



SOCIÉTÉ DE TRANSPORT DE LAVAL

POLITIQUE-CADRE SUR LA GOUVERNANCE EN MATIÈRE DE PROTECTION DES
RENSEIGNEMENTS PERSONNELS

POLITIQUE ADMINISTRATIVE PA-54

ADOPTÉE PAR LE CONSEIL D'ADMINISTRATION

LE 25 SEPTEMBRE 2023

RÉSOLUTION 2023-81

Modifications subséquentes, dates et numéros de résolution

2024-06-26 (2024-43)

NOTE : Dans le présent document, l'emploi du genre masculin n'a pour but que d'alléger le texte

1. CONTEXTE ET OBJECTIFS

En tant qu'organisme public, la Société de transport de Laval (ci-après la « STL ») doit recueillir, traiter, conserver et communiquer des Renseignements personnels à des fins de gestion ou en vertu d'impératifs imposés par son cadre juridique. Elle est responsable de la protection des Renseignements personnels qu'elle détient.

La STL reconnaît que le droit à la vie privée est fondamental dans toute société démocratique. Elle adhère d'emblée à la nécessité de protéger les Renseignements personnels. Elle œuvre dans un environnement où les droits des personnes, incluant le droit à la protection de la vie privée, sont garantis par la Charte des droits et libertés de la personne du Québec, le Code civil du Québec et, en particulier, par la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (ci-après la « Loi sur l'accès »).

La présente Politique a pour objectif d'établir la gouvernance de ses activités en matière de protection des Renseignements personnels et d'identifier les mesures à mettre en place pour accomplir ses devoirs.

2. DÉFINITION

CAI : désigne la Commission d'accès à l'information.

Comité sur l'accès : désigne le Comité sur l'accès à l'information et sur la protection des renseignements personnels.

Consentement : désigne un consentement valable, c'est-à-dire qui est manifeste, libre, éclairé, donné à des fins spécifiques, en termes simples et clairs et donné que pour la durée nécessaire à la réalisation des fins auxquelles il a été demandé.

Un consentement peut être implicite, mais doit être fait de manière expresse lorsqu'il concerne des Renseignements personnels sensibles.

EFVP : désigne une évaluation des facteurs relatifs à la vie privée.

Employé : désigne toute personne embauchée, tant comme salarié que non salarié (i.e. travailleur autonome), par la STL.

Incident de confidentialité : désigne

- L'accès non autorisé par la Loi sur l'accès à un Renseignement personnel;
- L'utilisation non autorisée par la Loi sur l'accès d'un Renseignement personnel;
- La communication non autorisée par la Loi sur l'accès d'un Renseignement personnel;
- La perte d'un Renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

Responsable AI : désigne la personne responsable de l'accès à l'information, dont le mandat lui a été délégué par le Directeur général.

Responsable PRP : désigne la personne responsable de la protection des Renseignements personnels, dont le mandat lui a été délégué par le Directeur général.

Renseignement personnel : désigne tout renseignement qui concerne une personne physique et qui permet directement ou indirectement de l'identifier, tel que : le nom, l'adresse, le numéro de téléphone, l'adresse courriel, l'occupation, le matricule d'employé, le numéro d'assurance sociale, la date de naissance, la photographie et les coordonnées bancaires.

Renseignement personnel sensible : désigne tout Renseignement personnel qui, par sa nature ou en raison du contexte de son utilisation ou de sa communication, suscite un haut degré d'attente raisonnable en matière de vie privée.

Sont notamment considérés comme sensibles les renseignements médicaux, biométriques, génétiques ou financiers, ou, encore, des renseignements sur la vie ou l'orientation sexuelle, les convictions religieuses ou bien l'origine ethnique.

3. PORTÉE

La présente Politique concerne la gouvernance de l'ensemble des Renseignements personnels détenus par la STL ou par des tierces parties en son nom, qu'il s'agisse de ceux relatifs aux membres de son personnel ou à toute autre personne. Elle s'applique à tous les documents détenus par la STL qui contiennent des Renseignements personnels, quel que soit leur forme ou support (écrit, graphique, sonore, visuel, informatisé ou autre).

4. COLLECTE DES RENSEIGNEMENTS PERSONNELS

La STL recueille uniquement les Renseignements personnels nécessaires à l'exercice de ses attributions ou à la mise en œuvre d'un programme dont elle a la gestion.

La STL prend des mesures pour s'assurer que les Renseignements personnels qu'elle recueille sont adéquats, pertinents, non excessifs et utilisés à des fins limitées.

Préalablement à la cueillette et par la suite sur demande, la STL informe la personne concernée notamment des modalités de la cueillette, des fins auxquelles ces renseignements sont recueillis ainsi que de leurs droits quant à ces renseignements conformément à la Loi sur l'accès.

La STL peut recueillir un Renseignement personnel si cela est nécessaire à l'exercice des attributions ou à la mise en œuvre d'un programme d'un organisme public avec lequel elle collabore pour la prestation de services ou pour la réalisation d'une mission commune. Dans ce cas, la collecte doit être précédée d'une évaluation des facteurs relatifs à la vie privée et s'effectuer dans le cadre d'une entente écrite transmise à la CAI conformément à la Loi sur l'accès. Cette entente doit également être consignée dans un registre prévu par la Loi sur l'accès.

5. UTILISATION DES RENSEIGNEMENTS PERSONNELS

La STL utilise des Renseignements personnels aux seules fins précisées lors de la collecte, à moins que la personne concernée par les renseignements n'y consente ou que la Loi sur l'accès le permette. Ce Consentement doit être manifesté de façon expresse dès qu'il s'agit d'un Renseignement personnel sensible.

La STL doit tenir un registre et y inscrire toute utilisation de Renseignements personnels effectuée sans le Consentement des personnes concernées dans les situations prévues par la Loi sur l'accès.

La STL peut anonymiser des Renseignements personnels pour les utiliser à des fins d'intérêt public.

6. COMMUNICATION DES RENSEIGNEMENTS PERSONNELS

La STL ne communique pas les Renseignements personnels qu'elle collecte, à moins que la personne concernée par les renseignements n'y consente ou que la Loi sur l'accès ne le permette. Ce Consentement doit être manifesté de façon expresse dès qu'il s'agit d'un Renseignement personnel sensible.

La STL peut communiquer les Renseignements personnels qu'elle collecte à des fournisseurs de services et à d'autres tiers qui la soutiennent. Dans ce cas, un contrat liant la STL à ces tiers, ou une formule d'engagement signée par ces derniers, doit les obliger à garder les Renseignements personnels confidentiels, de les utiliser uniquement aux fins pour lesquelles la STL les divulgue et de traiter les Renseignements personnels selon les normes énoncées dans la présente Politique et en respect des lois.

La STL peut communiquer certains Renseignements personnels à des fins d'étude, de recherche ou de production de statistiques sous réserve des conditions prévues par la Loi sur l'accès. Elle traite alors la situation conformément à la Loi sur l'accès et à la Directive portant sur l'utilisation ou la communication de Renseignements personnels à des fins d'étude, de recherche ou de production de statistiques adoptée par le Comité sur l'accès.

Avant de communiquer à l'extérieur du Québec des Renseignements personnels ou de confier à une personne, à un tiers ou à un organisme public à l'extérieur du Québec la tâche de recueillir, d'utiliser, de communiquer ou de conserver pour son compte des Renseignements personnels, notamment à des fins d'hébergement de données, la STL doit procéder à une EFVP.

La STL doit tenir un registre et y inscrire toute communication de Renseignements personnels effectuée sans le Consentement des personnes concernées dans les situations prévues par la Loi sur l'accès.

La STL peut créer une banque de caractéristiques ou de mesures biométriques, mais elle doit préalablement divulguer sa création à la CAI. La STL doit divulguer l'existence de telle banque qu'elle soit ou non en service. La CAI peut rendre toute ordonnance concernant cette banque afin d'en déterminer la confection, l'utilisation, la consultation, la communication et la conservation y compris l'archivage ou la destruction des mesures ou caractéristiques prises pour établir l'identité d'une personne. La CAI peut aussi suspendre ou interdire la mise en service de telle banque ou en ordonner la destruction.

7. CONSERVATION ET DESTRUCTION DES RENSEIGNEMENTS PERSONNELS

La STL conserve les Renseignements personnels qu'elle détient pour le temps nécessaire pour atteindre les fins pour lesquelles elle les a collectés et conformément à son calendrier de conservation, à moins d'autorisation ou d'exigence des lois ou de la réglementation applicable.

Lorsque la STL procède à la destruction de documents contenant des Renseignements personnels, elle s'assure de prendre les mesures de protection nécessaires visant à assurer la confidentialité de ceux-ci. La STL détermine la méthode de destruction utilisée en fonction de la sensibilité des renseignements, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support.

8. PROTECTION DES RENSEIGNEMENTS PERSONNELS

La STL met en place des mesures de sécurité appropriées et raisonnables afin de protéger les Renseignements personnels contre la perte ou le vol et contre l'accès, la divulgation, la copie, l'utilisation ou la modification non autorisés par la Loi sur l'accès. Seuls les membres du personnel qui doivent absolument avoir accès aux Renseignements personnels dans le cadre de leurs fonctions sont autorisés à y accéder.

Les Employés de la STL ou les tiers qui travaillent en son nom doivent, notamment :

- Prendre connaissance de la présente Politique;
- Faire des efforts raisonnables pour minimiser le risque de divulgation non intentionnelle de Renseignements personnels;
- Prendre des précautions particulières pour s'assurer que les Renseignements personnels ne sont pas surveillés, entendus, consultés ou perdus lorsqu'ils travaillent dans des bureaux ouverts ou tout autre lieu public; et
- Prendre des mesures raisonnables pour protéger les Renseignements personnels lorsqu'ils se déplacent d'un endroit à l'autre.

Les tiers ayant accès aux Renseignements personnels détenus par la STL sont informés de la présente Politique ainsi que des autres politiques et processus applicables pour assurer la sécurité et la protection des Renseignements personnels.

9. DROIT DES PERSONNES CONCERNÉES SUR LES RENSEIGNEMENTS PERSONNELS

9.1 Demande d'accès à ses Renseignements personnels

Toute personne qui en fait la demande a un droit d'accès aux Renseignements personnels la concernant détenus par la STL, sous réserve des exceptions prévues par la Loi sur l'accès. Le Responsable AI traite la demande conformément à la Loi sur l'accès.

9.2 Demande d'accès aux Renseignements personnels du conjoint ou proche parent d'une personne décédée

Tout conjoint ou proche parent qui en fait la demande a un droit d'accès aux Renseignements personnels de la personne décédée détenus par la STL si la connaissance de ces Renseignements personnels est susceptible d'aider le conjoint ou proche parent dans son processus de deuil et que la personne décédée n'a pas consigné par écrit son refus d'accorder ce droit d'accès. Le Responsable AI traite la demande conformément à la Loi sur l'accès.

9.3 Droit à la portabilité des Renseignements personnels

Toute personne concernée par les Renseignements personnels et qui en fait la demande a droit de recevoir, dans un format technologique structuré et couramment utilisé, le Renseignement personnel informatisé recueilli auprès d'elle. Cette communication peut aussi être faite à une personne ou à un organisme autorisé à recueillir le Renseignement personnel, à la demande de la personne concernée. Le Responsable AI traite la demande conformément à la Loi sur l'accès.

9.4 Demande de rectification

Toute personne qui reçoit confirmation de l'existence, dans un fichier, d'un Renseignement personnel la concernant peut, s'il est inexact, incomplet ou ambigu, ou si sa collecte, sa communication ou sa conservation ne sont pas autorisées par la Loi sur l'accès, demander que le fichier soit rectifié. Le Responsable AI traite la demande conformément à la Loi sur l'accès.

9.5 Dépôt d'une plainte relative à la protection des Renseignements personnels

Toute personne qui a des motifs de croire qu'un Incident de confidentialité s'est produit ou que la STL a fait défaut d'assurer la confidentialité des Renseignements personnels qu'elle détient peut adresser une plainte écrite auprès du Responsable PRP pour demander que la situation soit corrigée.

La plainte doit être formulée à responsable.acces@stl.laval.qc.ca et comporter une description de la situation, la date ou la période où la situation s'est produite, la nature des Renseignements personnels visés et le nombre de personnes concernées.

Sur réception de la plainte, le Responsable PRP ou le Directeur général, selon le cas, en accuse la réception auprès de son auteur. Il analyse et traite la plainte conformément à la Loi sur l'accès.

10. RÔLES ET RESPONSABILITÉS

10.1 Directeur général

La personne ayant la plus haute autorité à la STL, soit le Directeur général, veille à assurer le respect et la mise en œuvre de la Loi sur l'accès. Elle exerce la fonction de Responsable AI et celle de Responsable PRP.

Ces fonctions peuvent être déléguées par écrit, en tout ou en partie, à un ou des Employés. Lorsqu'elle n'exerce pas elle-même ces fonctions, la personne ayant la plus haute autorité au sein d'un organisme public veille à en faciliter l'exercice.

Le Directeur général est également responsable de déterminer le mandat du Comité sur l'accès et d'en déterminer la composition.

En certaines circonstances, le Directeur général peut recevoir les plaintes qui mettent en cause la protection des Renseignements personnels et les traiter en collaboration avec le Responsable PRP.

10.2 Comité sur l'accès à l'information et la protection des renseignements personnels

Le Comité sur l'accès, qui relève du Directeur général, est chargé de soutenir la STL dans l'exercice de ses responsabilités et dans l'exécution de ses obligations en vertu de la Loi sur l'accès. À ce titre, son mandat, ses rôles et responsabilités, sa composition ainsi que son fonctionnement sont définis dans la Charte de comité du Comité sur l'accès approuvée par le Directeur général.

10.3 Responsable de l'accès à l'information

La personne qui assume ce rôle applique la Loi sur l'accès. Elle exerce tous les pouvoirs nécessaires à son application. Elle agit de manière autonome en cette matière. Les membres du personnel doivent collaborer avec elle pour répondre efficacement aux exigences qui y sont prévues. À cet effet, cette personne est notamment responsable de recevoir et traiter les demandes d'accès et de rectification en respect de la protection des Renseignements personnels et de la confidentialité.

10.4 Responsable de la protection des renseignements personnels

La personne qui assume ce rôle applique la Loi sur l'accès. Elle exerce tous les pouvoirs nécessaires à son application. Elle agit de manière autonome en cette matière. Les membres du personnel doivent collaborer avec elle pour répondre efficacement aux exigences qui y sont prévues. À cet effet, cette personne est notamment responsable de :

- Recevoir les Incidents de confidentialité et les traiter;
- Recevoir les plaintes qui mettent en cause la protection des Renseignements personnels, sauf celles qui la concernent, et les traiter;
- Tenir à jour le registre des communications de Renseignements personnels et le registre des Incidents de confidentialités;
- En collaboration avec la Direction, Technologies de l'information ainsi que le Responsable de la gestion documentaire, réaliser lorsque nécessaire l'inventaire des fichiers de Renseignements personnels;
- En collaboration avec le Comité, participer au processus d'EFVP lorsque la Loi l'exige;
- S'assurer que des formations et des activités de sensibilisation soient dispensées auprès des employés.

10.5 Direction, Technologies de l'information

La Direction, Technologies de l'information est notamment responsable de :

- Assurer la mise en place des mesures de protection des Renseignements personnels;
- Appliquer des mesures de réaction appropriées à toute menace et à tout incident de sécurité de l'information et de confidentialité lorsque les circonstances l'exigent, et ce, en vue d'assurer la sécurité de l'information et la protection des Renseignements personnels en cause;
- Assurer le fonctionnement du processus de gestion des accès selon les mécanismes mis en place;
- Soutenir les activités du Comité sur l'accès, lorsque requis.

10.6 Direction, Ressources humaines

La Direction, Ressources humaines est notamment responsable de :

- Informer la Direction, Technologies de l'information d'une embauche, d'un changement de fonction et de la fin d'emploi d'une personne, afin de mettre à jour les accès aux actifs informationnels de la STL;

- Informer tout nouvel Employé de ses obligations découlant de la présente Politique ainsi que de tout cadre normatif qui découle de ces derniers, et obtient son engagement à leur respect;
- Intervenir auprès des Employés concernés en cas d'atteinte à la confidentialité et la protection des Renseignements personnels, en collaboration avec le Responsable PRP et les autres personnes intervenantes;
- Contribuer à la promotion des activités de sensibilisation et des séances de formation pour les Employés reliées à la protection des Renseignements personnels et la confidentialité.

10.7 Poste intégré de vigilance et d'opérations

Le Poste intégré de vigilance et d'opérations (ci-après le « PIVO ») est notamment responsable de :

- Sécuriser et contrôler les accès physiques aux bâtiments et aux lieux publics dont la STL est propriétaire ou dont elle a la gestion;
- Concevoir et mettre en œuvre les mesures de protection physique contre les sinistres, les pertes, les dommages, le vol ainsi que l'interruption des activités, afin de sécuriser les lieux et les accès;
- Gérer les moyens d'accès physique aux locaux à accès restreint;
- Mettre à jour les informations dans la base de données des clés, puces et cartes d'accès en suivant le mouvement du personnel au sein de la STL.

10.8 Responsable de la gestion documentaire

Le Responsable de la gestion documentaire est notamment responsable de :

- Participer à l'analyse et à la planification des besoins et des actions concernant la gestion des documents et des archives qui impliquent la protection de Renseignements personnels;
- Veiller à l'accès aux documents contenant des Renseignements personnels entreposés aux archives;
- Élaborer le plan de classification et le calendrier de conservation;
- Conseiller les Employés dans la classification des informations qu'ils détiennent en fonction du plan de classification et du calendrier de conservation;
- Collaborer à l'élaboration et à la mise en œuvre des mesures de protection adéquates dans la gestion documentaire, la conservation et la destruction eu égard à la Loi sur les archives et la Loi sur l'accès;
- S'impliquer dans l'ensemble des activités relatives à la gestion des risques, notamment dans l'élaboration et l'application des procédures de prévention, de préservation et de rétablissement des opérations à la suite d'un Incident de confidentialité;
- Sensibiliser les Employés à l'aspect de protection des Renseignements personnels dans le cadre des formations en gestion documentaire;
- En collaboration avec le Responsable AI, supporter ce dernier dans les demandes d'accès, de consultation et de communication de documents en respect de la protection des Renseignements personnels;
- Coordonner la destruction des documents contenant des renseignements personnels.

10.9 Gestionnaires

Les Gestionnaires sont notamment responsables de :

- Informer les Employés relevant de leur autorité des dispositions de la présente Politique et s'assurer de ses applications;
- Informer le Responsable PRP de toute violation des mesures de protection des Renseignements personnels ou de confidentialité dont ils pourraient être témoins;
- S'assurer que la protection des Renseignements personnels et la confidentialité sont prises en compte dans tout contrat de service attribué par leur unité administrative et voir à ce que tout collaborateur, lié par contrat, respecte les règles de la STL;
- Approuver les accès à chacun des utilisateurs selon leur profil (directeurs seulement).

10.10 Auditeur interne

L'auditeur interne est notamment responsable de réaliser des audits portant sur l'application des règles de gouvernance des Renseignements personnels selon son plan d'audit convenu.

10.11 Employés

Les Employés sont notamment responsables de :

- Prendre connaissance de la présente Politique et y adhérer en respectant les normes, directives et procédures en vigueur en matière de confidentialité et de protection des Renseignements personnels;
- Appliquer le plan de classification et le calendrier de conservation aux documents dont ils ont la responsabilité et consulter le Responsable de la gestion documentaire en cas d'ambiguïté;
- Veiller à ce que les Renseignements personnels qu'ils conservent soient à jour;
- S'impliquer dans l'ensemble des activités relatives à la gestion des risques, notamment des Incidents de confidentialité;
- Diriger toute demande d'accès à l'information provenant de tiers au Responsable AI;
- Veiller à la mise en place et à l'application des mesures de sécurité de l'information, y compris celles liées au respect des exigences de protection des Renseignements personnels;
- Informer le Responsable PRP de toute violation des mesures de protection des Renseignements personnels ou de confidentialité dont ils pourraient être témoins.

11. GESTION DES INCIDENTS DE CONFIDENTIALITÉ

Lorsque la STL a des motifs de croire que s'est produit un Incident de confidentialité impliquant un Renseignement personnel qu'elle détient, elle traite la situation conformément à la Loi sur l'accès et au Processus de gestion des incidents de confidentialité adopté par le Comité sur l'accès. Elle doit notamment prendre les mesures raisonnables pour diminuer les risques qu'un préjudice ne soit causé et éviter que de nouveaux incidents de même nature ne se produisent, ce qui peut inclure la sanction des individus en cause.

La STL tient un registre des Incidents de confidentialité, dont le contenu est déterminé par la Loi sur l'accès.

12. ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE

La STL procède à une EFVP lorsque la Loi sur l'accès l'exige, incluant tout projet d'acquisition, de développement ou de refonte d'un système d'information ou d'une prestation électronique de services qui impliquerait la collecte, l'utilisation, la communication, la conservation ou la destruction de Renseignements personnels ainsi que toute communication de Renseignements personnels à l'extérieur du Québec ou le fait de confier à un tiers situé à l'extérieur du Québec la tâche de recueillir, d'utiliser, de communiquer ou de conserver des Renseignements personnels pour le compte de la STL, notamment pour de l'hébergement de données.

Les situations où la STL doit procéder à une EFVP sont plus amplement détaillées dans la Directive sur l'élaboration et l'approbation des évaluations des facteurs relatifs à la vie privée (ci-après la « Directive EFVP »).

L'EFVP doit être complétée conformément à la Directive EFVP, le tout en collaboration avec le Comité sur l'accès ainsi que le Responsable PRP.

13. UTILISATION DE L'IMAGE, DE LA VIDÉOSURVEILLANCE ET DE L'ENREGISTREMENT

La STL doit consulter le Comité sur l'accès quant aux mesures particulières à respecter en matière de protection des Renseignements personnels relativement à l'utilisation de l'image, à une technologie de vidéosurveillance ou à un enregistrement.

Dans l'élaboration des mesures en ces matières, le Comité sur l'accès évaluera notamment :

- La nécessité de recourir à une captation de l'image, à une technologie de vidéosurveillance ou à un enregistrement;
- Les mesures de protection à prendre à l'égard des Renseignements personnels recueillis ou utilisés lors de la captation de l'image, de l'usage d'une technologie de vidéosurveillance ou d'un enregistrement, que celui-ci soit réalisé par la STL ou par un tiers qui agit pour son compte;
- La conformité des règles entourant la captation de l'image ou de l'utilisation de ces technologies au droit au respect de la vie privée ainsi que la conservation et la destruction de celles-ci;

le tout en concordance avec les règlements et les politiques en vigueur à la STL, dont la Politique relative à la vidéosurveillance dans les véhicules, équipements et lieux publics de la Société de transport de Laval ainsi que la Directive sur la gestion de la vidéosurveillance sur les lieux de travail de la STL.

14. SONDAGE

La STL doit consulter le Comité sur l'accès sur les mesures particulières à respecter en matière de protection des Renseignements personnels relativement au sondage recueillant ou utilisant des Renseignements personnels.

Dans l'élaboration des mesures en cette matière, le Comité sur l'accès évaluera notamment :

- La nécessité de recourir au sondage;
- Les mesures de protection à prendre à l'égard des Renseignements personnels recueillis ou utilisés lors d'un sondage, que celui-ci soit réalisé par la STL ou par un tiers qui agit pour son compte;
- L'aspect éthique du sondage compte tenu, notamment, de la nature du sondage, des personnes visées, de la sensibilité des Renseignements personnels recueillis et de la finalité de l'utilisation de ceux-ci.

15. DÉCISION FONDÉE EXCLUSIVEMENT SUR UN TRAITEMENT AUTOMATISÉ DES RENSEIGNEMENTS PERSONNELS

Si la STL utilise des Renseignements personnels afin que soit rendue une décision fondée exclusivement sur un traitement automatisé de ceux-ci, elle doit, au moment de la décision ou avant, informer la personne concernée de cette décision.

Elle doit aussi, à la demande de la personne concernée, l'informer :

- Des Renseignements personnels utilisés pour rendre la décision;
- Des raisons, ainsi que des principaux facteurs et paramètres, ayant mené à la décision;
- De son droit de faire rectifier les Renseignements personnels utilisés pour rendre la décision.

16. ACTIVITÉS DE FORMATION ET DE SENSIBILISATION À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Le Comité sur l'accès met en place des activités de formation et de sensibilisation qu'il offre aux Employés en matière de protection des Renseignements personnels.

Un programme de sensibilisation à la protection des Renseignements personnels sera offert annuellement à tous les Employés, et ce de manière obligatoire pour les nouveaux Employés.

De l'information portant sur la protection des Renseignements personnels est mise à la disposition des Employés via l'intranet de la STL.

17. REDDITION DE COMPTES

Annuellement, le Responsable PRP dépose un bilan de ses activités et de celles du Comité sur l'accès au Directeur général dans le cadre d'une séance du comité de direction de la STL ainsi qu'au conseil d'administration de la STL ou à son comité Gouvernance, éthique et ressources humaines, ou toute autre instance remplaçant ces dernières.

18. MANQUEMENTS ET SANCTIONS

La Loi sur l'accès contient des dispositions pénales prévoyant que le non-respect de certaines obligations constitue une infraction passible d'une amende.

Plus précisément, tout Employé qui contrevient à la présente Politique, aux mesures de sécurité de l'information et de protection des Renseignements personnels qui en découlent ou au cadre légal sur lequel elles s'appuient, s'expose à des sanctions selon la nature, la gravité et les conséquences de la contravention.

19. DIFFUSION ET MISE À JOUR DE LA POLITIQUE

Le Responsable PRP, assisté du Comité sur l'accès, s'assure de la diffusion de la Politique et de ses mises à jour, notamment sur le site Web de la STL.

20. ENTRÉE EN VIGUEUR ET RÉVISION

La Politique de protection des renseignements personnels est approuvée par le Comité sur l'accès.

Dès son approbation par le conseil d'administration de la STL, elle entre en vigueur rétroactivement le 22 septembre 2023. Elle demeure en application tant et aussi longtemps qu'elle n'est pas abrogée, modifiée ou remplacée par une autre politique.

Elle est régulièrement évaluée par le Comité sur l'accès, notamment en ce qui a trait à la pertinence de ses énoncés à l'égard des nouveaux enjeux de protection des Renseignements personnels.