;
- avant d'entrer dans le réseau corporatif de la STM, un avertissement rappelle à chacun des utilisateurs qu'il doit respecter les consignes de la politique de gestion « Utilisation du patrimoine informatique ».

L'examen des diverses mesures mises en place nous permet de conclure que celles-ci sont adéquates pour sensibiliser les employés et les gestionnaires relativement aux questions liées à la protection des RP. Aucune recommandation n'est nécessaire.

3.1.3. ATTRIBUTION DES RESPONSABILITÉS

3.1.3.A. CONTEXTE ET CONSTATATIONS

À la STM, la responsabilité et la reddition de comptes en regard des RP sont formellement assignées à une entité ou à un service à l'intérieur de la politique corporative « Sécurité de l'information et protection de l'information ». L'entité responsable doit développer, documenter et mettre en œuvre les mesures et les suivis nécessaires lui permettant de démontrer le respect des exigences de cet encadrement. L'entité désignée doit avoir la plus haute autorité.

Lors de nos travaux d'audit, nous avons constaté que la responsabilité a été adéquatement attribuée à la Direction exécutive – Technologies de l'information et innovation et au Secrétariat corporatif et direction affaires juridiques. Ces responsabilités ont été déléguées au secrétaire corporatif (Secrétariat corporatif et direction affaires juridiques) et au chef de division, Risques, sécurité et conformité (TI et innovation). Ces personnes travaillent en collaboration afin d'assurer la mise en application de la politique.

Les deux principaux responsables participent à des comités où les aspects de protection des RP sont abordés.

Le premier comité, nommé « Comité de gestion de ressources et actifs informationnels », traite notamment de sujets comme la proposition d'orientation sur les principaux enjeux de risques pour la STM, de même que sur l'examen des principaux incidents de risques informationnels survenus à la STM et dans le domaine du transport collectif.

Un second comité, auquel participe le secrétaire corporatif, dresse le bilan annuel des demandes d'accès à l'information et de leurs traitements sous forme de statistiques. Ce bilan est également présenté au comité « Gouvernance, éthique et développement durable » du conseil d'administration et se retrouve dans une des sections du rapport annuel de la STM.

L'examen de ces éléments nous permet de conclure que les responsabilités en matière de RP sont correctement attribuées et qu'un processus de reddition de comptes a été mis en place et fonctionne adéquatement. Aucune recommandation n'est nécessaire.

3.1.4. INVENTAIRE ET CLASSIFICATION DES RENSEIGNEMENTS PERSONNELS

3.1.4.A. CONTEXTE ET CONSTATATIONS

Ce dernier élément de notre travail portant sur le volet de la gouvernance est spécifiquement défini dans la LAD. En effet, l'article 76 mentionne qu'« *un organisme public doit établir et maintenir à jour un inventaire de ses fichiers de renseignements personnels* ».

Selon cet article, l'inventaire doit contenir les indications suivantes :

- La désignation de chaque fichier, les catégories de renseignements qu'il contient, les fins pour lesquelles les renseignements sont conservés et le mode de gestion de chaque fichier;
- La provenance des renseignements versés à chaque fichier;
- Les catégories de personnes concernées par les renseignements versés à chaque fichier;
- Les catégories de personnes qui ont accès à chaque fichier dans l'exercice de leurs fonctions;
- Les mesures de sécurité prises pour assurer la protection des renseignements personnels.

Toute personne qui en fait la demande a droit d'accès à cet inventaire, sauf à l'égard des renseignements dont la confirmation de l'existence peut être refusée en vertu des dispositions de la présente loi.

En outre, la réalisation de l'inventaire et la classification des RP pour l'ensemble des processus manuels et informatisés afférents au traitement des RP permettent d'avoir une vue d'ensemble qui facilitera les processus :

- d'analyses de risque de la STM;
- d'établissement de contrôles pour assurer la protection des RP.

La STM a inventorié ses RP sous la forme d'un tableau. Pour chacun de ses secteurs corporatifs, ce tableau identifie, comme requis par la LAD :

- les catégories de renseignements;
- la provenance de ces renseignements;
- la catégorie de personnes visées par ces renseignements;
- la catégorie de personnes qui ont accès à ces renseignements;
- les mesures de sécurité prises pour assurer la protection de ces renseignements.

La STM a également établi un plan de classification des documents par sujet, selon une hiérarchie logique basée sur ses principales activités. Parmi celles-ci, nous notons plus particulièrement les catégories suivantes en lien avec la gestion des RP :

- Gestion de l'information et des communications;
- Gestion des ressources humaines (la dotation, le dossier de ressources humaines, la santé et sécurité).

À la lumière des informations contenues dans ces deux documents, la STM nourrit annuellement son processus d'analyse de risques où l'aspect de la protection des RP est pris en compte et où des mesures d'atténuation et de contrôle sont établies.

Cependant, malgré le fait que l'inventaire des RP semble complet, nous notons que ce tableau ne précise pas spécifiquement chacun des types de RP contenus dans les systèmes informatiques ou les dossiers physiques.

Par exemple, pour le système SIGESST (la santé et sécurité, les congés de maladie), le système E-Dotation (les candidatures externes) ou le système ACCÈS (les clients du transport adapté), il n'est pas possible de connaître précisément quels sont les RP qu'ils contiennent, ni même les RP qui sont enregistrés de manière facultative.

De plus, le nombre de dossiers ou d'éléments se rattachant aux catégories de renseignements n'est pas précisé, et ce, même de façon approximative. Ces données statistiques permettraient de bonifier le processus d'analyse de risques.

Bien que ces éléments ne soient pas des exigences de la LAD, la STM pourrait ainsi prendre de meilleures décisions relativement aux mesures d'atténuation et de contrôle à apporter si ces renseignements y étaient inclus.

RECOMMANDATION

3.1.4.B. **Nous recommandons au Secrétariat corporatif et direction affaires juridiques de bonifier l'inventaire des renseignements personnels en ajoutant les informations suivantes :**

- **Tous les types de renseignements personnels détenus, qu'ils soient facultatifs ou non, pour chaque support physique et/ou électronique;**
- **Le nombre de dossiers ou d'éléments détenus pour chaque type de renseignements personnels.**

RÉPONSE DE L'UNITÉ D'AFFAIRES

3.1.4.B. ***Société de transport de Montréal***

Considérant le niveau de risque résiduel évalué comme faible, voici une des actions que nous proposons :

- *Bonifier l'inventaire des renseignements personnels pour tous les nouveaux fichiers à venir en créant une sous-catégorie afin de préciser les types de renseignements personnels et le nombre de dossiers s'y rattachant.* ***(Échéancier prévu : décembre 2018)***

3.2. CONSERVATION ET DESTRUCTION DES RENSEIGNEMENTS PERSONNELS

3.2.A. CONTEXTE ET CONSTATATIONS

Pour les aspects de conservation et de destruction des RP, la LAD édicte à l'article 63.1 que :

> *un organisme public doit prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support.*

La conservation des RP doit se conformer à la *Loi sur les archives*[4] : elle doit être basée sur des calendriers formellement définis et les accès aux données doivent être restreints uniquement aux personnes autorisées à l'aide de moyens de protection physique et logique. Un calendrier de conservation spécifie généralement le nombre d'années de rétention propre à chacun des RP. Dans le cas de la STM, le calendrier est sous la forme de fiches. Ces dernières spécifient le nombre d'années pour les états actifs et semi-actifs des dossiers.

4 RLRQ, chapitre A-21.1.

Lors de la destruction des RP, des mesures doivent être prises pour assurer la protection du caractère confidentiel des RP. Par exemple :

- définir et appliquer une politique de destruction de supports et de documents contenant des RP;

- lors d'un appel à une entreprise spécialisée, un contrat doit être défini et contenir des clauses qui permettent d'assurer la confidentialité des RP. Cette entreprise doit suivre les normes de l'industrie pour s'assurer de la confidentialité des RP lors de la destruction des documents.

Pour les fins de notre audit, nous avons examiné deux des actions visées, soit la conservation et la destruction des RP.

CONSERVATION

Notre travail visait à nous assurer que les RP amassés étaient conservés uniquement pour la période de temps nécessaire aux fins des objectifs pour lesquels ils avaient été recueillis.

Pour les RP contenus dans les dossiers physiques, nous avons validé l'existence de fiches indiquant la durée de conservation fixée pour les dossiers :

- d'employés de même que leurs dossiers médicaux;
- d'employés en accidents de travail;
- d'admissibilité au transport adapté;
- de candidatures externes.

De plus, notre analyse des systèmes informatiques a permis de constater que la STM, pour les nouvelles applications récemment implantées, précise les règles de conservation de données informatiques dans une fiche en annexe du tableau des RP. Cependant, pour les plus vieux systèmes comme VP, SAP, SIGESST, ACCÈS et E-Dotation, la STM ne possède pas ces fiches. Ainsi, il est difficile de savoir si l'on doit appliquer les mêmes règles que pour la contrepartie physique. Précisons toutefois que pour le système VP, l'information relative à la durée de conservation se retrouve dans des procédures de système.

Sans un portrait global des délais de conservation des RP, tant au niveau des dossiers physiques que des systèmes informatiques, la STM fait face au risque d'une interprétation aléatoire des règles de conservation qui pourrait engendrer une perte de confidentialité des RP, car ceux-ci seraient détenus plus que le temps nécessaire par rapport aux besoins opérationnels.

Il serait souhaitable qu'une synthèse contenant les calendriers de conservation des RP, et ce, pour l'ensemble des supports (papier et informatique) soit produite, ce qui permettrait de faciliter le suivi des temps de conservation et de destruction de tous les RP.

DESTRUCTION

Les renseignements qui ne sont plus requis doivent être rendus anonymes ou détruits d'une façon à en prévenir la perte, le vol, l'abus ou l'accès non autorisé.

Pour les dossiers physiques, nous avons constaté qu'une firme externe assure l'archivage des dossiers à l'état semi-actif. Cette firme en assure également la destruction. Ce fournisseur s'engage à respecter la confidentialité des informations qui lui sont fournies. Nous avons observé que les exigences quant aux services sont précisées au devis et incluent notamment la prise en charge de l'inventaire (le transfert de dossiers). La firme est certifiée NAID AAA (*National Association for Information Destruction*), attestant que la destruction de données papier et informatiques est effectuée de manière sécuritaire. La firme remet à la STM un certificat une fois la destruction complétée.

Dans le cas des fichiers numériques, la destruction des données ne s'effectue qu'à l'intérieur des applications VP et ACCÈS. Pour celles-ci, nous avons obtenu des rapports indiquant que les RP avaient été détruits.

Pour les applications E-Dotation, SIGESST et SAP, il nous a été confirmé que la STM n'effectue aucune destruction de RP. Le fait de ne pas effectuer de destruction de RP à l'intérieur de ces applications risquerait d'engendrer une détention d'information au-delà du temps nécessaire, augmentant la probabilité de divulgation de RP.

RECOMMANDATION

3.2.B. **Nous recommandons au Secrétariat corporatif et direction affaires juridiques conjointement avec la Direction exécutive des technologies de l'information et innovation d'établir :**

- **des règles de conservation pour les systèmes informatisés hormis les plus récents afin d'obtenir un portrait global pour l'ensemble des renseignements personnels;**
- **des procédures de destruction de renseignements personnels pour les systèmes suivants : le système de gestion des candidatures (E-Dotation), le système de gestion de la santé et sécurité au travail traitant également les congés de maladie (SIGESST) et le progiciel de gestion intégré pour, entre autres, les ressources humaines et la paie (SAP).**

RÉPONSE DE L'UNITÉ D'AFFAIRES

3.2.B. ***Société de transport de Montréal***

Faire l'inventaire des systèmes nécessitant la mise en place de règles de conservation. Établir les règles de conservation avec les parties prenantes des systèmes inventoriés. Faire approuver les règles par les autorités requises. Définir une procédure de destruction des renseignements personnels avec les parties prenantes pour chacun des systèmes inventoriés. Mettre en application la procédure de destruction de façon périodique. ***(Échéancier prévu : juin 2019)***

3.3. MESURES DE PROTECTION SUR LES RENSEIGNEMENTS PERSONNELS

Une mesure de protection représente tout processus, mécanisme ou action permettant de limiter les risques qu'une personne puisse s'accaparer d'une manière quelconque des RP sans autorisation. Parmi ces mesures, nous retrouvons :

- la gestion des accès physiques et logiques aux équipements et aux systèmes informatiques;
- l'effacement ou le caviardage de RP dans les environnements autres que ceux de production;
- une gestion des incidents qui permet de réagir en temps opportun (lorsqu'un bris de sécurité survient);
- le chiffrement des données transmises à un tiers;
- l'exécution de tests d'intrusion permettant d'identifier les vulnérabilités.

Une divulgation, un accès non autorisé ou une perte de confidentialité portant sur des RP pourrait entraîner :

- une atteinte à la sécurité des personnes;
- une usurpation d'identité;
- un vol ou une divulgation de RP ou médicaux des employés;
- un vol ou une divulgation de RP des clients;
- une atteinte à la réputation ou une perte de confiance des usagers;
- des poursuites judiciaires.

Afin de s'assurer que la STM protège adéquatement les RP contre tous ces risques, nous avons examiné :

- les procédures liées aux RP contenus dans les environnements autres que ceux de production;
- les procédures liées à la gestion des accès aux systèmes informatiques;
- l'accès physique aux dossiers contenant des RP;
- les mécanismes de contrôle portant sur la transmission de RP à des tiers;
- la gestion des incidents;
- la présence et le fonctionnement d'un programme de tests d'intrusion.

3.3.1. RENSEIGNEMENTS PERSONNELS DANS LES ENVIRONNEMENTS AUTRES QUE CEUX DE PRODUCTION

3.3.1.A. CONTEXTE ET CONSTATATIONS

Pour ce volet de notre audit, nous voulions nous assurer que des mécanismes étaient mis en place afin d'éviter l'utilisation de RP dans les environnements informatiques de la STM autres que ceux de production.

Les systèmes d'information ont, en général, plusieurs environnements distincts. Parmi ceux ci, il y a l'environnement de production utilisé par les employés dans le cadre de leur travail et qui contient des données réelles afin de répondre aux besoins d'affaires. Ensuite, il y a les environnements utilisés à d'autres fins, par exemple :

- les environnements dits de développement : ces derniers sont utilisés par les spécialistes en TI pour développer ou améliorer les fonctionnalités des applications;
- les environnements dits de tests : ils sont utilisés par des groupes d'utilisateurs et d'informaticiens pour s'assurer que les changements apportés aux applications fonctionnent correctement avant de les déployer en production;
- les environnements de formation : ils permettent aux employés d'acquérir l'expertise nécessaire pour utiliser efficacement les systèmes d'information.

Cependant, sauf exception les environnements autres que ceux de production n'ont nullement besoin d'utiliser des données réelles, surtout lorsqu'il s'agit de données confidentielles comme les RP. Les saines pratiques de l'industrie recommandent que des données fictives soient utilisées dans les environnements autres que ceux de production.

Au cours de nos travaux, nous avons constaté que le système VP ne contient pas de RP réels dans ses trois environnements hors production. En effet, ceux-ci utilisent des données représentant une combinaison entre des fausses données et des données modifiées (p. ex la date de naissance).

Par contre, pour les systèmes d'information énumérés ci-après, des RP réels étaient copiés, en totalité ou en partie, des environnements de production aux différents environnements de tests et de développement. De plus, aucune procédure systématique d'effacement des RP n'est appliquée une fois que les tests ou les travaux de développement sont terminés.

- **SAP** : Quatre environnements sur cinq utilisent des RP réels (préproduction, assurance qualité, développement, projet) provenant de l'environnement de production, comme le nom, le prénom, le NAS, la date de naissance, les coordonnées bancaires, l'adresse domiciliaire et le numéro de téléphone résidentiel.
- **E-Dotation** : Pour les trois environnements (développement, assurance qualité et préproduction), toutes les données de production y sont importées, ce qui inclut des RP comme le nom, le prénom, l'adresse domiciliaire, le numéro de téléphone personnel, l'adresse de courriel personnel, le numéro de permis de conduire (le cas échéant), le sexe, le groupe d'appartenance (le groupe ethnique) et l'indicateur de handicap (oui ou non).

- **SIGESST** : Pour l'unique environnement de préproduction, les employés y ayant accès utilisent des RP réels provenant de l'environnement de production, comme le nom, le prénom, le NAS, la date de naissance, le sexe, le numéro de téléphone à domicile et le courriel.

- **ACCÈS** : Quatre environnements (développement, assurance qualité, préproduction et formation) utilisent des RP réels provenant de l'environnement de production comme le nom, le prénom, le NAS, la date de naissance, l'adresse et le numéro de téléphone résidentiel; le nom, le prénom et, le cas échéant, la date de naissance des enfants accompagnateurs de moins de 14 ans.

En permettant l'utilisation de RP réels en dehors des environnements de production, les RP de l'ensemble des employés, des clients et des postulants à un emploi pourraient être dérobés et divulgués à des personnes non autorisées. À l'aide de tels renseignements, des individus mal intentionnés pourraient perpétrer des actions frauduleuses comme le vol et l'usurpation d'identité. Dans tous les cas, cela porterait grandement atteinte à la réputation de la STM.

RECOMMANDATION

3.3.1.B. **Nous recommandons à la Direction exécutive des technologies de l'information et innovation de :**

- **supprimer les renseignements personnels réels des environnements autres que ceux de production (p. ex. par des mécanismes de caviardage ou d'anonymisation) relativement aux systèmes d'information suivants :**
  - **Progiciel de gestion intégré pour, entre autres, les ressources humaines et la paie (SAP);**
  - **Système de gestion de la santé et sécurité au travail traitant également les congés de maladie (SIGESST);**
  - **Système de gestion des clients du transport adapté (ACCÈS);**
  - **Système de gestion des candidatures (E-Dotation);**
- **instaurer un processus systématique d'effacement des renseignements personnels.**

RÉPONSE DE L'UNITÉ D'AFFAIRES

3.3.1.B. ***Société de transport de Montréal***

Pour chacun des systèmes identifiés, en collaboration avec les propriétaires des systèmes, réaliser une analyse pour identifier les solutions permettant d'atténuer le risque lié à l'utilisation de renseignements personnels dans les environnements hors production tout en répondant aux besoins du développement et de l'assurance qualité. Considérant le niveau de risque associé, prioriser l'analyse du progiciel de gestion intégré pour, entre autres, les ressources humaines et la paie.

- *Prioriser et livrer l'analyse pour le progiciel de gestion intégré pour, entre autres, les ressources humaines et la paie.* ***(Échéancier prévu : septembre 2018)***
- *Livrer les analyses pour les autres systèmes identifiés :* ***(Échéancier prévu : mars 2019)***
  - *Système de gestion de la santé et sécurité au travail traitant également les congés de maladie;*
  - *Système de gestion des clients du transport adapté; et*
  - *Système de gestion des candidatures.*
- *Réaliser un plan de mise en œuvre pour les solutions identifiées dans le cadre des analyses.* ***(Échéancier prévu : à venir)***

3.3.2. ACCÈS LOGIQUES

3.3.2.A. CONTEXTE ET CONSTATATIONS

Pour ce deuxième volet des mesures de protection, nous avons examiné les procédures en place restreignant les accès logiques aux RP uniquement aux personnes autorisées. Cet examen s'est effectué sous trois angles, soit l'octroi des accès aux utilisateurs et aux administrateurs, la révision de ceux-ci de même que les paramètres utilisés pour le durcissement des mots de passe.

Nous avons constaté que pour les systèmes ACCÈS, SIGESST et E-Dotation, la robustesse des mots de passe est adéquate, puisque les paramètres sont les suivants :

- La longueur minimale est de 8 caractères;
- La complexité est activée (des caractères spéciaux, des majuscules, des nombres, etc.);
- Le délai d'expiration est de 90 jours;
- L'historique empêche la réutilisation des cinq derniers mots de passe.

Pour les systèmes ACCÈS et SIGESST, les accès consentis aux utilisateurs et aux administrateurs sont légitimes selon leurs responsabilités actuelles de même qu'un formulaire de demande d'accès a été signé par une personne en autorité. Ces accès font l'objet d'une revue périodique formelle.

Toutefois, les accès au système E-Dotation ne font pas l'objet d'une telle revue. En effet, lors de nos tests sur les comptes administrateurs d'E Dotation, nous avons relevé que deux comptes dans la liste des accès étaient encore actifs alors que les utilisateurs avaient quitté la STM. E-Dotation contient les RP suivants :

- Nom et prénom;
- Adresse domiciliaire;
- Numéro de téléphone personnel;
- Adresse de courriel personnel;
- Numéro du permis de conduire (le cas échéant);
- Sexe.

Mentionnons que le système E-Dotation doit être remplacé en décembre 2018. Cependant, E Dotation conservera pour au moins trois ans ses données afférentes de plus de 200 000 dossiers pour des contraintes opérationnelles, car, entre autres, beaucoup de candidats postulent plus d'une fois et leurs informations personnelles doivent être récupérées. Lors de ce remplacement, les accès à l'ancien système E-Dotation seront limités à deux ou trois utilisateurs en mode lecture seulement.

Sans révision des accès, la STM fait face au risque que des personnes ayant quitté leur emploi conservent des droits d'accès au système E-Dotation, de même que celles qui auraient changé de fonctions pourraient maintenir d'anciens droits d'accès ne correspondant plus à leurs nouvelles tâches et responsabilités. Cela pourrait engendrer une perte de confidentialité des RP détenus par la STM.

RECOMMANDATION

3.3.2.B. **Nous recommandons à la Direction expertise ressources humaines en collaboration avec la Direction exécutive des technologies de l'information et innovation de mettre en place un processus récurrent de révision des accès et des privilèges afférents pour le système de gestion des candidatures (E-Dotation) jusqu'à son remplacement. Ce même processus devrait être mis en place pour le nouveau système.**

RÉPONSE DE L'UNITÉ D'AFFAIRES

3.3.2.B. ***Société de transport de Montréal***

Mettre en place le processus annuel de révision des accès sur le système de gestion des candidatures. ***(Échéancier prévu : septembre 2018)***

S'assurer de mettre en place le processus de révision annuelle des accès dans le cadre du projet Solution de Gestion des Talents (nouvelle solution qui remplacera le système de gestion des candidatures).
(Échéancier prévu : décembre 2018)

3.3.3. ACCÈS PHYSIQUES

3.3.3.A. CONTEXTE ET CONSTATATIONS

Afin de s'assurer que les procédures et les mécanismes de sécurité mis en place limitaient l'accès physique aux RP uniquement aux personnes autorisées, nous avons vérifié si les locaux protégeant les dossiers ayant des RP étaient pourvus d'un mécanisme de sécurité adéquat et si les personnes ayant accès à ces locaux étaient légitimes.

Selon les bonnes pratiques de l'industrie et conformément à l'esprit de la LAD, les accès aux locaux contenant des données sensibles doivent être protégés par des mécanismes de cloisonnement des accès physiques. Ces mécanismes peuvent être, par exemple, un local réservé à l'entreposage des dossiers, des portes installées séparant les couloirs d'accès des bureaux. Ces portes devraient être verrouillées par des lecteurs de cartes d'accès. Les systèmes d'accès par lecteur de carte permettent la traçabilité de l'utilisateur qui a pénétré dans le local en plus de limiter cet accès aux seules personnes autorisées.

Notre audit a porté sur les trois locaux suivants :

- Ressources humaines : contient les dossiers d'employés et les dossiers de candidatures;
- Transport adapté : contient les données médicales des clients inscrites sur les formulaires de demande d'admission au transport adapté;
- Bureau de santé : contient les dossiers médicaux des employés.

Cet examen nous a permis de constater que seul le local Bureau de santé abritant les dossiers médicaux des employés possède un système d'accès par lecteur de carte. Ces accès sont révisés plusieurs fois par an. Nous n'avons relevé aucune lacune dans la gestion de ces accès.

Pour les deux autres locaux (les ressources humaines et le transport adapté), ceux-ci sont munis d'une serrure à combinaison à cinq chiffres. Avec ce type de serrure, il est impossible d'identifier quelle est la personne qui est entrée et à quelle date et quelle heure cela s'est produit.

Voici les principaux RP qui pourraient être exposés :

- Ressources humaines : dossiers d'employés et les candidatures :
  - Nom, prénom;
  - Adresse domiciliaire;
  - Numéro de téléphone personnel;
  - NAS;
  - Date de naissance;
  - Permis de conduire (pour certaines catégories d'emploi comme les chauffeurs d'autobus);
  - Curriculum vitae;

- Transport adapté : formulaire de demande d'admission au transport adapté :
  - Nom, prénom;
  - Adresse domiciliaire;
  - Numéro de téléphone personnel;
  - Date de naissance;
  - Adresse courriel;
  - Données médicales;
  - Sexe;

- Poids;
- Taille;
- Nom, prénom et date de naissance des enfants accompagnateurs de moins de 14 ans.

Bien que les serrures à combinaison soient plus sécuritaires que les serrures traditionnelles, elles ne permettent pas de s'assurer que seules les personnes autorisées ont accès à ces locaux. En effet, les codes d'accès, qu'ils soient modifiés régulièrement ou non, viennent à être connus de personnes n'ayant pas nécessairement le besoin de tels accès dans le cadre de leurs fonctions. De plus, advenant des événements frauduleux (p. ex. le vol de RP), il serait alors impossible de déterminer qui était présent sur les lieux au moment des faits.

Un employé malintentionné pourrait avoir accès à des RP et les dérober en consultant certains dossiers d'employés, de candidatures ou de formulaires de demande d'admission au transport adapté.

RECOMMANDATION

3.3.3.B. **Nous recommandons aux directions expertise ressources humaines et transport adapté de remplacer les serrures à combinaison par des lecteurs de cartes d'accès sur les portes des locaux suivants :**

- **Ressources humaines;**
- **Transport adapté.**

RÉPONSE DE L'UNITÉ D'AFFAIRES

3.3.3.B. ***Société de transport de Montréal***

Mettre en place les lecteurs de cartes d'accès sur la porte du local des Ressources humaines. ***(Échéancier prévu : décembre 2018)***

Mettre en place les lecteurs de cartes d'accès sur la porte du local du Transport adapté. ***(Échéancier prévu : décembre 2018)***

3.3.4. TRANSMISSION DES RENSEIGNEMENTS PERSONNELS À DES TIERS

3.3.4.A. CONTEXTE ET CONSTATATIONS

Nous désirions examiner ici les mécanismes et les outils qui ont été mis en place, permettant de protéger les RP lors de la transmission par courriel ou par d'autres moyens dans le cadre d'échanges avec des tierces parties externes.

Lors de la transmission des RP, le détenteur (ou le gardien) a l'obligation de protéger les RP par un moyen approprié au mode de transmission (p. ex. le courrier, le courrier électronique, le fax).

Dans le cadre de l'audit, nous avons identifié trois types d'échanges d'informations à des tiers.

Pour l'application VP, des rapports de données des clients sont transférés aux autres organismes de transport utilisant la carte OPUS, notamment le Réseau de transport métropolitain (RTM), le Réseau de transport de Longueuil (RTL), la Société de transport de Laval (STL), le Réseau de transport de la Capitale (RTC). Selon notre audit, les données transmises sont chiffrées et il est impossible d'identifier des clients sur les rapports diffusés.

Pour le transport adapté, la grande majorité des transports s'effectuent avec des compagnies de taxi externes. Seuls le nom, le prénom et l'adresse domiciliaire des clients sont transmis par courriel aux chauffeurs. Nous estimons que cela est tout de même adéquat, car ces types de RP ne sont pas critiques et donc le risque d'usurpation d'identité est très faible.

Au niveau des ressources humaines (les candidatures), des formulaires de « vérification de pré-emploi » sont transmis par courriel à la firme chargée de la vérification d'antécédents criminels, de références d'emploi et de diplômes académiques, dans le cadre de l'embauche de nouveaux employés. Le tout est effectué avec le consentement du candidat. La firme retenue a acquiescé aux clauses de confidentialité et de protection des RP de la STM. Outre le nom, le prénom, l'adresse et le numéro de téléphone personnel, d'autres renseignements comme la date de naissance, le NAS et le numéro de permis de conduire (à titre d'exemple pour un postulant sur un poste de chauffeur d'autobus), sont transmis. Les informations transmises à l'aide des courriels ne bénéficient pas de moyens de protection comme le chiffrement.

En ne protégeant pas adéquatement les formulaires de candidatures transmis par courriel, des personnes malveillantes pourraient dérober les RP des postulants et les utiliser pour perpétrer des vols d'identité.

RECOMMANDATION

3.3.4.B. **Nous recommandons à la Direction expertise ressources humaines en collaboration avec la Direction exécutive des technologies de l'information et innovation d'instaurer un mécanisme de protection lors de la transmission des renseignements personnels des candidats à la firme externe.**

RÉPONSE DE L'UNITÉ D'AFFAIRES

3.3.4.B. ***Société de transport de Montréal***

Analyser et mettre en place un mécanisme pour assurer la protection des renseignements personnels dans la transmission au fournisseur pour les vérifications de candidats. ***(Échéancier prévu : décembre 2018)***

3.3.5. GESTION DES INCIDENTS

3.3.5.A. CONTEXTE ET CONSTATATIONS

L'examen du processus de gestion des incidents permet d'identifier les bris de sécurité afférents aux RP et permet de mesurer si les correctifs appropriés ont été mis en place. Les activités relatives à la gestion des incidents doivent comprendre des procédures de détection et d'escalade propre aux RP. Finalement, ces activités doivent être documentées de manière appropriée et conservées aux fins de vérification.

Nous avons obtenu les documents faisant foi de l'existence et de la mise en place d'un processus de gestion des incidents, à savoir, un graphique d'acheminement présentant le « processus de communication – incident majeur » de même qu'un survol du processus global du Service aux utilisateurs contenant, entre autres, le processus de gestion des incidents et de gestion des demandes de sécurité. Un tableau de bord des incidents de sécurité est produit et présenté mensuellement au comité de gestion de la Direction exécutive des technologies de l'information et innovation, ainsi qu'au comité trimestriel de gestion de ressources et actifs informationnels.

En appui au processus de gestion des incidents, il existe des procédures détaillées traitant d'événements de sécurité, comme :

- les accès physiques non autorisés;
- l'ingénierie sociale;
- le vol et la perte d'équipements;
- la perte, le vol et le coulage de données.

L'examen de cette documentation nous permet de conclure que les procédures en place sont adéquates afin de gérer correctement les incidents liés au RP. Aucune recommandation n'est nécessaire.

3.3.6. PROGRAMME DE TESTS D'INTRUSION

3.3.6.A. CONTEXTE ET CONSTATATIONS

L'existence d'un programme de tests d'intrusion permet à l'organisation de mesurer ses vulnérabilités relativement au coulage ou aux accès non autorisés de RP qui proviendraient de l'externe. Le déploiement d'un tel programme permet de réagir plus rapidement et de colmater les brèches de sécurité, advenant le constat de failles potentielles dans les systèmes, limitant ainsi les risques.

Notre audit a consisté à prendre connaissance du programme de tests d'intrusion qui est constitué de trois éléments principaux : la méthodologie afférente, les rapports de tests et les plans d'action.

Nous avons constaté que la STM effectue deux types de tests d'intrusion :

- En premier lieu, des tests d'intrusion sur les nouveaux projets TI sont effectués juste avant la mise en production de l'application. À cet effet, nous avons examiné la méthodologie afférente d'un nouveau projet ainsi que le rapport de tests qui contient les recommandations sur les vulnérabilités découvertes. Ce rapport fait l'objet d'un plan d'action.

- En regard du deuxième type, des tests sont effectués sur les systèmes opérationnels de la STM une fois par année et simulent une attaque provenant de l'externe. Nous avons examiné la méthodologie d'un test qui contenait l'objectif, la portée, la définition des cibles, ainsi que le protocole d'intervention. Nous avons examiné ensuite le rapport de tests d'intrusion qui comprenait les résultats des tests. Les vulnérabilités identifiées de même que les correctifs à apporter ont été pris en considération dans un plan d'action.

L'examen de ce programme de tests nous permet de conclure que la méthodologie en place est adéquate afin de gérer correctement les vulnérabilités des systèmes, limitant ainsi les risques. Aucune recommandation n'est nécessaire.

4. CONCLUSION

Globalement, nous pouvons conclure que la Société de transport de Montréal protège adéquatement la sécurité des renseignements personnels amassés dans le cours de ses activités, par la présence et l'efficacité de contrôles limitant les risques de perte de confidentialité, de vol ou d'accès non autorisé.

En effet, selon les critères d'évaluation suivants :

Critère d'évaluation – Gouvernance :

- La Société de transport de Montréal dispose de politiques corporatives et de gestion adéquates qui encadrent la protection des renseignements personnels;
- Les responsabilités sont clairement établies et attribuées aux personnes appropriées;
- Diverses mesures sont en place comme des formations et des présentations aux employés et gestionnaires qui permettent de les sensibiliser à l'importance de la protection des renseignements personnels;
- Une reddition de comptes existe où les aspects de protection des renseignements personnels sont abordés;
- La Société de transport de Montréal possède un inventaire des renseignements personnels répondant aux exigences de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*. Cependant, même si elle ne le requiert pas, les types de renseignements personnels ainsi que le nombre de dossiers ne sont pas tous répertoriés.

Nous croyons que si la Société de transport de Montréal ajouterait à l'inventaire les types de renseignements personnels ainsi que le nombre de dossiers détenus pour chaque type de renseignements personnels, ces éléments supplémentaires bonifieraient le processus d'analyse de risque.

Critère d'évaluation – Conservation et destruction des renseignements personnels :

- Un calendrier de conservation a été établi pour les renseignements personnels présents au sein de dossiers physiques et pour les nouveaux systèmes. Néanmoins, il n'y a pas de règles de conservation pour les systèmes d'information suivants :
  - Système de gestion pour la vente et la perception des cartes OPUS;
  - Progiciel de gestion intégré pour, entre autres, les ressources humaines et la paie;
  - Système de gestion de la santé et sécurité au travail traitant également les congés de maladie;
  - Système de gestion des clients du transport adapté;
  - Système de gestion des candidatures.

- La destruction des renseignements personnels pour les dossiers physiques est effectuée par une firme externe de manière sécuritaire;

- La destruction des renseignements personnels ne s'effectue qu'au sein du système de gestion pour la vente et la perception des cartes OPUS et du système de gestion des clients du transport adapté. Rien n'est prévu pour les applications système de gestion des candidatures, système de gestion de la santé et sécurité au travail traitant également les congés de maladie et progiciel de gestion intégré pour, entre autres, les ressources humaines et la paie.

Nous pensons que si la Société de transport de Montréal met en place des règles de conservation et des procédures de destruction de renseignements personnels pour les systèmes susmentionnés, les renseignements personnels seraient détruits dès qu'ils ne seraient plus nécessaires aux activités de la Société de transport de Montréal.

Critère d'évaluation – Mesures de protection sur les renseignements personnels :

- Le système VP contient des renseignements personnels uniquement dans son environnement de production. Quant au système de gestion des clients du transport adapté, au système de gestion de la santé et sécurité au travail traitant également les congés de maladie, au progiciel de gestion intégré pour, entre autres, les ressources humaines et la paie et au système de gestion des candidatures, des renseignements personnels réels sont présents dans les environnements autres que ceux de production;

- La gestion des accès logiques est adéquate pour le système de gestion des clients du transport adapté et le système de gestion de la santé et sécurité au travail traitant également les congés de maladie. Des lacunes sont présentes au niveau de la révision des accès du système de gestion des candidatures;

- Le local hébergeant les dossiers médicaux dispose d'un lecteur de cartes qui restreint l'accès physique uniquement aux personnes autorisées. Les deux locaux abritant respectivement les dossiers d'employés et de candidatures et les formulaires de demande d'admission au transport adapté disposent de serrures à code qui sont moins sécuritaires que des lecteurs de cartes;

- La transmission électronique des renseignements personnels aux autres organismes de transport est sécuritaire. Par contre, la transmission de dossiers de candidatures à une firme externe n'est pas confidentielle puisqu'elle n'est pas chiffrée;

- Un processus de gestion des incidents est en place et inclut l'aspect de la protection des renseignements personnels;

- Des tests d'intrusion sont réalisés régulièrement afin de mettre à l'épreuve les systèmes contenant des renseignements personnels et de corriger les lacunes, le cas échéant.

Nous considérons que si la Société de transport de Montréal applique les mesures suivantes, ceci augmenterait l'efficacité des mesures de protection sur les renseignements personnels :

- Supprimer les renseignements personnels réels des environnements informatiques autres que ceux de production (p. ex. par des mécanismes de caviardage) et instaurer un processus systématique d'effacement des renseignements personnels une fois les tests ou les travaux de développement terminés;
- Mettre en place un processus récurrent de révision des accès et des privilèges afférents pour le système de gestion des candidatures;
- Remplacer les deux serrures à combinaison par des lecteurs de cartes d'accès sur les portes des locaux contenant les dossiers des ressources humaines et du transport adapté;
- Instaurer un mécanisme de protection lors de la transmission des renseignements personnels des candidats à la firme externe chargée de la vérification de pré-emploi.

5. ANNEXE

5.1. CRITÈRES D'ÉVALUATION

Nous avons basé notre audit sur les critères d'évaluation suivants répartis en trois volets :

- **Gouvernance :**
  - **Politiques** : La Société de transport de Montréal dispose d'encadrements définissant les exigences quant à la saine gestion des renseignements personnels applicables à l'ensemble des unités d'affaires;
  - **Programme de sensibilisation** : Les employés sont sensibilisés quant aux enjeux et aux risques liés aux renseignements personnels afin qu'ils soient plus à même de respecter les règles de sécurité relatives à leur protection;
  - **Attribution des responsabilités** : La Société de transport de Montréal a formellement attribué la responsabilité et la reddition de comptes à une direction pour développer, documenter et mettre en œuvre les exigences des politiques de protection des renseignements personnels;
  - **Inventaire et classification des renseignements personnels** : Il existe un inventaire des renseignements personnels, complet et à jour, permettant à la Société de transport de Montréal de disposer d'un portrait global des données à protéger en vue d'en assurer la confidentialité. L'aspect de la protection des renseignements personnels est intégré au processus d'analyse de risque.
- **Conservation et destruction des renseignements personnels** :
  - Les renseignements personnels sont conservés selon un calendrier préétabli. Lorsque les renseignements personnels ne sont plus requis, ils sont détruits de manière à ce qu'ils ne puissent plus être reconstitués pour éviter toute utilisation frauduleuse.

- **Mesures de protection sur les renseignements personnels** :
  - **Renseignements personnels dans les environnements autres que ceux de production** : Des mécanismes sont mis en place afin d'interdire l'utilisation de renseignements personnels réels dans les environnements informatiques autres que ceux de production;
  - **Accès logiques** : Les accès sont accordés de manière à ce que seulement les personnes autorisées, de par leurs fonctions, accèdent aux systèmes d'information contenant des renseignements personnels. Les paramètres de sécurité (p. ex. les mots de passe) sont assez robustes pour prévenir des accès non autorisés aux renseignements personnels;
  - **Accès physiques** : Des mécanismes permettent de limiter l'accès aux renseignements personnels présents sur des supports physiques (p. ex. des dossiers médicaux et des dossiers d'employés) aux seules personnes autorisées;
  - **Transmission des renseignements personnels à des tiers** : Les renseignements personnels transmis à des tierces parties sont protégés par des mécanismes de sécurité afin de préserver la confidentialité des informations transférées;
  - **Gestion des incidents** : Advenant un événement majeur pouvant conduire à la divulgation massive de renseignements personnels, il existe une procédure de gestion des incidents permettant à la Société de transport de Montréal de réagir dans les meilleurs délais faisant en sorte de limiter les répercussions réelles et potentielles, et de prendre les mesures nécessaires à la résolution de l'incident;
  - **Programme de tests d'intrusion** : Il existe un programme de tests d'intrusion qui inclut l'aspect des renseignements personnels qui permet de mesurer les vulnérabilités des systèmes informatiques face aux cyberattaques.