

Titre : **Gouvernance des ressources et actifs informationnels**Sujet : **Gestion de l'information**

Approuvée par : Directeur général (DADG-18-376)

*L'utilisation du genre masculin n'a pour but que l'allègement du texte*No : **PG 5.01**Page : **1** de **9**Nouvelle : **X** Révisée :

Date : 17 décembre 2018

1.0 ÉNONCÉ

La présente politique définit la gouvernance des ressources et des actifs informationnels de la Société.

Elle repose sur trois piliers d'intervention soit : la « Gestion de l'information », la « Protection de l'information » et la « Cybersécurité ». Ces derniers sont définis dans la politique corporative « Gestion des ressources et actifs informationnels » (PC 5.01).

Pour chacun de ceux-ci, elle établit des contrôles, des mécanismes ou des mesures de protection permettant une exploitation efficace, optimale et sécuritaire dans le respect du cadre juridique en vigueur, notamment la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ., c.A-2.1). Ces éléments sont développés en fonction du niveau de tolérance aux risques de la Société, conformément au processus découlant de la politique corporative « Gestion intégrée des risques » (PC1.17).

Cette politique a pour objectif de mettre en place un encadrement rigoureux de la gestion de ses ressources et actifs informationnels. Elle vise à en assurer l'intégrité, la confidentialité, la disponibilité, la divulgation, la conservation et la disposition.

2.0 PORTÉE

La présente politique s'adresse à toute personne participant à la gestion, l'encadrement ou l'utilisation des ressources et actifs informationnels de la Société.

3.0 DÉFINITIONS

Actif informationnel :	Tout support physique ou virtuel « contenant » des ressources informationnelles. Il s'agit notamment d'un document étant constitué d'information, de système d'information, de matériel informatique, de logiciel, de progiciel, de média informatique, de système de courrier électronique. Il peut s'agir aussi de matériel de télécommunication, d'un système de messagerie vocale, d'un support papier ou d'une microforme.
Actif informatique :	Tout actif informationnel sous format informatique ou électronique. Il s'agit notamment d'un logiciel, d'un poste de travail, d'un téléphone portable, de l'infrastructure technologique.
Calendrier de conservation :	Le calendrier de conservation est un regroupement de règles comprenant la description, des actifs informationnels, leur utilisation, leur période de conservation, leur caractère confidentiel ainsi que leur disposition finale (conservation, élimination, tri et échantillonnage). On y retrouve aussi les rôles et responsabilités du détenteur principal et secondaire(s) des exemplaires d'un même actif.
Document essentiel :	Un actif informationnel sous forme de document indispensable au fonctionnement d'un organisme et qui assure la continuité de celui-ci à la suite d'un désastre.
Plan de classification :	Le plan de classification est un outil qui permet le regroupement des actifs informationnels selon un ordre logique afin de rendre l'information accessible rapidement. Il permet de classer les actifs informationnels en quelques étapes simples.
Renseignement personnel :	Ressource informationnelle qui concerne une personne physique et permet de l'identifier.

Titre : **Gouvernance des ressources et actifs informationnels**Sujet : **Gestion de l'information**

Approuvée par : Directeur général (DADG-18-376)

*L'utilisation du genre masculin n'a pour but que l'allègement du texte*No : **PG 5.01**Page : **2** de **9**Nouvelle : **X** Révisée :

Date : 17 décembre 2018

Ressource informationnelle : Information produite ou reçue dans le cadre des activités de la Société sous forme textuelle, sonore, symbolique ou visuelle. Il s'agit notamment du « contenu » d'une banque de données, d'une information consignée par écrit sur un document papier ou verbalement dans une boîte vocale.

Utilisateur : Toute personne qui travaille pour le compte de la Société à temps plein, à temps partiel, de façon occasionnelle ou contractuelle. Ceci comprend également toute personne externe à la Société qui utilise, garde ou accède aux ressources et actifs informationnels de même qu'aux actifs informatiques de la Société.

4.0 PRINCIPES

La gouvernance des ressources et actifs informationnels de la Société repose sur les principes suivants :

- La Société a le droit de regard exclusif sur la gestion de ses ressources et actifs informationnels.
- La STM adhère d'emblée à la nécessité de protéger la confidentialité des renseignements personnels qu'elle détient et au droit à la vie privée de ses employés.
- La Société doit procéder à la vérification de la saine gouvernance de ses ressources et actifs informationnels.
- Les ressources informationnelles doivent être identifiées et être l'objet de mesures de protection selon leur classification basée sur la disponibilité, l'intégrité de l'information ainsi que la confidentialité de l'information.

Les principes susmentionnés s'appliquent autant à la gestion de l'information, à la protection de l'information et à la cybersécurité.

5.0 GESTION DE L'INFORMATION

5.1 Classification de l'information

L'information doit être classifiée selon les impacts potentiels d'une perte de disponibilité, d'intégrité ou de confidentialité d'une ressource informationnelle. Les contrôles et mesures de protection doivent être appliqués selon la nature des impacts potentiels en cas de perte ou de compromission de la ressource informationnelle.

5.2 Renseignements personnels

Au sens de *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ., c.A-2.1), seuls les renseignements personnels nécessaires aux opérations de l'entreprise peuvent être recueillis et détenus à la STM ou par des tiers mandatés par elle. Les renseignements personnels ne doivent être utilisés qu'aux seules fins prévues lors de leur cueillette.

5.2.1 Accès aux renseignements personnels

- L'accès aux renseignements personnels détenus par la Société n'est accordé qu'aux utilisateurs dont l'exercice des responsabilités le requiert et le justifie. Ceux-ci s'engagent alors à traiter ces renseignements de manière à en assurer la confidentialité. Des contrôles et mécanismes de gestion d'accès doivent être mis en place afin d'en assurer la protection.

Titre : **Gouvernance des ressources et actifs informationnels**Sujet : **Gestion de l'information**

Approuvée par : Directeur général (DADG-18-376)

*L'utilisation du genre masculin n'a pour but que l'allègement du texte*No : **PG 5.01**Page : **3** de **9**Nouvelle : **X** Révisée :

Date : 17 décembre 2018

5.2.2 Communication de renseignements personnels à des tiers

- La communication de renseignements personnels à des tiers peut seulement être autorisée par le Secrétaire corporatif selon ses modalités.
- Le caractère sensible des renseignements personnels doit prévoir des mécanismes de protection appropriés lors de la transmission de cette information.

5.2.3 Conservation des renseignements personnels

- Les renseignements personnels détenus par la Société ne sont conservés que pour la durée et les fins pour lesquelles ils ont été recueillis, dans le respect des délais imposés par les lois en vigueur et conformément au Calendrier des délais de conservation des documents de la STM.
- Les renseignements personnels détenus par la STM ou par des tiers doivent être protégés comme ils le seraient par la STM.
- Les utilisateurs de la STM ne doivent pas transporter des actifs informationnels contenant des renseignements personnels hors installations des STM.

5.2.4 Destruction des renseignements personnels

- La destruction des renseignements personnels doit être réalisée de manière à assurer la protection de leur nature sensible. La disposition de tout actif informationnel contenant des renseignements personnels doit, dans tous les cas, être effectuée de façon sécuritaire.

5.2.5 Import de renseignements personnels à partir des actifs informatiques de la Société

- Seuls les utilisateurs autorisés à cette fin peuvent importer, à partir des systèmes d'information de la Société, des données nécessaires à l'exécution de leur travail. Le cas échéant, l'utilisateur concerné a la responsabilité de protéger, par des moyens adéquats, l'accès aux renseignements personnels qu'il a importés.

5.3 Calendrier de conservation

Le calendrier de conservation est l'outil qui détermine le temps de conservation d'un actif informationnel et qui renseigne sur sa disposition finale. Il comprend sa description, son utilisation, l'unité responsable, la période de conservation en plus d'indiquer son niveau de confidentialité, la présence de renseignements personnels ainsi que son caractère essentiel.

5.3.1 Disposition et destruction

- Tout actif informationnel doit être disposé ou détruit de façon sécuritaire à la fin de la vie utile de cet actif, et ce, selon la nature des ressources informationnelles contenues sur l'actif.

5.3.2 Archivage

- L'archivage de toute ressource informationnelle doit respecter les lois en vigueur conformément au Calendrier des délais de conservation des documents de la Société.

5.4 Ouverture des données

Selon les consignes de la *PC 5.09 – Données ouvertes*, toute donnée collectée ou acquise par la Société est considérée comme ouverte à moins d'une justification pertinente pour en restreindre l'accès. Ces

Titre : **Gouvernance des ressources et actifs informationnels**Sujet : **Gestion de l'information**

Approuvée par : Directeur général (DADG-18-376)

*L'utilisation du genre masculin n'a pour but que l'allègement du texte*No : **PG 5.01**Page : **4** de **9**Nouvelle : **X** Révisée :

Date : 17 décembre 2018

données ne doivent pas porter préjudice à des individus ou à la Société et doivent être conformes à toute loi ou règlement en vigueur.

5.5 Accès à l'information

Toute demande d'accès à de l'information formulée par des tiers doit être adressée au « Secrétariat corporatif et direction - Affaires juridiques ». Tout comme les demandes d'accès, la communication de renseignements personnels doit être explicitement autorisée en conformité avec les dispositions de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ., c.A-2.1).

Il est interdit de communiquer à des tiers, sans l'autorisation requise, des informations détenues par la Société si ces informations peuvent porter atteinte et préjudice à cette dernière.

5.6 Registre des déclarations de données

Une déclaration de données doit être produite pour tout nouveau regroupement d'actifs informatiques stockant, traitant ou transmettant des renseignements personnels ou des renseignements confidentiels.

Pour ces regroupements, toute règle de création, utilisation, disposition, destruction, archivage d'une ressource informationnelle doit être explicitée dans une déclaration de données et en conformité avec le calendrier de conservation. Cette déclaration doit être ajoutée au registre des déclarations de données.

6.0 PROTECTION DE L'INFORMATION

6.1 Habilitation de sécurité

Les utilisateurs doivent faire preuve de loyauté et d'intégrité professionnelle dans le cadre de l'utilisation des ressources informationnelles dans le poste occupé.

Un cadre de gestion des habilitations de sécurité des utilisateurs doit être mis en place. Il devra déterminer les règles et procédures à suivre en matière de gestion du personnel. Notamment, toute description d'un poste doit inclure des critères généraux d'évaluation de sécurité des utilisateurs.

6.2 Protection physique et environnementale

Des mesures particulières de protection physique s'appliquent à toutes les installations de la STM. Entre autres, des contrôles d'accès doivent être en place aux points d'entrées afin de sécuriser les locaux.

Une maintenance des équipements et actifs informatiques doit être effectuée afin de prévenir des bris, pannes et de voir à la destruction sécuritaire de ces actifs.

Pour protéger adéquatement les actifs informationnels, des conditions environnementales favorables doivent être en place. Ceci inclut la climatisation, le chauffage, la filtration de l'air, les autres contrôles et les mécanismes environnementaux.

Des mesures particulières de protection doivent être définies et appliquées aux centres de données de la Société.

Titre : Gouvernance des ressources et actifs informationnels**Sujet : Gestion de l'information****Approuvée par : Directeur général (DADG-18-376)***L'utilisation du genre masculin n'a pour but que l'allègement du texte***No : PG 5.01****Page : 5 de 9****Nouvelle : X Révisée :****Date : 17 décembre 2018**

6.3 Sensibilisation à la sécurité

La sensibilisation à la protection de l'information est obligatoire à la Société. Une sensibilisation adéquate permet de réduire considérablement les comportements à risques des utilisateurs. Plusieurs activités de sensibilisation à la protection de l'information sont offertes à chaque utilisateur en fonction de ses fonctions dans l'entreprise.

6.4 Incidents de sécurité de l'information

Afin de minimiser son exposition à des risques potentiels et des impacts subséquents, la Société doit se doter d'un cadre de gestion d'incidents de sécurité de l'information.

La tentative ou la réussite de tout accès non autorisé d'un actif informatique géré par la Société à quelque fin que ce soit présente un incident potentiel de sécurité de l'information.

Tout employé est invité à déclarer tout potentiel d'incident de sécurité de l'information, résultant d'une tentative de compromission réussie ou non. Toute déclaration sera traitée avec diligence et confidentialité.

7.0 CYBERSÉCURITÉ

7.1 Contextualisation des actifs informationnels

Une multitude d'actifs informationnels sont des actifs informatiques. Des contrôles et mesures de protection particuliers sont nécessaires pour contrer les menaces de cybersécurité.

Les mécanismes de protection des actifs informationnels peuvent varier selon le contexte d'utilisation de ces derniers et en fonction des menaces et des risques. Les contrôles et mécanismes de protection en place doivent être variés et appropriés selon les risques attendus.

7.2 Utilisation des actifs informatiques

Afin de minimiser ses risques, la Société favorise l'encadrement rigoureux de l'utilisation de ses actifs informatiques, notamment les postes informatiques et les appareils intelligents de ses utilisateurs. La Société considère ces actifs comme des outils de travail qu'elle met à la disposition de ses employés pour favoriser l'accomplissement de leurs tâches. L'utilisation des actifs informatiques doit ainsi être exercée de façon raisonnable par les seuls utilisateurs autorisés par la Société et uniquement à l'intérieur des limites fixées par elle.

Tout actif informatique pouvant être laissé sans surveillance doit être sécurisé physiquement.

Toute installation ou désinstallation, tout déplacement, toute correction, toute mise à jour apportés à des actifs informatiques, dont des logiciels, à des applications particulières ou aux équipements doit être réalisé selon les processus établis par la Société.

7.3 Gestion des accès informatiques

Tout accès aux actifs informatiques de la Société, internes ou externes, doit être effectué en utilisant les routes, moyens et mécanismes informatiques prescrits par la Société. Le contournement des contrôles et des mécanismes de sécurité mis en place pour protéger les actifs informatiques de la Société est strictement interdit.

Titre : Gouvernance des ressources et actifs informationnels**Sujet : Gestion de l'information****Approuvée par : Directeur général (DADG-18-376)***L'utilisation du genre masculin n'a pour but que l'allègement du texte***No : PG 5.01****Page : 6 de 9****Nouvelle : X Révisée :****Date : 17 décembre 2018**

À l'obtention d'un code d'accès et suite à la détermination d'un mot de passe, chaque utilisateur devient responsable des activités effectuées sur les actifs informatiques en son nom. Tout usage non autorisé des codes d'accès et des mots de passe doit être signalé aux autorités compétentes sans délai.

7.4 Sécurité dans l'exploitation des technologies

L'exploitation des technologies doit être effectuée en minimisant les risques de cybersécurité pour la Société. Des contrôles et mécanismes de protection doivent être en place sur les actifs informatiques. Ces contrôles incluent, sans s'y limiter : la documentation et le maintien des procédures d'exploitation TI, la mise en place d'une gestion des changements, le bastionnage des actifs informatiques, la mise en place d'un inventaire pour retracer les actifs informatiques, la mise en place de pare-feu et la gestion des vulnérabilités technologiques.

Ces contrôles et mécanismes doivent être mis en place proportionnellement à la menace, réelle ou anticipée en incluant une analyse d'impacts.

7.5 Développement sécuritaire

Un cadre de développement sécuritaire doit être mis en place et être suivi par les développeurs.

Ce cadre comprend des pratiques de programmation reconnues comme sécuritaires dans développement informatique qui doivent être utilisées pour les logiciels ayant des renseignements personnels, confidentiels ou en fonction des risques pour l'entreprise.

Des audits et tests d'intrusion doivent également être effectués pour ces actifs informatiques à risque avant un déploiement et ultimement de son utilisation.

Une formation en cybersécurité est obligatoire pour tout personnel développant des applications.

7.6 Sécurité des tiers

Des clauses de gestion de l'information, protection de l'information et de cybersécurité doivent être intégrées dans chaque contrat avec des tiers en fonction des risques associés, qu'ils s'agissent d'une autre société de transport, d'un fournisseur, etc. Ces clauses sont des contrôles de sécurité permettant d'assurer une gestion équivalente de ce qu'il se ferait à la Société.

Tout contrat avec un tiers doit également inclure des clauses permettant à la Société d'établir la conformité aux contrôles de sécurité par le tiers, d'en assurer le suivi et le maintien, ainsi qu'exiger la remise aux normes du tiers en cas de manquements aux clauses contractuelles.

7.7 Continuité informatique

Un cadre de gestion de la continuité informatique doit être en place pour assurer la disponibilité et la qualité des services informatiques offerts. Ce cadre doit également inclure la détermination de la criticité des actifs informatiques ainsi que les niveaux de services. Un plan de continuité informatique doit être mis en place pour chacune des catégories d'actifs informatiques. De plus, ces plans doivent être testés et mis à jour selon le cadre de gestion.

Titre : **Gouvernance des ressources et actifs informationnels**Sujet : **Gestion de l'information**

Approuvée par : Directeur général (DADG-18-376)

*L'utilisation du genre masculin n'a pour but que l'allègement du texte*No : **PG 5.01**Page : **7** de **9**Nouvelle : **X** Révisée :

Date : 17 décembre 2018

7.8 Acquisition d'actifs informatiques

L'acquisition d'actifs informatiques ainsi que de services en infonuagiques doit être centralisée. Ceci est pour s'assurer d'une saine gouvernance en gestion des actifs informatiques de même que pour assurer la sécurisation adéquate de chacun des actifs acquis.

Seule la DE TII a l'autorité dans l'entreprise d'acquérir, de configurer, de déployer et de rendre disponibles aux utilisateurs des actifs informatiques, incluant des services informatiques en infonuagique ou fournis par des tiers.

8.0 RESPONSABILITÉS**Direction exécutive - Technologies de l'Information et Innovation**

- assumer la responsabilité de la présente politique, de son application, de son interprétation, de son suivi et de sa mise à jour à titre de propriétaire de ce document;
- définir le processus de gestion et d'approbation de risques en lien avec la gestion des ressources et actifs informationnels;
- maintenir les modalités de partage des ressources et actifs informationnels;
- mettre en place et assurer une saine gestion des contrôles et mécanismes relatifs à la sensibilité des actifs informatiques;
- procéder à la sensibilisation des utilisateurs concernant la protection des ressources et actifs informationnels;
- mettre en place un cadre de développement sécuritaire pour ses actifs informatiques;
- définir les contrôles de sécurité pour les ententes contractuelles avec les tierces parties (exemples : partenaires transports, fournisseurs externes);
- auditer les tierces parties pour le volet sécurité, selon le risque établi;
- définir le cadre de gestion des accès informatiques de ses actifs;
- définir le cadre de gestion des incidents de sécurité de l'information, en incluant l'analyse des incidents, le recueil des évidences, les mécanismes de prise de décision et les post mortem d'incidents;
- définir un cadre de gestion de continuité informatique pour tous ses actifs informatiques;
- établir ses exigences dans la mise en place et l'exploitation des centres de données;
- assurer la saine gestion des contrôles et des mécanismes appropriés relatifs à la protection des actifs informatiques; et
- exploiter et maintenir les actifs informatiques de la Société.

Secrétaire corporatif

- fournir les principes de gestion de l'information et de protection de l'information selon les lois et réglementation en vigueur;
- s'assurer de l'application de la *Loi sur les archives* (RLRQ., c.A-21.1) et la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ., c.A-2.1);

Titre : Gouvernance des ressources et actifs informationnels**Sujet : Gestion de l'information****Approuvée par : Directeur général (DADG-18-376)***L'utilisation du genre masculin n'a pour but que l'allègement du texte***No : PG 5.01****Page : 8 de 9****Nouvelle : X Révisée :****Date : 17 décembre 2018**

- conseiller les unités administratives en matière de gestion de l'information;
- établir le cadre de gestion des demandes d'accès à l'information;
- établir le cadre de gestion documentaire, incluant les documents essentiels;
- établir la classification des ressources informationnelles;
- maintenir le calendrier des délais de conservation des documents;
- maintenir le registre des déclarations de données des actifs informatiques; et
- coordonner les activités relatives à la gestion de l'information.

Comité de Gestion des Actifs et Ressources Informationnels

- appuyer le Directeur général dans la surveillance et la gestion des actifs et ressources informationnelles à l'échelle de la Société (ci-après GRAI);
- proposer les orientations sur les principaux enjeux liés à la GRAI de la Société;
- planifier les activités concernant les orientations et stratégies reliées à la GRAI;
- émettre des recommandations quant à l'adoption du cadre documentaire (politiques, directives, règles, etc.) de GRAI;
- effectuer un suivi sur le respect du cadre documentaire de GRAI;
- effectuer le suivi sur l'évolution des risques liés à la GRAI pour l'ensemble de la Société dans le respect
- du niveau de tolérance aux risques; et
- examiner les principaux incidents touchants la GRAI survenus mondialement dans le domaine du transport et formuler des recommandations.

Direction exécutive - Capital humain, Approvisionnement et Affaires juridiques

- fournir les documents pertinents à cette politique à l'embauche de tout nouvel employé; et
- établir le cadre de gestion des habilitations de sécurité.

Direction exécutive - Métro / Direction - Sûreté et Contrôle de la DE

- établir le cadre de gestion des contrôles d'accès des installations de la Société;
- assurer la sécurité physique et environnementale des actifs informationnels dans les immeubles, et
- assurer la sûreté des utilisateurs.

Gestionnaire

- distribuer, respecter ainsi que voir à l'application de la présente politique auprès des utilisateurs sous sa gouverne et de maintenir leur compréhension;
- autoriser l'accès aux actifs informatiques des utilisateurs sous sa gouverne;
- autoriser, pour chacun de ses employés, la fourniture des actifs informatiques requis pour l'exercice de ses fonctions ainsi que les privilèges d'accès aux actifs;

Titre : Gouvernance des ressources et actifs informationnels**Sujet : Gestion de l'information****Approuvée par : Directeur général (DADG-18-376)***L'utilisation du genre masculin n'a pour but que l'allègement du texte***No : PG 5.01****Page : 9 de 9****Nouvelle : X Révisée :****Date : 17 décembre 2018**

- voir au retrait ou à la modification des privilèges d'accès dès qu'un utilisateur sous sa gouverne voit ses responsabilités modifiées, qu'il change de poste ou qu'il quitte l'entreprise; et
- appliquer les mesures disciplinaires appropriées, le cas échéant.

Utilisateur

- gérer et utiliser adéquatement les actifs informatiques mis à sa disposition par la Société dans le cadre de son travail;
- assurer la confidentialité des ressources informationnelles ayant une nature sensible ou confidentielle en prenant les mesures de protection appropriées lors du stockage, du traitement et de la transmission de ses ressources;
- restreindre la communication de ses codes d'accès, mots de passe ou tout autre mécanisme d'identification, incluant sa carte d'accès.

9.0 RÉFÉRENCES

- PC 1.17 – Gestion intégrée des risques
- PC 5.01 – Gestion des ressources et actifs informationnels
- PC 5.09 – Données ouvertes

10.0 ABROGATION

La présente politique remplace et abroge les politiques de gestion suivantes :

- PG 5.07 – Acquisition et accès à des sources externes de documentation
- PG 5.08 – Protection des renseignements personnels
- D 5.03 – Gestion des documents

Historique : -Adoption : 2018-12-17

- Révision suggérée : 2023