Politique de gestion

Titre : **Gouvernance de la protection des renseignements personnels**

Sujet : **Gestion de l'information**

Nº : **PG 5.11**

Approuvée par : Direction générale (DG-22-122)

1.0 CONTEXTE ET OBJECTIFS

En tant qu'organisme public, la STM 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 STM 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* (RLRQ, chapitre A-2.1), ci-après « la Loi ».

La présente politique a pour objectif d'établir la gouvernance de ses activités en cette matière et d'identifier les mesures à mettre en place pour accomplir ses devoirs envers les membres de son personnel et les citoyens.

2.0 DÉFINITIONS

Renseignement personnel :	Information qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier.
Incident de confidentialité :	Accès, utilisation ou communication non autorisé par la loi à un renseignement personnel, de même que sa perte ou toute autre forme d'atteinte à sa protection.
Évaluation des facteurs relatifs à la vie privée :	Démarche préventive qui vise à mieux protéger les renseignements personnels et à respecter davantage la vie privée des personnes physiques.

3.0 PORTÉE

La présente politique concerne la gouvernance de l'ensemble des renseignements personnels détenus par la STM 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 STM qui contiennent des renseignements personnels, quelles que soient leurs formes (écrites, graphiques, sonores, visuelles, informatisées ou autres).

4.0 RESPONSABLE

La personne occupant le poste de Secrétaire corporatif agit à titre de responsable auprès de la Commission d'accès à l'information en matière d'accès aux documents et de protection des renseignements personnels (ci-après « personne responsable »). Elle agit de manière autonome dans ce dossier. Elle exerce tous les pouvoirs nécessaires à l'application de la Loi. Les membres du personnel doivent collaborer avec elle pour répondre efficacement aux exigences qui y sont prévues.

5.0 COMITÉ SUR L'ACCÈS À L'INFORMATION ET LA PROTECTION DES RENSEIGNEMENTS PERSONNELS (ci-après « CAIPRP »)

La mise en place de ce comité vise à consolider la protection des renseignements personnels à la STM, à supporter l'harmonisation des pratiques dans ce domaine et à contribuer à la promotion d'une culture organisationnelle qui renforce la protection des renseignements personnels et qui favorise la transparence.

5.1 Mandat

Le comité a pour mandat :

- D'appuyer la personne responsable dans l'exercice de ses responsabilités et dans l'exécution de ses obligations énoncées dans la Loi;
- De proposer des orientations et des solutions concernant les principaux enjeux en matière de protection des renseignements personnels;
- Assure le suivi du registre des incidents de confidentialité et valide la grille de criticité permettant de les évaluer;
- D'examiner, selon le risque perçu, les incidents touchant la protection des renseignements personnels et de formuler des recommandations;
- D'étudier les règles de gouvernance à l'égard des renseignements personnels et de faire des recommandations aux instances qui en autorisent la mise en place;
- D'étudier l'évaluation des facteurs relatifs à la vie privée au début de tout projet d'acquisition ou de développement impliquant des renseignements personnels et d'émettre des recommandations concernant la mise en place de mesures particulières de protection des renseignements personnels aux instances qui les administrent;
- D'accomplir les autres fonctions habituellement dévolues à ce type de comité qui ont une incidence sur la protection des renseignements personnels et qui lui sont assignées par la personne responsable.
- D'informer le Comité de Gestion des Actifs et Ressources informationnels (ci-après GRAI) de toute situation, de tout événement, de tout projet ou de toute technologie pouvant avoir une incidence sur la protection des renseignements personnels et sur les actifs informatiques.

5.2 Composition

Le comité est composé des personnes suivantes :

- Secrétaire corporatif, qui y agit à titre de président et membre d'office.
- Au moins 2 membres du comité de direction élargi proposés par la ou le secrétaire corporatif et nommés par une demande d'autorisation à la direction générale.
- Gestionnaire de la direction – Affaires juridiques responsable de l'accès à l'information, qui y agit à titre de membre d'office ainsi qu'à titre de secrétaire.
- Gestionnaire responsable la Division – Sécurité et gestion des risques TI de la DE –Technologies de l'information et Innovation, qui y agit à titre de membre d'office.

- Gestionnaire responsable de la gestion de l'information au Secrétariat corporatif, qui y agit à titre de membre d'office.

5.3 Fonctionnement

Le comité se réunit minimalement 6 fois par année.

Le comité peut inviter toute personne ayant une expertise pertinente pour l'appuyer dans l'exécution de son mandat.

La création de tout sous-comité permanent visant à l'assister dans la réalisation de son mandat doit être approuvée par les membres du comité. Sous réserve de ce qui précède, la présidence du comité peut créer un sous-comité « ad hoc » portant sur des enjeux spécifiques découlant du mandat du comité pour des travaux s'échelonnant sur une période de moins d'une année.

6.0 MESURES VISANT LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Afin d'assurer la protection des renseignements personnels détenus par la STM, la personne responsable s'assure que des mesures sont en place ou que les démarches nécessaires soient lancées pour que celles-ci soient déployées dans les délais prévus à la Loi. Il s'agit notamment des éléments suivants :

- Un cadre administratif qui contrôle :
  - La cueillette, l'utilisation, la communication, la conservation, la diffusion, la portabilité des renseignements personnels;
  - Le traitement d'une demande d'accès à des renseignements personnels ou de rectification;
  - La gestion des incidents de confidentialité;
  - La vidéosurveillance;
  - La communication de renseignements personnels dans le cadre d'un processus contractuel.
  - Les projets de développement ou de mise à jour des actifs informatiques (ou de prestation électronique) impliquant des renseignements personnels.
- Un plan de communication visant à sensibiliser les membres du personnel, les citoyennes ou les citoyens en leur faisant connaître et en leur expliquant :
  - les règles de confidentialité pour les utilisateurs des médias électroniques;
  - les encadrements sur la protection des renseignements personnels;
  - les moyens pour contacter les responsables de la protection des renseignements personnels.
- Un plan de formation et de sensibilisation des membres du personnel utilisant des renseignements personnels.
- Un processus de consentement conforme aux exigences juridiques en matière de renseignements personnels.
- Un processus de gestion des renseignements personnels sensibles.

7.0 REDDITION DE COMPTES

Annuellement, la personne responsable dépose un bilan de ses activités et de celles du CAIPRP à la directrice ou au directeur général dans le cadre d'une séance du comité de direction.

8.0 RESPONSABILITÉS

Secrétaire corporatif

- Assurer la mise en œuvre, le suivi et la mise à jour de la présente politique;

- Voir à l'application de la *Loi sur les archives* (RLRQ., c.A-21.1), de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ., c.A-2.1) et de la présente politique;
- Tient le registre des incidents de confidentialité prévu à la Loi et informe le CAIRP des événements qui y sont consignés.

Direction exécutive - Technologies de l'Information et Innovation

- Gérer et sécuriser les actifs informatiques de la STM contenant des renseignements personnels;
- Mettre en place des moyens raisonnables afin de procéder à la détection et au traitement des incidents de confidentialité de nature technologique, notamment par l'automatisation;
- Informer la personne responsable du Secrétariat corporatif des incidents de confidentialité pour qu'ils soient consignés dans un registre;
- Assurer l'évolution des actifs informatiques dans le respect des obligations liées à la protection des renseignements personnels.

Membres du comité de direction élargi

- Mettre en place des moyens raisonnables visant à s'assurer que les renseignements personnels sous leur responsabilité sont collectés, conservés, sécurisés et utilisés dans le respect des encadrements applicables (notamment, les lois, les politiques et les directives);
- Déclarer les incidents de confidentialité portés à leur connaissance au responsable du registre des incidents de confidentialité du Secrétariat corporatif.

9.0 RÉFÉRENCES

- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ., c.A-2.1)*
- *Loi sur les archives (RLRQ, c.A-21.1)*
- *Loi sur les sociétés de transport en commun (RLRQ, c. S-30.01)*

HISTORIQUE

Adoption : 19-06-2022

Contact pour révision – 2026