Ministère du Tourisme
Québec

POLITIQUE MINISTÉRIELLE DE LA SÉCURITÉ DE L'INFORMATION

MINISTÈRE DU TOURISME
900, boulevard René-Lévesque Est
Québec (Québec) G1R 2B5
Téléphone : 418 643-5959
www.tourisme.gouv.qc.ca

Dans le présent document, le générique masculin est utilisé sans aucune discrimination et uniquement dans le but d'alléger le texte.

POLITIQUE MINISTÉRIELLE DE LA SÉCURITÉ DE L'INFORMATION

TABLE DES MATIÈRES

CONTEXTE

Le ministère du Tourisme (Ministère) a pour mission de soutenir le développement et la promotion du tourisme au Québec, en favorisant la concertation et le partenariat des intervenants associés à ce développement et à cette promotion, et ce, dans une perspective de création d'emplois, de prospérité économique et de développement durable.

Dans le cadre de ses mandats, le Ministère doit produire et détenir des documents qui revêtent un caractère économique, stratégique et confidentiel. Il se doit donc de mettre en place les mesures de sécurité nécessaires, afin d'assurer une protection adéquate de l'information relevant de son autorité.

La présente politique est adoptée en application du paragraphe a) de l'article 7 de la *Directive sur la sécurité de l'information gouvernementale* (Décret 7-2014 du 15 janvier 2014) qui stipule que le sous-ministre doit notamment, en prenant appui sur les orientations et les bonnes pratiques en matière de sécurité de l'information, adopter et mettre en œuvre une politique de sécurité de l'information, la maintenir à jour et assurer son application.

La définition des différents termes utilisés dans cette politique est consignée dans le Glossaire de la sécurité de l'information du Ministère

1. OBJET DE LA POLITIQUE MINISTÉRIELLE DE LA SÉCURITÉ DE L'INFORMATION

La présente politique a pour objectif de renforcer le cadre de gestion et d'affirmer l'engagement du Ministère à s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information, quel que soit son support ou son moyen de communication. Plus précisément, il s'agit d'assurer la disponibilité, l'intégrité et la confidentialité de l'information tout au long de son cycle de vie. La présente politique a également pour objet de définir les rôles et les responsabilités des intervenants dans le but d'assurer la sécurité des actifs informationnels.

Enfin, elle s'applique à tout le personnel[1] du Ministère.

2. CADRE LÉGAL ET ADMINISTRATIF

Le cadre juridique de cette politique s'appuie sur les lois, règlements, directives et politiques en vigueur au Québec, notamment :

- Loi canadienne sur les droits de la personne, L.R.C. (1985), chapitre H-6;
- Code criminel, L.R.C (1985) chapitre C-46;
- Loi sur le droit d'auteur, L.R.C. (1985), chapitre C-42;
- Charte des droits et libertés de la personne, RLRQ, chapitre C-12;
- Code civil du Québec;
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ, chapitre A-2.1;
    - Règlement sur la diffusion de l'information et sur la protection des renseignements personnels, chapitre A-2.1, r. 2;
- Loi sur l'administration publique, RLRQ, chapitre A-6.01;
- Loi sur les archives, RLRQ, chapitre A-21.1;

[1] Le personnel inclut les employés du Ministère, les consultants et les stagiaires.

- Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques, chapitre A-21.1, r. 2;

- Loi concernant le cadre juridique des technologies et l'information, RLRQ, chapitre C-1.1;
- Loi sur la fonction publique, RLRQ, chapitre F-3.1.1;
- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, RLRQ, chapitre G-1.03;
- Loi sur le ministère du Tourisme, RLRQ, chapitre M-31.2;
- Directive sur la sécurité de l'information gouvernementale, Décret 7-2014 du 15 janvier 2014;
- Directive sur l'utilisation éthique du courriel, d'un collecticiel et des services d'Internet par le personnel de la fonction publique, C.T. 198872 du 1er octobre 2002;
- Directive sur les services de certification offerts par le gouvernement du Québec, Décret 6-2014 du 15 janvier 2014;
- Directive concernant le traitement et la destruction de tout renseignement, registre, donnée, logiciel, système d'exploitation ou autre bien protégé par un droit d'auteur, emmagasiné sur un équipement micro-informatique ou sur un support informatique amovible, C.T. 193953 du 19 octobre 1999 modifié par le C.T. 199891 du 27 mai 2003;
- Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics, Décret 261-2012 du 28 mars 2012.

3. PRINCIPES DIRECTEURS

Les actifs informationnels sont essentiels aux opérations courantes et doivent faire l'objet d'une utilisation et d'une protection adéquates. Ainsi, les mesures de sécurité doivent être proportionnelles à la valeur de l'information à protéger. Elles sont établies en fonction des risques, de leur probabilité d'occurrence et de leurs conséquences. Tous les actifs informationnels peuvent faire l'objet de mesures de surveillance et de contrôle, y compris l'information qui est propre à un employé et qui est conservée au moyen des technologies de l'information du Ministère.

Cette politique s'applique à tous les actifs informationnels appartenant au Ministère, que ce soit dans ses locaux ou ailleurs.

Elle s'applique également, dans la mesure prévue dans leur contrat ou entente, à tout consultant, partenaire, fournisseur ou personne qui utilise ou détient des actifs informationnels appartenant au Ministère, que ceux-ci soient situés dans les locaux du Ministère ou ailleurs. Elle peut aussi s'appliquer, dans certains cas et sous réserve de leur contrat ou entente, à un consultant, à un mandataire, à un partenaire, à un fournisseur ou à une autre personne qui utilise ses propres actifs informationnels pour exécuter des activités à la demande du Ministère.

Plus particulièrement, ces mesures visent à :

- assurer la disponibilité de l'information de façon à ce qu'elle soit accessible en temps voulu et de la manière requise par une personne autorisée;
- assurer l'intégrité de l'information de manière à ce que celle-ci ne soit pas détruite ou altérée de quelque façon sans autorisation, et que le support de cette information lui procure la stabilité et la pérennité voulues;
- limiter la divulgation de l'information aux seules personnes autorisées à en prendre connaissance, assurant ainsi une stricte confidentialité.

4. PRINCIPES GÉNÉRAUX

4.1 PROTECTION DE L'INFORMATION

Le Ministère adhère aux orientations et objectifs stratégiques gouvernementaux en matière de sécurité de l'information et s'engage à ce que les pratiques et les solutions retenues en la matière correspondent, dans la mesure du possible, à des façons de faire reconnues et généralement utilisées à l'échelle gouvernementale, nationale et internationale.

Le Ministère reconnaît que les actifs informationnels qu'il détient sont essentiels à ses activités courantes et, de ce fait, doivent faire l'objet d'une évaluation constante, d'une utilisation appropriée et d'une protection adéquate.

La sécurité des actifs informationnels du Ministère est soutenue par une démarche d'éthique visant à favoriser la régulation des conduites et la responsabilisation individuelle.

4.2 PROTECTION DES RENSEIGNEMENTS PERSONNELS

Toute information confidentielle doit être préservée d'une divulgation ou d'une utilisation non autorisée, et son accès doit être restreint aux seules personnes y ayant droit.

Sont notamment considérés confidentiels, au sens de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (art. 53), les renseignements personnels ainsi que tout renseignement dont la divulgation aurait des incidences, notamment sur l'image, l'intégrité et la crédibilité du Ministère, les relations intergouvernementales, les négociations entre organismes publics, l'économie, les tiers relativement à leurs renseignements industriels, financiers, commerciaux, scientifiques ou techniques, l'administration de la justice et la sécurité publique, les décisions administratives ou politiques et la vérification.

4.3 SENSIBILISATION ET FORMATION

Le Ministère s'engage, sur une base périodique, à sensibiliser et à former les utilisateurs à la sécurité des actifs informationnels, aux conséquences d'une atteinte à leur sécurité ainsi qu'à leur rôle et à leurs obligations en cette matière.

4.4 HABILITATION DE SÉCURITÉ

S'il le juge opportun, le Ministère peut demander qu'une enquête de sécurité soit réalisée pour toute personne qui aura accès aux actifs informationnels visés par la politique. L'habilitation de sécurité doit être consentie, par écrit, par la personne concernée et être effectuée dans le respect des personnes, des lois, des règlements, des politiques et des conventions collectives en vigueur. Les résultats de l'enquête de sécurité appartiennent et sont conservés par le Ministère.

4.5 DROIT DE REGARD

Le Ministère exerce, en conformité avec la législation et la réglementation en vigueur, un droit de regard sur tout usage de ses actifs informationnels.

5. RÔLES ET RESPONSABILITÉS

L'ensemble des rôles et responsabilités des divers intervenants ainsi que les structures internes de concertation et de coordination en matière de sécurité de l'information sont définis dans le Cadre de gestion de la sécurité de l'information du Ministère, en complément à la présente politique.

6. OBLIGATIONS DES UTILISATEURS

Tout utilisateur a l'obligation de protéger les actifs informationnels mis à sa disposition par le Ministère. À cette fin, il doit :

- prendre connaissance de la *Directive sur l'utilisation des actifs informationnels*, y adhérer et prendre l'engagement de s'y conformer;
- utiliser les actifs informationnels mis à sa disposition en se limitant aux fins auxquelles ils sont destinés, uniquement lorsqu'ils sont nécessaires à l'exercice de ses fonctions et en respectant les droits d'accès qui lui sont attribués;
- respecter les mesures de sécurité mises en place pour protéger les actifs informationnels, quel qu'en soit le support, sans essayer de les contourner ou de les modifier;
- se conformer aux exigences légales portant sur l'utilisation de produits (logiciels, progiciels, applications) ou de documents à l'égard desquels des droits de propriété intellectuelle pourraient exister;
- signaler à son supérieur immédiat, dès qu'il en a connaissance, tout acte susceptible de constituer une violation réelle ou présumée des règles de sécurité ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels du Ministère;
- au moment de son départ du Ministère, remettre les différentes cartes d'identité et d'accès, les actifs informationnels quel qu'en soit le support, ainsi que tout l'équipement informatique ou de téléphonie mis à sa disposition dans le cadre de ses fonctions. L'utilisateur d'actifs informationnels peut toutefois faire une demande à la DRI pour lui rendre disponibles certains renseignements de nature personnelle. La transmission de ceux-ci sera alors convenue dans le cadre d'un engagement de confidentialité joint en annexe.

7. SANCTIONS

Lorsqu'un utilisateur contrevient à la présente politique ou aux directives en découlant, il s'expose à des mesures disciplinaires, administratives ou légales, en fonction de la gravité de son geste et de ses conséquences. Ces mesures peuvent inclure la suspension des privilèges, la réprimande, la suspension, le congédiement ou toute autre mesure disciplinaire, et ce, conformément aux dispositions des lois applicables, des conventions collectives, des ententes ou des contrats.

Le Ministère peut transmettre à toute autorité judiciaire les renseignements colligés qui le portent à croire qu'une infraction à une loi ou à un règlement en vigueur a été commise.

8. DISPOSITIONS FINALES

La présente Politique ministérielle de la sécurité de l'information remplace la Politique de sécurité de l'information et de protection des renseignements personnels approuvée par la sous-ministre associée le 20 février 2013.

Le responsable organisationnel de la sécurité de l'information s'assure de la mise en œuvre des dispositions de la présente politique et de ses directives d'application.

La présente politique doit être révisée à l'occasion de changements significatifs qui pourraient l'affecter.

La présente politique est complétée par le cadre de gestion de la sécurité de l'information, et les obligations qui en découlent sont précisées par des directives.

9. ENTRÉE EN VIGUEUR

La Politique ministérielle de la sécurité de l'information entre en vigueur à la date de son approbation par le sous-ministre.

Patrick Dubé
Sous-ministre

1-11-18
Date

ANNEXE – ENGAGEMENT DE CONFIDENTIALITÉ LORS DE LA REMISE D'ACTIFS INFORMATIONNELS AU DÉPART D'UN EMPLOYÉ DU MINISTÈRE DU TOURISME

Déclaration :

Je, soussigné(e), _____,
(lettres moulées)

déclare formellement ce qui suit :

- Je suis, ou j'ai été, un(e) employé(e) du ministère du Tourisme (MTO);
- Je m'engage, sans limites de temps, à garder le secret le plus entier et à ne pas communiquer ou permettre que soient communiquées à quiconque les données suivantes :

    a. (ex. : liste de contacts personnels, courriels personnels)
    b. …
    c. …

    que j'ai obtenues de la Direction des ressources informationnelles, à moins d'avoir été dûment autorisé(e) à le faire par le sous-ministre du MTO ou par l'un(e) de ses représentant(e)s autorisé(e)s;

- Je m'engage également, sans limites de temps, à ne pas faire usage d'un tel renseignement ou document à une fin autre que celle s'inscrivant dans le cadre des rapports qui me lient ou qui m'ont lié(e) au MTO;
- J'ai été informé(e) que le défaut par le (la) soussigné(e) de respecter en tout ou en partie le présent engagement de confidentialité m'expose à des recours légaux, des réclamations, des poursuites et toutes autres procédures en raison du préjudice causé à quiconque est concerné;
- Je confirme avoir lu les termes du présent engagement et en avoir saisi toute la portée.

Et j'ai signé à _____, ce _____ jour du mois _____, 20___

_____
(Signature)