Langue française
Québec

Secrétariat général et
direction du bureau de la sous-ministre

PAR COURRIEL

Québec, le 21 février 2024

N/Réf. : DA30-20240206

Objet : Votre demande d'accès à l'information

Conformément à 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 sur l'accès », votre demande d'accès reçue le 6 février 2024, laquelle se lit comme suit, a été traitée :

> *« […] je désire recevoir le ou les documents suivants :*
>
> *Au sujet la politique gouvernementale en cybersécurité :*
>
> *Toutes mesures mise en place afin de renforcer l'encadrement de la sécurité de l'information, rehausser l'efficacité de la prise en charge des incidents et de la gestion de crise et les mécanismes de gestion mise en place afin d'améliorer la performance en cybersécurité au sein du ministère; »*

Je vous transmets une copie des documents détenus par le ministère concernant votre demande dont la communication est conforme aux dispositions de la Loi sur l'accès.

800, rue D'Youville, 13e étage
Québec (Québec) G1R 3P4
Téléphone : 418 932-0078
mathieu.chabot@mlf.gouv.qc.ca

Toutefois, conformément à l'article 14 de la *Loi sur l'accès*, certains documents ne vous sont pas communiqués parce qu'ils contiennent, en substance, des renseignements qui sont visés par certaines restrictions prévues à la loi. En ce sens, nous appuyons notre décision sur les articles suivants :

- L'article 29, lequel précise qu'un organisme public doit refuser de confirmer l'existence ou de donner communication d'un renseignement portant sur une méthode ou une arme susceptible d'être utilisée pour commettre un crime ou une infraction à une loi. Il doit aussi refuser de confirmer l'existence ou de donner communication d'un renseignement dont la divulgation aurait pour effet de réduire l'efficacité d'un programme, d'un plan d'action ou d'un dispositif de sécurité destiné à la protection d'un bien ou d'une personne.

- L'article 9, qui précise que le droit d'accès ne s'étend pas aux notes personnelles inscrites sur un document, ni aux esquisses, ébauches, brouillons, notes préparatoires ou autres documents de même nature.

De plus, lors de notre analyse, nous avons recensé des documents provenant du ministère de la Cybersécurité et du Numérique (MCN) et du ministère de l'Emploi et de la Solidarité sociale (MESS). L'analyse de l'accessibilité de ces documents relève de la compétence de ces organismes publics. En vertu de l'article 48 de la *Loi sur l'accès*, nous vous invitons, si ce n'est déjà fait, à formuler votre demande auprès de la responsable de l'accès aux documents de cet organisme, aux coordonnées suivantes :

Madame Isabelle Goulet
Responsable de l'accès aux documents et de la protection des renseignements personnels
Ministère de la Cybersécurité et du Numérique
900, place D'Youville, 3e étage
Québec, (Québec) G1R 3P7
Téléphone : 418 528-0880, poste 3125
Courriel : acces@mcn.gouv.qc.ca

Madame Marie-Michèle Genest
Directrice des mandats ministériels et secrétaire générale adjointe
Direction des mandats ministériels et Secrétariat général adjoint
Ministère de l'Emploi et de la Solidarité sociale
425, rue Jacques-Parizeau, 4e étage
Québec (Québec) G1R 4Z1
Téléphone : 418 643-4820
Courriel : acces@mtess.gouv.qc.ca

Il convient de préciser que le MCN apporte à notre Ministère les services bureautiques, ainsi que l'environnement de stockage, de sécurité et d'équipements informatiques. Le MESS nous offre quant à lui le soutien à la gouvernance et au développement des systèmes de mission au Ministère.

Conformément à l'article 51 de la *Loi sur l'accès*, je vous informe que vous pouvez demander la révision de cette décision auprès de la Commission d'accès à l'information dans les 30 jours qui la suivent, conformément à la section III du chapitre IV de cette loi. Des informations relatives à l'exercice d'un tel recours sont jointes à la présente.

Je vous prie d’agréer mes salutations distinguées.

Le responsable de l’accès aux documents et de la protection des renseignements personnels,

Mathieu Chabot

p. j.

Avis de recours

Un recours peut s'exercer à la suite d'une décision rendue en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1), ci-après la « Loi sur l'accès ».

Révision

a) Pouvoir

L'article 135 de la Loi sur l'accès prévoit qu'une personne dont la demande écrite a été refusée en tout ou en partie par le responsable de l'accès aux documents ou de la protection des renseignements personnels peut demander à la Commission d'accès à l'information de réviser cette décision. La demande de révision doit être faite par écrit et elle peut exposer brièvement les raisons pour lesquelles la décision devrait être révisée (art. 137).

L'adresse de la Commission d'accès à l'information est la suivante :

Québec
Bureau 2.36
525, boul. René-Lévesque Est
Québec (Québec) G1R 5S9
Téléphone : 418 528-7741
Numéro sans frais : 1 888 528-7741

Montréal
Bureau 18.200
500, boul. René-Lévesque Ouest
Montréal (Québec) H2Z 1W7
Tél. : 514 873-4196
Numéro sans frais : 1 888 528-7741

b) Motifs

Les motifs relatifs à la révision peuvent porter sur la décision, sur le délai de traitement de la demande, sur le mode d'accès à un document ou à un renseignement, sur les frais exigibles ou sur l'application de l'article 9 (notes personnelles inscrites à un document, esquisses, ébauches, brouillon, notes préparatoires ou autres textes de même nature qui ne sont pas considérés comme des documents d'un organisme public).

c) Délais

Les demandes de révision doivent être adressées à la Commission d'accès à l'information dans les 30 jours suivant la date de la décision ou de l'expiration du délai accordé au responsable pour répondre à une demande (art. 135).

La Loi sur l'accès prévoit explicitement que la Commission d'accès à l'information peut, pour motif raisonnable, relever le requérant du défaut de respecter le délai de 30 jours (art. 135).

Langue française
Québec

Titre **Cadre de gestion de la sécurité de l'information**	Date d'entrée en vigueur **2023-03-08**
Pour information **Direction de la coordination administrative**	Date dernière mise à jour

1. INTRODUCTION

Le présent cadre est adopté en application de la Politique ministérielle de sécurité de l'information. Il vise à renforcer la gouvernance de la sécurité de l'information du Ministère par la mise en place d'une structure organisationnelle de la sécurité de l'information ainsi que la définition des rôles et responsabilités à tous les niveaux du Ministère.

2. CADRE NORMATIF

Le présent cadre de gestion doit être interprété et appliqué conformément au cadre juridique et administratif en annexe de la Politique ministérielle de sécurité de l'information.

3. RÔLES ET RESPONSABILITÉS DES INTERVENANTS

3.1. La sous-ministre

La sous-ministre est la première responsable de la sécurité de l'information relevant de son autorité. Elle doit assurer le respect des lois et des règles de sécurité de l'information déterminées par le Secrétariat du Conseil du trésor (SCT), notamment en ce qui a trait à la mise en place de mesures permettant la réduction des risques reliés à la sécurité de l'information. À ce titre, elle doit notamment :

a) adopter les orientations stratégiques de la sécurité de l'information du Ministère, la politique, le cadre de gestion, les directives et les plans d'action en la matière et en assurer la mise en œuvre;

b) approuver les bilans de sécurité de l'information avant transmission au SCT;

c) s'assurer de la mise en place de mesures permettant de réduire les risques de sécurité de l'information à un niveau acceptable par le Ministère;

d) s'assurer de l'adéquation des mesures de sécurité de l'information en vigueur par rapport aux risques encourus;

e) s'assurer de la mise en œuvre des processus officiels de sécurité de l'information permettant notamment de veiller à la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents;

f) s’assurer de la réalisation périodique d’audits de sécurité de l’information et de tests d’intrusion et de vulnérabilité, conformément aux énoncés de la Directive sur la sécurité de l’information gouvernementale (décret 7-2014 du 15 janvier 2014), et en dégager les priorités d’action ainsi que les échéanciers afférents;

g) favoriser l’utilisation des services communs de sécurité de l’information déterminés par le SCT;

h) s’assurer que les ententes de service et les contrats conclus avec les prestataires de services, les partenaires et les mandataires comprennent des clauses garantissant le respect des exigences de sécurité de l’information;

i) s’assurer de la mise en place d’un programme officiel et continu de formation et de sensibilisation du personnel en matière de sécurité de l’information;

j) approuver et présenter aux instances gouvernementales concernées les plans d’action et les bilans requis, conformément aux énoncés de la Directive sur la sécurité de l’information gouvernementale;

k) désigner les détenteurs de l’information, le responsable organisationnel de la sécurité de l’information (ROSI) et le coordonnateur organisationnel de gestion des incidents (COGI);

l) s’assurer de la saine gouvernance de la sécurité de l’information et veiller à en établir les objectifs stratégiques;

m) déléguer sa responsabilité au ROSI de déclarer les incidents de sécurité de l’information à portée gouvernementale à l’équipe de réponse aux incidents de sécurité de l’information de l’Administration québécoise (CERT/AQ).

3.2. Dirigeant principal de l’information

Le dirigeant principal de l’information (DPI) est responsable de veiller à l’application, par chaque organisme public auquel il est rattaché, des règles de gouvernance et de gestion établies en vertu de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement. À ce titre, il doit notamment :

a) définir des règles particulières en matière de gestion de l’information, incluant celles inhérentes à la sécurité de l’information, qui seront applicables aux organismes publics auxquels il est rattaché;

b) veiller à la pérennité des actifs informationnels des organismes publics auxquels il est rattaché.

3.3. Le responsable organisationnel de la sécurité de l'information

La sous-ministre désigne le ROSI. Le ROSI joue le rôle de porte-parole du dirigeant principal de l'information (DPI) et relaie au Ministère les orientations et les priorités d'intervention gouvernementales en sécurité de l'information. Il assure la coordination et la cohérence des mesures de sécurité de l'information mises en œuvre par d'autres intervenants du Ministère. Il coordonne également la contribution du Ministère aux processus de gestion des risques et de gestion des incidents à portée gouvernementale. À ce titre, il doit notamment :

a) soumettre, aux fins de recommandation pour approbation de la sous-ministre ou de consultation au Comité ministériel de la sécurité de l'information (CMSI), les orientations, les politiques, les directives, les cadres de gestion, les priorités d'action, les éléments de reddition de comptes ainsi que tout événement ayant mis ou aurait pu mettre en péril la sécurité de l'information;

b) s'assurer de la coordination et de la cohérence des actions de sécurité de l'information menées au sein du Ministère par d'autres intervenants, dont notamment les détenteurs de l'information ainsi que les unités responsables des ressources informationnelles, de l'accès à l'information et de la protection des renseignements personnels, de la gestion documentaire, de la sécurité physique et de l'éthique;

c) déclarer au dirigeant principal de l'information les risques de sécurité de l'information à portée gouvernementale;

d) déclarer au CERT/AQ les incidents de sécurité de l'information à portée gouvernementale;

e) recommander à la sous-ministre, pour approbation, les processus officiels de sécurité de l'information, tels que la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents;

f) coordonner l'élaboration et la mise en œuvre d'un programme continu de formation et de sensibilisation en matière de sécurité de l'information;

g) participer aux tables de coordination et de concertation gouvernementales en matière de sécurité de l'information;

h) participer à des comités interministériels et représenter le Ministère en matière de sécurité de l'information;

i) autoriser une mesure d'exception au détenteur de l'information qui a une raison valable de ne pas se conformer à une exigence particulière ou de ne pas recourir à une mesure de sécurité déterminée;

j) déterminer la composition du CMSI et du comité ministériel de gestion de crise.

3.4. Le responsable de la sécurité des actifs informationnels

Le responsable de la sécurité des actifs informationnels (RSAI) appuie et conseille le ROSI dans son rôle de coordination afin d'assurer la cohérence des mesures de sécurité mises en œuvre au Ministère. À ce titre, il doit notamment :

a) proposer au ROSI les orientations, les politiques, les directives, les cadres de gestion, les priorités d'action, les éléments de reddition de comptes et les mettre en œuvre;

b) élaborer et mettre en œuvre un programme de formation continue et de sensibilisation en matière de sécurité de l'information;

c) produire les bilans de sécurité de l'information et identifier les risques à portée gouvernementale;

d) mettre en œuvre les orientations et les priorités d'intervention gouvernementales en matière de sécurité de l'information;

e) s'assurer de l'intégration de la sécurité dans les projets et les initiatives afin que les risques demeurent à un niveau acceptable pour le Ministère;

f) réaliser périodiquement des audits de sécurité de l'information et des tests d'intrusion et de vulnérabilité, conformément aux énoncés de la Directive sur la sécurité de l'information gouvernementale, et en dégager les priorités d'action ainsi que les échéanciers afférents;

g) mettre en œuvre les processus officiels de sécurité de l'information permettant notamment la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents et en coordonner l'application;

h) gérer la réponse aux incidents de sécurité de l'information et faire rapport au ROSI de tout incident de sécurité de l'information;

i) mettre à jour le présent cadre de gestion.

3.5. Le conseiller organisationnel en sécurité de l'information

Le COSI apporte son soutien aux différents intervenants, notamment en ce qui a trait à la mise en œuvre des mesures d'atténuation des risques et à la mise en place de processus formels de sécurité de l'information.

Le COSI est de plus responsable de la révision annuelle de la Politique ministérielle de sécurité de l'information afin de s'assurer de son adéquation aux besoins du Ministère. À ce titre, il doit notamment :

a) contribuer à la mise en œuvre des orientations internes découlant des directives gouvernementales, des politiques internes et des pratiques généralement admises à cet égard;

b) conseiller le Ministère en matière d'ententes de service et de contrats et formuler des recommandations quant à l'intégration de dispositions garantissant le respect des exigences de sécurité de l'information;

c) tenir à jour le registre d'autorité de la sécurité de l'information;

d) tenir à jour le registre de catégorisation et transmettre au CMSI l'analyse de la catégorisation pour recommandation;

e) assister les détenteurs de l'information dans l'exercice de catégorisation concernant les systèmes qui traitent de l'information relevant de leur responsabilité et dans la réalisation des analyses de risques de sécurité des actifs informationnels;

f) contribuer à la définition et à la mise en œuvre des processus formels de sécurité de l'information.

3.6. Le coordonnateur organisationnel de gestion des incidents

Le COGI est désigné par la sous-ministre et collabore étroitement avec les différents intervenants afin de leur fournir le soutien technique nécessaire à l'exercice de leurs responsabilités. Il participe activement au réseau d'alertes gouvernemental et contribue à la mise en place du processus de gestion des incidents de sécurité de l'information au sein du Ministère et du processus de gestion des incidents à portée gouvernementale. À ce titre, il doit notamment :

a) contribuer aux analyses de risques de sécurité de l'information, identifier les menaces et les situations de vulnérabilité et mettre en œuvre les solutions appropriées;

b) contribuer à la définition, la mise en œuvre et l'exécution des processus formels de sécurité de l'information, dont notamment celui concernant les incidents de sécurité de l'information tant à portée ministérielle que gouvernementale;

c) collaborer à l'élaboration et à la mise à jour des guides portant sur la sécurité opérationnelle notamment des systèmes, des réseaux et des infrastructures;

d) collaborer étroitement avec les différents intervenants et leur fournir le soutien technique nécessaire à l'exercice de leurs responsabilités;

e) coordonner la réponse aux incidents de sécurité de l'information.

3.7. Le détenteur d'information

Le détenteur de l'information est la personne désignée par la sous-ministre pour assumer la responsabilité de la catégorisation des actifs informationnels et de la classification de l'information, de l'identification et de la mise en œuvre des mesures de sécurité propres à assurer la protection de l'information collectée, utilisée, communiquée, conservée ou détruite.

Chaque détenteur de l'information collabore étroitement avec les différents intervenants, notamment à la détermination des exigences de sécurité, à la gestion des incidents et à la reddition de comptes en matière de sécurité. À ce titre, il doit notamment :

a) identifier les besoins en matière de sécurité et s'assurer que des mesures de sécurité appropriées sont élaborées, mises en place et appliquées systématiquement;

b) approuver le choix des mesures appropriées pour la protection de l'information dont il est responsable ainsi que des moyens de contrôle et des règles d'accès à cette information;

c) déléguer au besoin, à des représentants qu'il désigne, certaines responsabilités en matière de sécurité de l'information;

d) catégoriser l'information relevant de sa responsabilité selon sa valeur et ses exigences en matière de disponibilité, d'intégrité et de confidentialité;

e) classifier l'information relevant de sa responsabilité selon sa valeur et sa sensibilité;

f) veiller à ce que les mesures de sécurité de l'information, y compris celles reliées au respect des exigences légales de protection des renseignements personnels, soient mises en place et appliquées;

g) agir comme maître d'œuvre de la gestion des risques de ses actifs informationnels en sélectionnant et approuvant les mesures de sécurité de l'information adéquates et proportionnelles aux risques, tout en assumant les risques résiduels;

h) s'assurer du respect des lois, des politiques, des normes, des cadres de gestion et des processus en matière de sécurité de l'information dans les procédures opérationnelles, techniques ou administratives, relativement à l'information relevant de sa responsabilité;

i) autoriser les accès aux actifs informationnels sous sa responsabilité;

j) maintenir à jour les procédures et les listes des privilèges d'accès des personnes autorisées.

3.8. Le gestionnaire

Le gestionnaire doit faire connaître au personnel de son unité les règles de sécurité de l'information et veiller à leur application. Il autorise les demandes d'accès aux actifs informationnels nécessaires à l'exercice de leurs fonctions et les révoque en conformité avec les règles applicables. Il doit notamment :

a) s'assurer que le personnel de son unité est informé et sensibilisé à la sécurité de l'information et sur les modalités de sa mise en œuvre;

b) indiquer clairement au personnel de son unité le rôle et les obligations de l'utilisateur ainsi que les conséquences d'une atteinte à la sécurité de l'information;

c) s'assurer que l'information est utilisée en conformité avec les politiques, les directives, les processus et les consignes en matière de sécurité de l'information;

d) autoriser au personnel de son unité l'accès aux seuls actifs informationnels nécessaires à l'exercice de leurs fonctions;

e) aviser l'assistance technique de tout problème ou risque pouvant affecter la disponibilité, l'intégrité ou la confidentialité de l'information.

3.9. Le responsable de l'audit interne

Il joue un rôle-clé dans la reddition de comptes en matière de sécurité de l'information, plus particulièrement en regard de l'identification, de l'évaluation et de la gestion des risques d'atteinte à la sécurité de l'information. À ce titre, il doit évaluer, examiner ou vérifier :

a) l'application, la validité et l'efficacité des règles, des mesures administratives et des moyens technologiques en matière de sécurité de l'information élaborés et mis en œuvre;

b) l'adéquation de l'intégration de la sécurité de l'information dans les processus d'affaires.

Il peut réaliser, sur demande, des enquêtes administratives concernant des cas possibles de dérogation, de non-respect ou d'atteinte aux règles relatives à la sécurité de l'information au Ministère.

3.10. Le Comité ministériel de la sécurité de l'information

Le CMSI est la principale instance de concertation en matière de sécurité et les membres sont nommés par le ROSI. En vue de l'approbation par la sous-ministre, son mandat consiste à assurer la cohérence des actions avec les orientations, politiques, directives et autres dispositions gouvernementales, à examiner et formuler des recommandations concernant :

a) les orientations, politiques, directives, cadres de gestion, plans d'action et bilans de l'organisation en matière de sécurité de l'information;

b) les propositions de mesures, les projets et autres éléments stratégiques en matière de sécurité de l'information;

c) les analyses de risques et les mesures à mettre en place pour protéger les actifs informationnels de l'organisation.

3.11. L'équipe de réponse aux incidents de sécurité de l'information

L'équipe de réponse aux incidents de sécurité de l'information est un groupe ad hoc présidé par le COGI et composé de personnes jugées pertinentes à la prise en charge d'un incident de sécurité. Elle a notamment pour rôle de :

a) procéder à la résolution de l'incident de sécurité de l'information;

b) convoquer toute personne jugée utile à la compréhension et la résolution de l'incident de sécurité de l'information.

3.12. Le Comité ministériel de gestion de crise

Le Comité ministériel de gestion de crise est le groupe décisionnel appelé à intervenir en cas d'incident critique de sécurité de l'information, notamment lorsque les tentatives de rétablissement des activités n'ont pas apporté les résultats escomptés ou qu'aucune mesure palliative n'a pu assurer la continuité ou la reprise rapide des services. À ce titre, il a notamment pour rôle :

a) d'autoriser la mise en œuvre de stratégies permettant d'assurer la prise en charge des incidents critiques de sécurité de l'information;

b) d'adopter la déclaration de sinistre proposée par le responsable de la continuité des services et d'approuver les budgets spéciaux correspondants;

c) de décider du déploiement ou non des plans de continuité des services;

d) de proposer des orientations à suivre ou des actions à poser en cas de sinistre;

e) de formuler des recommandations concernant le délestage, en totalité ou en partie, des activités de l'organisation;

f) de communiquer avec les médias.

La composition du Comité ministériel de gestion de crise est déterminée par le ROSI.

4. DISPOSITIONS FINALES

4.1. Mise en œuvre, suivi et révision

Le ROSI, appuyé par le RSAI, est responsable de l'élaboration et de l'application du cadre de gestion.

Ce cadre sera révisé à l'occasion de changements importants qui pourraient l'affecter ou, au plus tard, tous les cinq ans à partir de la date d'approbation. Toute modification devra être approuvée par la sous-ministre sur recommandation du CMSI.

5. ENTRÉE EN VIGUEUR

Le présent cadre entre en vigueur à la date de sa signature par la sous-ministre.

Original signé

Juliette Champagne
Sous-ministre de la Langue française

Québec, 27 mars 2023
Date

Langue française
Québec

Titre	Date d'entrée en vigueur
Directive sur la gestion de l'accès aux données et aux systèmes d'information	**2023-03-08**
Pour information **Direction de la coordination administrative**	Date dernière mise à jour

1. OBJET

La présente directive définit les lignes directrices relatives aux privilèges qui sont accordés aux utilisateurs pour l'accès aux données et aux systèmes d'information ainsi que les rôles et responsabilités des principaux intervenants. Elle prévoit également les sanctions dans le cas de transgression aux dispositions énoncées.

2. CADRE LÉGAL ET ADMINISTRATIF

- Loi concernant le cadre juridique des technologies de l'information (RLRQ, chapitre C 1.1);
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1);
- Loi sur les archives (RLRQ, chapitre A-21.1);
- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, chapitre G-1.03);
- Directive sur la sécurité de l'information gouvernementale (décret 7-2014 du 15 janvier 2014).

3. CHAMP D'APPLICATION

Cette directive s'applique à tous les utilisateurs qui détiennent des privilèges d'accès aux données et aux systèmes d'information ministériels, ainsi qu'aux données et aux systèmes d'information faisant l'objet d'une entente avec un autre ministère ou organisme, peu importe le statut de l'utilisateur (exemple : permanent, occasionnel, consultant, stagiaire, partenaire, fournisseur ou autre, ayant un accès, sur place ou à distance, à l'information détenue par le Ministère).

4. PRINCIPE DIRECTEUR

L'attribution d'un accès aux données et aux systèmes d'information est un privilège et non un droit accordé à un utilisateur, afin de lui permettre de rendre une prestation de service strictement associée à ses responsabilités.

Aux fins de l'encadrement de tout accès aux données et aux systèmes d'information ministériels par un tiers et lors de tout accès aux données et aux systèmes d'information d'un tiers par le Ministère, une entente de service est signée.

5. RÔLES ET RESPONSABILITÉS

5.1 La sous-ministre

La sous-ministre est la première responsable de la sécurité de l'information. À ce

titre, elle :

- Approuve la présente directive;
- S'assure de la mise en place de mesures permettant de réduire les risques de gestion de l'accès aux données et aux systèmes d'information à un niveau acceptable par le Ministère;
- S'assure de l'adéquation des mesures de gestion de l'accès aux données et aux systèmes d'information par rapport aux risques encourus.

5.2 Le responsable organisationnel de la sécurité de l'information (ROSI)

Le ROSI est désigné par la sous-ministre pour le représenter en matière de sécurité de l'information. À ce titre, elle :

- Assure l'application et la diffusion de la présente directive et procède au besoin à sa révision;
- Soutien la sous-ministre dans sa responsabilité de réduction des risques associés à la gestion de l'accès aux données et aux systèmes d'information du Ministère;
- Met en œuvre les mesures nécessaires pour corriger toute situation qui lui a été signalée relativement à la sécurité de l'accès aux données et aux systèmes d'information;
- Détermine les modalités d'attribution des comptes qui bénéficient de privilèges élevés et autorise l'attribution de ces privilèges.

5.3 La direction de la coordination administrative (DCA)

Conjointement avec son prestataire de services bureautiques et informatiques, le Ministère établit les procédures, mécanismes de contrôle et d'octroi des accès et des mesures de sécurité. Le Ministère se plie aux directives du ministère de la cybersécurité et du numérique (MCN). La DCA est détentrice du processus de gestion de l'accès aux données et aux systèmes. À ce titre elle :

- Définit, en collaboration avec l'ensemble des intervenants en matière de gestion de l'accès aux données et aux systèmes d'information, les processus d'attribution desdits accès internes et externes;
- S'assure de la mise en œuvre des processus d'attribution des accès aux données et aux systèmes d'information internes et externes;
- Détermine, avec le responsable de la sécurité opérationnelle, si une demande d'accès interne aux données d'un employé du Ministère est autorisée ou non;
- Maintient et transmet au responsable de la sécurité opérationnelle la liste des utilisateurs actifs et tous les mouvements du personnel.

5.4 Les détenteurs de l'information

La sécurité de l'information des données et des systèmes relève de la responsabilité des détenteurs de l'information. À ce titre, ils :

- Définissent les modalités permettant les accès aux données et aux systèmes d'information relevant de leur autorité tout en respectant les lois, les politiques, les normes, les cadres de gestion et les processus en matière de sécurité de l'information;

- Déterminent les personnes autorisées à attribuer des accès aux données et aux systèmes d'information relevant de leur autorité;
- Veillent à ce que l'accès aux données et aux systèmes d'information qu'ils jugent plus sensibles fassent l'objet de mesures plus restrictives et d'un suivi plus important;
- S'assurent qu'une entente de service est conclue lorsqu'un accès aux données et aux systèmes d'information ministériels est octroyé à un tiers;
- Signalent rapidement au ROSI, toute atteinte à la sécurité liée aux accès aux données et aux systèmes d'information dont ils sont responsables.

5.5 Les gestionnaires

Les gestionnaires assument la sécurité de l'information traitée par les employés relevant de leur unité administrative. À ce titre, ils :

- Informent et sensibilisent le personnel de leur unité sur la présente directive;
- S'assurent que les accès aux données et aux systèmes d'information sont utilisés exclusivement par la personne à laquelle ils ont été accordés et ils en sont imputables auprès de la haute direction;
- Déterminent les profils de tâches de leurs employés et font suivre, au responsable de la sécurité opérationnelle, les demandes d'autorisation d'accès aux données et aux systèmes d'information;
- S'assurent que leurs employés ont accès seulement aux données et aux systèmes d'information nécessaires pour effectuer leurs tâches;
- Effectuent les modifications requises des accès aux données et aux systèmes d'information des employés sous leur responsabilité au moment de la mutation, de l'affectation, ou de tout changement relatif aux fonctions et aux tâches de ces employés. Dans le cas spécifique d'un départ d'un employé du Ministère, le gestionnaire entreprend les mesures afin que tous ses accès aux données et aux systèmes d'information soient retirés et que tous ses comptes soient fermés;
- Demandent, lors d'une absence pour un congé prolongé, la suspension de tous les accès aux données et aux systèmes d'information de l'employé pour la période couverte par l'absence;
- Revoient les accès aux données et aux systèmes d'information attribués à leurs employés au moins une fois par année;
- Signalent rapidement au ROSI, toute atteinte à la sécurité liée aux accès aux données et aux systèmes d'information dont ils sont responsables.

5.6 La personne responsable de la sécurité opérationnelle (RSO)

La fonction de responsable de la sécurité opérationnelle est confiée au ministère de la Cybersécurité et du Numérique (MCN) par son entente de services. Le MCN collabore à l'ensemble des opérations de mise en œuvre des processus et systèmes de l'accès aux données et aux systèmes d'information. À ce titre il :

- Attribue les accès autorisés par les détenteurs de l'information et les

gestionnaires;

- S’assure que les utilisateurs aient réussi une enquête d’habilitation de sécurité avant de leur attribuer des privilèges élevés;
- Attribue les demandes des comptes d’administrateurs des postes de travail et de ceux qui bénéficient de privilèges élevés en fonction des modalités déterminés par le ROSI;
- Tient un registre des comptes d’administrateurs des postes de travail et des comptes qui bénéficient de privilèges élevés;
- Répertorie les privilèges d’accès aux données et aux systèmes d’information ainsi que leurs modifications et leurs violations;
- Fournit les outils et l’expertise qui permettent la production de suivi périodique de la gestion et l’audit de la sécurité des accès aux données et aux systèmes d’information, qu’il transmet aussi aux gestionnaires et aux détenteurs de l’information au moins une fois par an;
- Met en place et exploite un système de journalisation de la conformité des accès aux données et aux systèmes d’information.

5.7 Le conseiller organisationnel en sécurité de l’information (COSI)

Le COSI apporte son soutien au ROSI. Dans ce cadre, il collabore aux divers travaux associés à la gestion de l’accès aux données et aux systèmes d’information.

5.8 Le responsable de la vérification interne (RVI)

Le RVI joue un rôle-clé dans la reddition de comptes en matière de sécurité de l'information, plus particulièrement en regard de l'identification, de l'évaluation et de la gestion des risques d'atteinte à la sécurité de l'information. À ce titre, il :

- Répond aux demandes officielles d’audit des accès aux données et aux systèmes d’information ou aux demandes d’enquêtes administratives;
- Valide les processus d’attribution de l’accès aux données et aux systèmes d’information.

5.9 Le responsable de l’accès et de la protection des renseignements personnels (RAIPRP)

Le RAIPRP veille au respect de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1). À ce titre, il:

- Participe aux divers travaux associés à la gestion de l’accès aux données et aux systèmes d’information;
- S’assure que les règles en matière de protection des renseignements personnels sont respectées.

5.10 Les utilisateurs

Les utilisateurs ont une responsabilité non négligeable en matière de sécurité de l’information et de gestion de l’accès aux données et aux systèmes d’information. À ce titre, ils :

- S’assurent de comprendre la présente directive ainsi que son application dans leurs activités quotidiennes;
- Reconnaissent que les accès aux données et aux systèmes d’information qui leur sont accordés sont un privilège et non un droit et qu’ils peuvent leur être retirés en tout temps;
- Utilisent et consultent les données et les systèmes d’information uniquement aux fins des tâches qui leur sont assignées dans le cadre de leur travail;
- Sont responsables des accès aux données et aux systèmes d’information qui leur sont octroyés et sont redevables auprès de leur gestionnaire de toute action exécutée avec leur identifiant et leur mot de passe;
- Signalent rapidement à leur gestionnaire, toute violation à la sécurité concernant l’accès aux données et aux systèmes d’information dont ils ont connaissance;
- Accèdent aux données et aux systèmes d’information exclusivement avec l’identifiant qui leur a été personnellement attribué.

6. SANCTIONS

Selon la gravité du manquement, toute personne qui contrevient à la présente directive peut faire l’objet d’une mesure administrative ou disciplinaire pouvant aller jusqu'au congédiement, une poursuite en responsabilité civile, une plainte pénale ou une poursuite criminelle, en conformité notamment avec les contrats, conventions collectives, lois ou règlements applicables.

7. APPROBATION ET DATE D’ENTRÉE EN VIGUEUR

La présente directive entre en vigueur à la date de son approbation par la sous-ministre.

Original signé

Juliette Champagne
Sous-ministre de la Langue française

2023-03-09

Date

Langue française
Québec

Titre	Date d'entrée en vigueur
Politique ministérielle de sécurité de l'information	**2023-03-09**
Pour information **Direction de la coordination administrative**	Date dernière mise à jour

1. CONTEXTE

Le ministère de la Langue française (ci-après le Ministère) a pour mission de promouvoir, valoriser et protéger la langue française et son statut au Québec, où le français est la seule langue officielle ainsi que la langue commune. Le Ministère élabore et fait connaître les grandes orientations définissant l'aménagement linguistique au Québec, en plus de favoriser la connaissance, la protection, la mise en valeur et la transmission du patrimoine linguistique francophone du Québec.

Le Ministère a aussi pour mission de veiller à la cohérence de l'action de l'Administration et à sa conformité aux dispositions de la Charte de la langue française. Pour ce faire, il entretient des liens étroits avec les ministères et organismes du gouvernement québécois, de même qu'avec les organismes municipaux, et travaille en collaboration avec eux.

La présente politique est adoptée en application du paragraphe (a) du premier alinéa de l'article 7 de la *Directive sur la sécurité de l'information gouvernementale du Secrétariat du Conseil du trésor* (SCT) (Décret 1514-2021 du 8 décembre 2021). Celle-ci enjoint les organismes publics à adopter et à mettre en œuvre une politique de sécurité de l'information, à la maintenir à jour et à en assurer l'application. La mise en œuvre de cette politique est notamment soutenue par un cadre de gestion de la sécurité de l'information.

Le ministère de la Langue française assume ses responsabilités dans le domaine de la sécurité de l'information dans un contexte où il s'engage par entente de services auprès du ministère de la cybersécurité et du numérique (MCN) pour l'hébergement, la gestion et la préservation des données numériques ainsi que par la fourniture des équipements bureautiques et de télécommunications et par la gestion sécuritaire de ceux-ci. À cet égard, l'actualisation de ces responsabilités est partagée entre le ministère et son fournisseur de services des technologies de l'information. L'entente de services prévoit les conditions opérationnelles de réalisation des divers obligations ici-bas énumérées ainsi qu'aux rôles assumés par le ministère ainsi que par le MCN. Le ministère demeure responsable de ses obligations mais confie la réalisation des actions à son fournisseur de services qui assument la responsabilité de répondre favorablement à ses obligations présentées à l'entente de services.

2. OBJECTIF

La présente politique a pour objectif d'affirmer l'engagement du Ministère à s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information et d'assurer, tout au long du cycle de vie de l'information, sa disponibilité, son intégrité et sa confidentialité.

3. PORTÉE

Cette politique porte sur l'information et les actifs informationnels (ci-après actifs informationnels) dont le Ministère a la responsabilité, peu importe leur nature, leur localisation et le support sur lequel ils se trouvent, et ce, durant tout leur cycle de vie, c'est-à-dire depuis leur collecte ou leur création jusqu'à leur versement à la Bibliothèque et aux Archives nationales du Québec ou leur destruction en conformité avec le calendrier de conservation établi.

Sous réserve de politiques ou de dispositions particulières propres à certains utilisateurs, cette politique s'applique à toute personne ayant accès aux actifs informationnels du Ministère sans égard à leur statut d'emploi, y compris notamment les ressources contractuelles, les partenaires, les fournisseurs ou autres intervenants.

4. PRINCIPES DIRECTEURS

4.1. Notions générales de sécurité de l'information

4.1.1 Disponibilité

Le Ministère s'assure de la disponibilité de l'information afin qu'elle soit accessible aux entités autorisées, en temps voulu et de la manière requise.

4.1.2 Intégrité

Le Ministère s'assure de l'intégrité de l'information de sorte que celle-ci ne soit pas détruite ou altérée de quelque façon sans autorisation, et que le support sur lequel cette information est conservée lui procure la stabilité et la pérennité voulues.

4.1.3 Confidentialité

Le Ministère s'assure de limiter l'accès et la divulgation de l'information aux seules entités autorisées à en prendre connaissance. De plus, il recueille et conserve uniquement l'information nécessaire à l'accomplissement de sa mission, dans le respect du cadre juridique et administratif auquel il est soumis.

4.2. Le Ministère assure la sécurité de l'information conformément aux principes directeurs suivants :

4.2.1 Cadre normatif

Le Ministère s'assure que son cadre normatif et ses pratiques en matière de sécurité de l'information soient réévalués périodiquement afin de tenir compte des changements juridiques, organisationnels, technologiques, physiques et environnementaux, ainsi que de l'évolution des menaces et des risques.

4.2.2 Responsabilités et imputabilité

Le Ministère identifie clairement les responsabilités à tous les niveaux de l'organisation et met en place un processus de gestion interne de la sécurité permettant une reddition de comptes adéquate, conformément aux rôles et responsabilités définis dans le *Cadre de gestion de la sécurité de l'information*.

4.2.3 Sensibilisation

Le Ministère s'engage à sensibiliser et à former les utilisateurs à la sécurité de l'information, aux conséquences d'une atteinte à sa sécurité, ainsi qu'à leur rôle et à leurs obligations en cette matière.

Le Ministère s'assure que le processus de gestion de la sécurité de l'information est soutenu par une démarche d'éthique visant à assurer la régulation des conduites et la responsabilisation individuelle.

4.2.4 Gestion des actifs informationnels

Le Ministère fait l'inventaire des actifs informationnels sous sa responsabilité, peu importe leur support (ex. : papier, numérique, audio et vidéo), procède à leur catégorisation, évalue leur état et détermine les mesures de protection à leur accorder.

De plus, l'information fait l'objet d'une classification de sécurité en fonction de critères touchant la valeur, les exigences juridiques, la sensibilité et la criticité de l'information pour l'organisation. Les mesures de sécurité visant à protéger l'information sont établies notamment en fonction de cette classification et tiennent compte de son contexte d'utilisation et de son cycle de vie.

4.2.5 Gestion des risques

Le Ministère procède régulièrement à des analyses de risques en vue de déterminer la protection qui doit être accordée à l'information sous sa responsabilité. Ces analyses conduisent au choix de mesures de sécurité proportionnelles aux risques, afin de les mitiger pour les amener à un niveau acceptable.

Cette analyse doit également accompagner tous les changements importants tant en termes d'infrastructure technologique, de processus ou de sécurité physique.

4.2.6 Gestion des accès

Le Ministère s'engage à mettre en place un processus formel de gestion des accès pour s'assurer que les accès à l'information sont accordés selon le principe du moindre privilège, en fonction d'un profil d'accès prédéfini basé sur le rôle assumé au sein de l'organisation et sur les besoins qui en découlent pour une période requise. L'utilisation et la consultation de l'information d'un système doivent se limiter aux seules personnes autorisées.

Le Ministère se réserve le droit de procéder au besoin à une vérification des utilisateurs qui ont accès à ses actifs informationnels dans le cadre de leurs fonctions. Ce contrôle de sécurité doit être réalisé dans le respect des droits et libertés de la personne.

4.2.7 Environnement physique

Le Ministère s'assure que les lieux physiques qu'il occupe sont adéquatement protégés, notamment contre les menaces environnementales (ex. : feu, inondation), et que des contrôles sont en place pour limiter l'accès physique aux seules personnes autorisées.

4.2.8 Acquisition, développement et maintenance des systèmes d'information

Le Ministère doit déterminer ses exigences de sécurité lors de l'acquisition de nouvelles technologies et s'assurer que ces dernières s'y conforment.

Lorsque le Ministère développe ou effectue l'entretien d'un système informatique, il doit

s’assurer d’intégrer les règles et les bonnes pratiques en matière de développement sécuritaire dans sa démarche pour s’assurer de ne pas créer de vulnérabilités.

4.2.9 Contrats et ententes de service

Le Ministère s’assure de prévoir l’obligation de respecter les règles de sécurité de l’information dans les contrats et les ententes de service conclus avec des tiers tels que des prestataires de services, des partenaires ou des mandataires.

4.2.10 Gestion des incidents de sécurité de l’information

Le Ministère met en place un processus de gestion des incidents de sécurité de l’information. Il s’assure de le faire connaître à tous les utilisateurs pour qu’ils puissent identifier et signaler, sans tarder, tout acte susceptible de constituer un manquement ou un incident de sécurité.

Les incidents ou manquements doivent être documentés dans un registre formel et signalés conformément au processus établi. Ils peuvent donner lieu à une prise de mesures correctives ou de sanctions administratives.

Le Ministère déclare au réseau d’alerte gouvernemental, selon les modalités fixées par ce dernier, tout incident de sécurité de l’information à portée gouvernementale.

4.2.11 Continuité de service

Le Ministère doit prévoir les mesures nécessaires afin de s’assurer de la continuité des activités nécessaires à la réalisation de sa mission dans un délai raisonnable lors d’un sinistre ou d’un incident majeur affectant la disponibilité de l’information jugée essentielle et stratégique.

4.2.12 Sécurité opérationnelle

Le Ministère doit documenter ses procédures opérationnelles de sécurité et s’assurer qu’elles s’inscrivent dans un cadre de gestion du changement.

Le Ministère doit s’assurer que les accès aux actifs informationnels sont journalisés sur des supports sécuritaires et permettant leur exploitation. Les journaux doivent être conservés selon un calendrier établi.

Le Ministère met en place un plan de sauvegarde et de récupération des données de ses actifs informationnels afin d’assurer ses activités de reprise et de continuité des affaires.

Le Ministère met en place un processus de gestion des vulnérabilités et des mises à jour de sécurité pour ses équipements.

4.2.13 Sécurité des communications

Le Ministère s’engage à ce que son infrastructure technologique soit conçue de façon à se prémunir des menaces afin de protéger adéquatement son information.

Le Ministère s’assure de mettre en place des pratiques pour protéger les échanges d’information, au sein de cette infrastructure ou avec des tiers, afin qu’ils puissent être faits sans compromettre la confidentialité et l’intégrité de l’information.

4.2.14 Droit de regard

Le Ministère a un droit de regard sur la manipulation et l'utilisation de ses actifs informationnels par les utilisateurs à partir des équipements normalisés du Ministère. Ce droit s'exerce en conformité avec le cadre juridique et administratif applicable au Ministère sous réserve de dispositions particulières propres à certains utilisateurs.

5. CADRE NORMATIF

La présente politique doit être interprétée et appliquée conformément aux lois, aux règlements et aux autres textes normatifs énumérés à l'annexe 1.

6. MODALITÉS D'APPLICATION

Les modalités d'application de la présente politique se retrouvent dans les documents formant le cadre normatif de la sécurité de l'information, notamment dans des politiques, des cadres de gestion, des directives, des guides et des procédures.

7. RÔLES ET RESPONSABILITÉS DES INTERVENANTS

Les rôles et responsabilités des intervenants ci-dessous sont détaillés dans le Cadre de gestion de la sécurité de l'information.

7.1. La sous-ministre

La sous-ministre est la première responsable de la sécurité de l'information relevant de son autorité. Elle doit assurer le respect des lois et des règles de sécurité de l'information déterminées par le SCT, notamment en ce qui a trait à la mise en place de mesures permettant la réduction des risques reliés à la sécurité de l'information.

7.2. Dirigeant de l'information

Le dirigeant de l'information (DI) est responsable de veiller à l'application, par chaque organisme public auquel il est rattaché, des règles de gouvernance et de gestion établies en vertu de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement.

7.3. Le responsable organisationnel de la sécurité de l'information

La sous-ministre désigne le responsable organisationnel de la sécurité de l'information (ROSI). Le ROSI joue le rôle de porte-parole du dirigeant principal de l'information (DPI) et relaie au Ministère les orientations et les priorités d'intervention gouvernementale en sécurité de l'information. Il assure la coordination et la cohérence des mesures de sécurité de l'information mises en œuvre par d'autres intervenants du Ministère. Il coordonne également la contribution du Ministère aux processus de gestion des risques et de gestion des incidents à portée gouvernementale.

7.4. Le responsable de la sécurité des actifs informationnels

Le responsable de la sécurité des actifs informationnels (RSAI) appuie et conseille le ROSI dans son rôle de coordination afin d'assurer la cohérence des mesures de sécurité mises en œuvre au Ministère.

7.5. Le conseiller organisationnel en sécurité de l'information

Le COSI apporte le soutien nécessaire aux différents intervenants, notamment en ce qui a trait à la mise en œuvre des mesures d'atténuation des risques et à la mise en place de processus formels de sécurité de l'information.

Le COSI est de plus responsable de la révision de la présente politique afin de s'assurer de son adéquation aux besoins du Ministère.

7.6. Le coordonnateur organisationnel de gestion des incidents

Le COGI est désigné par la sous-ministre et apporte le soutien technique nécessaire aux différents intervenants. Il participe activement au réseau d'alertes gouvernemental et contribue à la mise en place du processus de gestion des incidents de sécurité de l'information au sein du Ministère et du processus de gestion des incidents à portée gouvernementale.

7.7. Le détenteur de l'information

Le détenteur de l'information est une personne désignée par la sous-ministre pour assumer la responsabilité de la catégorisation des actifs informationnels et de la classification de l'information, de l'identification et de la mise en œuvre des mesures de sécurité propres à assurer la protection de l'information collectée, utilisée, communiquée, conservée ou détruite.

Chaque détenteur de l'information collabore étroitement avec les différents intervenants, notamment à la détermination des exigences de sécurité, à la gestion des incidents et à la reddition de comptes en matière de sécurité.

7.8. Le gestionnaire

Le gestionnaire doit faire connaître au personnel de son unité les règles de sécurité de l'information et veiller à leur application. Il autorise les demandes d'accès des utilisateurs aux actifs informationnels nécessaires à l'exercice de leurs fonctions et les révoque en conformité avec les règles applicables.

7.9. L'utilisateur

Tout utilisateur a l'obligation de protéger l'information mise à sa disposition par le Ministère. À cette fin, il doit notamment :

a) prendre connaissance de la présente politique, des directives, des guides et autres lignes de conduite en découlant, y adhérer et prendre l'engagement de s'y conformer;

b) signaler immédiatement à la personne désignée ou à son gestionnaire, conformément au processus établi en matière de gestion des incidents de sécurité, tout acte ou toute situation pouvant nuire à la protection de l'information;

c) utiliser, à l'intérieur des droits d'accès qui lui sont attribués et uniquement lorsqu'elle est nécessaire à l'exercice de ses fonctions, l'information mise à sa disposition en se limitant aux fins auxquelles elle est destinée;

d) respecter les mesures de sécurité mises en place sur son poste de travail et sur tout équipement contenant de l'information à protéger, et ne doit pas modifier leur configuration ni les désactiver;

e) remettre les différentes cartes d'identité et d'accès, ainsi que tout document appartenant au Ministère, à la fin de l'exercice de ses fonctions.

8. DISPOSITIONS FINALES

Sanctions et mesures disciplinaires

Toute personne qui contrevient à la présente politique ou directive en découlant s'expose à des sanctions dont des mesures disciplinaires, administratives ou à des recours judiciaires.

Lorsqu'une vérification ou une enquête permet de soupçonner qu'une infraction à une loi ou à un règlement a été commise, la sous-ministre peut également informer toute autre autorité compétente pour vérifier notamment s'il y a matière à poursuite.

Mesures d'exception

Le détenteur de l'information qui a une raison valable de ne pas se conformer à une exigence particulière ou de ne pas recourir à une mesure de sécurité déterminée peut demander une mesure d'exception au ROSI après avoir pris soin d'évaluer les risques associés à la mesure d'exception. Ces exceptions doivent être documentées et rendues disponibles au ROSI et au RSAI.

Mise en œuvre, suivi et révision

Le ROSI est chargé de la mise en œuvre des dispositions de la présente politique et de ses directives d'application.

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.

La présente politique doit être revue annuellement suivant son adoption ou à la suite d'un changement qui justifie une révision.

9. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur à compter de sa signature par la sous-ministre.

Original signé

Juliette Champagne
Sous-ministre de la Langue française

2023-03-09
Date

ANNEXE 1

CADRE JURIDIQUE ET ADMINISTRATIF

CANADA

- Charte canadienne des droits et libertés de la Loi constitutionnelle de 1982
- Code criminel, L.R., 1985, c. C-46

QUÉBEC

Lois et règlements

- Code civil du Québec, RLRQ, c. CCQ-1991
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ, c. A-2.1 :
  - ✓ Règlement sur la diffusion de l'information et sur la protection des renseignements personnels, RLRQ, c. A-2.1, r. 2
- Loi sur les archives, RLRQ, c. A-21.1
- Loi concernant le cadre juridique des technologies de l'information, RLRQ, c. C-1.1
- Charte des droits et libertés de la personne, RLRQ, c. C-12
- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, RLRQ, c. G-1.03
- Loi sur le ministère de la Justice, RLRQ, c. M-19
- Loi sur les tribunaux judiciaires, RLRQ, c. T-16

Politiques, cadres et directives

- Politique ministérielle d'utilisation du courriel, des services d'Internet et du collecticiel
- Directive sur la sécurité de l'information gouvernementale, décret 1514-2021 du 8 décembre 2021 Cadre gouvernemental de gestion - Sécurité de l'information (2014)

Langue française
Québec

Titre	Date d'entrée en vigueur
Directive sur l'attribution, l'utilisation et la gestion des appareils mobiles	**2023-03-08**
Pour information **Direction de la coordination administrative**	Date dernière mise à jour

1. CONTEXTE

La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (L.R.Q., chapitre G-1.03) et la publication de la politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics démontrent l'importance que le gouvernement accorde à la gestion des finances publiques en s'assurant que chaque dollar investi dans le domaine des ressources informationnelles ait une incidence sur l'amélioration et l'efficience des opérations de l'État. Cette directive se veut complémentaire aux orientations gouvernementales et témoigne de l'importance que le Ministère accorde à la bonne gestion concernant l'utilisation de ses ressources informationnelles.

2. OBJET

La présente directive détermine les règles et les conditions rattachées à l'attribution, l'utilisation et la gestion des appareils mobiles prêtés par le Ministère à ses employés. Elle s'applique à tous les employés du Ministère à qui celui-ci a prêté un appareil mobile, ci-après nommés « utilisateurs ».

3. DÉFINITIONS

- Appareil mobile : un appareil mobile est un appareil informatique portatif utilisable de manière autonome lors d'un déplacement.
- Téléphone voix : dispositif à main qui ne combine que les fonctions de téléphone et celles reliées à la transmission et réception de messages textes. Aucun accès à Internet n'est possible sur ces appareils;
- Téléphone intelligent : dispositif à main qui combine l'ordinateur, le téléphone et des caractéristiques de réseautage, principalement utilisé pour ses fonctions vocales, d'agenda, de répertoire téléphonique et de bloc-notes. Les avancées technologiques ont permis de lui adjoindre des fonctionnalités multimédias telles que la messagerie, le dictaphone, le lecteur MP3, la captation d'images, la vidéo, etc.
- Téléphonie CIC : service offert par le MCN visant à informatiser le service téléphonique à même les outils mobiles et ordinateurs.
- Tablette forfait internet (incluant iPad) : appareil portatif en forme de tablette, pourvu ou non d'un clavier physique, ayant pour principale interface un écran tactile, qui offre de nombreuses possibilités de personnalisation, intègre plusieurs applications et dont les fonctionnalités se rapprochent souvent de l'ordinateur de bureau. Cellulaire signifie qu'un forfait est attaché à l'appareil.
- Frais d'itinérance : frais applicables lorsque l'utilisateur sort de la zone de couverture du réseau du fournisseur, c'est-à-dire lorsqu'il quitte le Canada. Ils s'appliquent aux appels vocaux, aux messages textes, à l'envoi d'images, à l'accès Internet et aux

autres données que l'utilisateur reçoit, télécharge ou envoie lorsqu'il se trouve à l'extérieur du Canada. Des frais d'itinérance peuvent s'accumuler dès que l'utilisateur laisse son appareil en fonction pendant un déplacement à l'extérieur du Canada, car des données peuvent être émises ou reçues automatiquement.

4. LIGNES DIRECTRICES CONCERNANT L'ATTRIBUTION, L'UTILISATION ET LA GESTION DES APPAREILS MOBILES

- Le Ministère fournit un appareil mobile aux seuls employés dont la fonction au Ministère l'exige. Les appareils fournis sont ceux déterminés par le ministère de la Cybersécurité et du Numérique, lequel agit à titre de fournisseur exclusif. Les appareils au catalogue du gouvernement et les appareils homologués par le Ministère sont privilégiés.
- Par souci d'économie, d'écoresponsabilité et d'efficacité du soutien technique, les téléphones et abonnements cellulaires sont acquis par achats regroupés tels que définis dans l'article 5.2 des règlements liés à la Loi sur les contrats des organismes publics. L'appareil mis à la disposition de l'utilisateur demeure en tout temps la propriété du Ministère.
- Le Ministère et l'utilisateur veillent à la sécurité de l'information et à la protection des renseignements personnels dans l'utilisation des appareils mobiles :
  - Chaque appareil acquis et remis à un utilisateur par le Centre de services à la clientèle (CSC) est protégé par un mot de passe. Le Centre de services à la clientèle est responsable d'installer et de mettre à jour tous les dispositifs de sécurité nécessaires dans chaque appareil mobile afin de protéger l'information transmise, conservée et utilisée.
  - À des fins de sécurité, le nombre de tentatives pour entrer le mot de passe est limité sur tous les appareils mobiles. Une fois la limite atteinte sans succès, les données sont effacées automatiquement et l'appareil doit être rapporté au CSC pour réinstallation, le cas échéant.
- L'utilisation de l'appareil à des fins personnelles est permise si cela n'occasionne pas de frais supplémentaires au Ministère.
  - Seuls les appareils et les applications normalisés sont supportés par le Ministère. L'installation et l'utilisation d'autres applications engagent uniquement la responsabilité de l'utilisateur et ces dernières ne sont pas supportées ni remboursées.
- L'usage d'un appareil mobile à l'extérieur du Canada est proscrit, car il entraîne des frais d'itinérance. Exceptionnellement, un utilisateur voyageant à l'étranger pourra faire ajouter temporairement une option d'itinérance sur son appareil après avoir obtenu l'autorisation de son gestionnaire.
- Le Ministère peut facturer l'utilisateur si des frais supplémentaires s'appliquent et qu'ils ne sont pas en lien avec une utilisation professionnelle.

  Voici les situations susceptibles d'entraîner de tels frais :
  - appels et messages textes vers un autre pays;
  - utilisation à l'extérieur du Canada.

5. RÈGLES OPÉRATIONNELLES

L'utilisateur doit :

- Respecter les politiques, normes et procédures en vigueur au Ministère, notamment la Politique ministérielle sur l'éthique, la Politique ministérielle sur la sécurité de l'information, la Politique ministérielle d'utilisation du courriel, du collecticiel et des services d'Internet, ainsi que cette directive;
- Connaître et respecter les modalités d'utilisation de l'appareil;
- Utiliser l'appareil dans le respect du forfait voix ou données qui lui est applicable;
- Laisser en place les configurations de sécurité apportées à l'appareil, telles que l'obligation de protéger l'appareil par un mot de passe et permettre l'effacement à distance des données d'un appareil perdu;
- Appliquer les mises à niveau de sécurité du système d'exploitation de l'appareil mobile, lorsque celles-ci sont recommandées par le CSC;
- Maintenir la confidentialité des données et fichiers enregistrés sur l'appareil et faire preuve de discrétion lors d'une utilisation en public;
- Prendre les mesures nécessaires afin de minimiser les risques de perte, de vol, de destruction ou de détérioration de l'appareil;
- Aviser immédiatement son gestionnaire ainsi que le CSC en cas de perte, de bris ou de vol;
- Remettre l'appareil et les accessoires à son gestionnaire lors de son départ.

Actions du CSC :

- ✓ Confirmer la remise de l'appareil lors du départ d'un utilisateur ou lors d'un changement de fonctions ne répondant plus aux critères prévus à la présente directive;
- ✓ Récupérer, le cas échéant, l'appareil ainsi que les accessoires et les acheminer au CSC.

6. CRITÈRES D'ATTRIBUTION DES APPAREILS

Téléphone voix (à coût nul)

Si le besoin n'est pas couvert par le système téléphonique informatisé CIC, un appareil peut être attribué à tout membre du personnel dont la fonction demande :

- d'être accessible par téléphone, lorsque c'est nécessaire;
- de se déplacer à l'extérieur du bureau et de communiquer avec des membres de son équipe de travail durant ces déplacements.

L'autorisation pour un téléphone voix est donnée par la sous-ministre pour le secrétariat général et le Bureau de la sous-ministre ainsi que pour la Direction de la coordination administrative. Les sous-ministres adjointes autorisent les téléphones voix pour le personnel sous leur responsabilité.

Lorsqu'un rehaussement de téléphone est demandé, l'avis de la Direction de la coordination administrative doit être donné.

Téléphone intelligent (à coût nul)

Si le besoin n'est pas couvert par le système téléphonique informatisé CIC, un appareil peut être attribué à tout membre du personnel dont la fonction demande :

- d'être accessible par téléphone et par courriel, lorsque c'est nécessaire;
- de se déplacer à l'extérieur du bureau et de communiquer avec des membres de son équipe de travail durant ces déplacements;
- de prendre connaissance d'information écrite permettant d'assurer une continuité des services;
- d'intervenir pour mettre en place des mesures immédiates lors d'événements imprévus ou de situations d'urgence.

L'autorisation pour un téléphone intelligent est donnée par la sous-ministre pour le secrétariat général et le Bureau de la sous-ministre ainsi que pour la Direction de la coordination administrative. Les sous-ministres adjointes autorisent les téléphone intelligents pour le personnel sous leur responsabilité.

Lorsqu'un rehaussement de téléphone est demandé, l'avis de la Direction de la coordination administrative doit être donné.

Tablette forfait internet (incluant iPad)

L'attribution de tablettes est restreinte aux membres du personnel du cabinet, du Bureau de la sous-ministre et des sous-ministres adjointes. Toute autre demande exige une dérogation de la sous-ministre. La tablette forfait internet permet :

- de prendre connaissance d'information écrite permettant d'assurer une continuité des services;
- d'intervenir pour mettre en place des mesures immédiates lors d'événements imprévus ou de situations d'urgence.

Toute autre demande d'appareil mobile dont le critère d'attribution n'est pas énoncé ci-haut exige une dérogation de la sous-ministre.

7. SUIVI ET REDDITION DE COMPTES

Le règlement sur la diffusion de l'information et sur la protection des renseignements personnels publié sur le site Internet du Ministère exige un état de situation trimestriel sur le nombre de forfaits cellulaires et pour chacun des types d'appareils, en plus d'avoir un sommaire des acquisitions. De plus, un suivi régulier ou ponctuel sera fourni à chacune des sous-ministres adjointes.

8. MANQUEMENT À LA DIRECTIVE

L'utilisateur qui contrevient à la présente directive ou qui va à l'encontre des politiques, normes et procédures en vigueur au Ministère peut faire l'objet d'une mesure administrative ou disciplinaire selon la gravité du manquement.

9. DISPOSITIONS FINALES

La Direction de la coordination administrative est responsable de l'exécution de cette directive.

10. ENTRÉE EN VIGUEUR

La présente directive entre en vigueur à la date de sa signature par la sous-ministre.

Original signé

Juliette Champagne
Sous-ministre de la Langue française

2023-03-09
Date

Langue française
Québec

Titre	Date d'entrée en vigueur
Politique ministérielle d'utilisation du courriel, des services d'internet et du collecticiel	**2023-03-09**
Pour information **Direction de la coordination administrative**	Date dernière mise à jour

1. PRÉAMBULE

En assurant l'encadrement adéquat de l'utilisation des services des réseaux informatiques par les employés et les contractuels du ministère de la Langue française (Ministère), celui-ci répond à la fois à son obligation de veiller sur la sécurité de l'information qu'il détient dans le cadre de sa mission conformément à la Directive sur la sécurité de l'information gouvernementale (Décret 7-2014 du 15 janvier 2014) et à celle de prendre les mesures nécessaires pour mettre en œuvre la Directive concernant l'utilisation éthique du courriel, du collecticiel et des services d'Internet par le personnel de la fonction publique (C.T. 198872 du 1er octobre 2002). Cet encadrement lui permet également de se prémunir contre les risques technologiques, organisationnels et juridiques qui pourraient être engendrés par une utilisation abusive ou inappropriée de ces services.

2. OBJET

La présente politique définit les lignes directrices en matière d'utilisation des services des réseaux informatiques par les personnes visées à l'article 4. Elle énonce également les rôles et responsabilités des principaux intervenants dans l'encadrement de cette utilisation et les sanctions prévues pour tout utilisateur qui contrevient aux dispositions énoncées.

Plus précisément, elle a pour objet de fixer les règles relatives à l'utilisation des services des réseaux informatiques du Ministère afin d'assurer, notamment, l'intégrité des systèmes et la protection des renseignements personnels et confidentiels. Elle vise aussi à sensibiliser l'utilisateur relativement à ses obligations quant à l'utilisation des services des réseaux informatiques mis à sa disposition dans le cadre de son emploi et les gestionnaires quant à leur responsabilité de veiller à la sécurité des actifs informationnels du Ministère.

Les services des réseaux informatiques comprennent le courriel, les services d'Internet et les collecticiels, y compris, sans s'y restreindre, la participation à des groupes de discussion, les médias sociaux, les services de partage ou toute autre application utilisant les services d'Internet, sans égard au type d'équipement ministériel utilisé.

3. CADRE LÉGAL ET ADMINISTRATIF

Les lois, règlements et autres textes normatifs sur lesquels s'appuie la présente politique sont énumérés à l'annexe 1.

4. CHAMP D'APPLICATION

La présente politique s'adresse à tout utilisateur qui utilise les services des réseaux informatiques du Ministère, c'est-à-dire tout le personnel ainsi que toute autre personne dûment autorisée à y avoir accès, notamment un consultant, un partenaire, un fournisseur ou un employé d'un autre ministère ou organisme.

5. LIGNES DIRECTRICES

5.1. L'utilisateur peut faire usage des services des réseaux informatiques du Ministère à des fins professionnelles ainsi qu'à des fins personnelles limitées.

5.2. L'utilisation des services des réseaux informatiques à des fins personnelles constitue un privilège consenti par le Ministère. En conséquence, cette utilisation doit respecter les principes suivants :

- se faire occasionnellement;
- se limiter au strict minimum;
- ne pas nuire aux activités professionnelles;
- n'impliquer aucun frais supplémentaire et;
- ne causer aucun préjudice au Ministère ainsi qu'à son image.

5.3. L'utilisateur ne peut utiliser un accès aux services des réseaux informatiques ministériel notamment pour :

- télécharger tout logiciel incluant les gratuiciels, partager ou copier un logiciel installé sur l'équipement ministériel auquel l'utilisateur a accès, sans obtenir une autorisation préalable conformément à l'article 6.2 c);
- créer sciemment une interférence sur le réseau local ou porter atteinte à la sécurité du réseau;
- utiliser à son profit personnel ou professionnel lié à tout autre emploi rémunéré ou non, les équipements ministériels mis à sa disposition;
- exprimer ses opinions, préférences politiques ou livrer des commentaires liés à l'activité judiciaire de manière incompatible avec ses obligations déontologiques ou son code d'éthique;
- participer à une chaîne de lettre;
- harceler ou importuner une personne;
- visionner, télécharger, copier, partager, expédier ou conserver des images ou des fichiers érotiques, de sexualité explicite ou de pornographie juvénile ou dont le contenu a un caractère diffamatoire, offensant, harcelant, haineux, violent, menaçant, raciste, sexiste ou qui contrevient aux libertés et aux droits fondamentaux;
- créer, expédier ou réexpédier tout message électronique ou fichier qui contient un élément contraire aux prescriptions qui précèdent ou qui est susceptible d'affecter le fonctionnement de l'équipement mis à la disposition de l'utilisateur ou d'un réseau gouvernemental auquel il est relié;
- diffuser massivement des courriels de manière intentionnelle, à moins d'avoir obtenu l'autorisation préalable d'un gestionnaire;
- faire un usage qui irait à l'encontre des normes éthiques et déontologiques applicables.

5.4. La sous-ministre peut exceptionnellement autoriser un utilisateur, lorsque la nature des fonctions de ce dernier l'exige, à utiliser les services des réseaux informatiques à des conditions différentes de celles prévues à la présente politique.

5.5. L'utilisateur doit faire usage des services des réseaux informatiques à une fréquence et selon une durée qui est compatible avec sa prestation de travail.

5.6. La communication de renseignements personnels et confidentiels visés notamment par la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, c. A-2.1) et concernant une personne autre que l'usager lui-même, ne peut être effectuée par l'intermédiaire des services des réseaux informatiques à moins d'employer préalablement une méthode appropriée pour rendre cette information inintelligible ou inaccessible aux personnes autres qu'à celles à qui elle est destinée.

5.7. L'utilisation des services des réseaux informatiques doit se faire dans le respect des lois et règlements en vigueur au Québec, notamment la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, plus particulièrement quant à la collecte, l'utilisation, la communication, la conservation ou, selon le cas, l'archivage ou la destruction d'un renseignement personnel, la Loi concernant le cadre juridique des technologies de l'information (RLRQ c. C-1.1), la Loi sur les archives (RLRQ, c. A-21.1), la Loi sur la fonction publique (RLRQ, c. F-3.1.1) et la Loi sur le droit d'auteur (L.R.C. (1985), c. C-42).

5.8. Dans le cadre de ses fonctions, l'utilisateur des services des réseaux informatiques :

- emploie les codes d'accès, les mots de passe ou tout autre mécanisme de contrôle d'accès qu'il est autorisé à utiliser, sans les faire connaître aux personnes qui n'ont pas obtenu les mêmes accès y compris, sans s'y restreindre, au personnel d'assistance informatique ou ses gestionnaires;
- utilise l'adresse courriel organisationnelle lors de l'inscription à des sites Internet, des forums de discussion ou des abonnements à des lettres de nouvelles, à moins d'une autorisation expresse de son gestionnaire;
- s'identifie dans tous ses messages électroniques;
- se soucie de préserver l'image du Ministère dans ses messages électroniques;
- veille à la conservation de ses courriels ou de ses échanges lorsqu'ils constituent des documents visés par le calendrier de conservation que l'on retrouve au manuel de gestion documentaire du Ministère, approuvé en vertu de la Loi sur les archives;
- utilise un langage correct, poli et approprié et porte une attention particulière à la qualité de la langue française.

5.9. L'utilisateur qui s'inscrit sur des sites Internet, des forums de discussion ou des abonnements à des lettres de nouvelles dans le cadre d'une utilisation personnelle, fait usage de son adresse courriel personnelle.

5.10 L'utilisateur qui navigue sur les services des réseaux informatiques :

- effectue la cueillette d'information dans le respect des droits d'auteur;
- quitte immédiatement un site ou un forum dont le contenu contrevient aux dispositions de la présente politique ou peut nuire à l'image du Ministère;
- lorsqu'une authentification est requise, utilise un mot de passe dont la conception est logiquement différente de son mot de passe utilisé sur le réseau local du Ministère.

6. RÔLES ET RESPONSABILITÉS DES PRINCIPAUX INTERVENANTS

6.1. La Direction de la coordination administrative par l'entremise de son entente de services avec le ministère de la Cybersécurité et du Numérique,

- Élabore et met en place des mécanismes de contrôle pour s'assurer du respect de la présente politique incluant un journal d'utilisation des services des réseaux informatiques du Ministère;
- Surveille les réseaux informatiques afin d'en assurer la sécurité et identifie les évènements de sécurité qui nécessitent une intervention particulière;
- Autorise, à des fins professionnelles, le téléchargement de logiciels, incluant les gratuiciels, ainsi que le partage ou la copie d'un logiciel installé sur l'équipement ministériel, dans le respect des règles relatives au droit d'auteur et aux exigences de sécurité du Ministère;
- Élabore un plan d'action pour correction des écarts à la suite de la réception des recommandations provenant de rapports d'audit ou de vérification d'un organisme contrôleur ou du ministère de la Cybersécurité et du Numérique et veille à sa mise en place;
- Révise la présente politique à la demande de la sous-ministre;
- Répond aux demandes de consultation des utilisateurs à l'égard des informations les concernant contenues au journal d'utilisation des services des réseaux informatiques du Ministère;
- Produit le journal d'utilisation des services des réseaux informatiques d'un utilisateur ciblé à la demande de la Direction de la coordination administrative et collabore aux enquêtes administratives, le cas échéant.

6.3. La Direction chargée de l'audit interne, des enquêtes et de l'évaluation de programmes au Ministère ou l'unité mandatée par impartition dans le cadre d'une entente interministérielle;

a) Procède, à l'égard d'un utilisateur ciblé, à une enquête administrative portant sur le respect de l'application de la présente politique à la suite d'une demande formulée par un gestionnaire et autorisée par un membre désigné du CDM.

6.4. La Direction de la coordination administrative (DCA)

- S'assure du suivi de l'évolution des risques éthiques associés à l'utilisation des services des réseaux informatiques;
- Sensibilise le personnel à l'utilisation éthique des services des réseaux informatiques mis à leur disposition par le Ministère;
- En collaboration avec le gestionnaire, oriente la démarche à entreprendre vis-à-vis un employé soupçonné de ne pas respecter la présente politique;
- Procède à une enquête administrative portant sur la navigation Internet d'un utilisateur ciblé à la suite d'une demande formulée par un gestionnaire;
- Selon les résultats de l'enquête administrative effectuée, la DCA détermine les mesures à prendre vis-à-vis l'employé et s'assure de la mise en application.

6.5. La Direction des communications (DCOM)

- Diffuse l'information pertinente relativement à l'application et au respect de la présente politique sur le site intranet du Ministère dont le contenu a été élaboré en collaboration avec les directions concernées;
- Diffuse, sur le site Internet du Ministère, un avertissement stipulant que les messages électroniques adressés aux personnes visées par la présente politique peuvent être contrôlés et surveillés par les autorités du Ministère;
- Coordonne l'application des normes concernant l'édition et la publication de documents sur les services des réseaux informatiques;
- Définit les orientations en matière d'utilisation des médias sociaux.

6.6. Le comité ministériel de la sécurité de l'information (CMSI)

- Détermine les éléments du journal d'utilisation des services des réseaux informatiques qui peuvent faire l'objet de surveillance constante;
- S'assure que les mécanismes en place répondent aux besoins de surveillance.

6.7. Le responsable organisationnel de la sécurité de l'information (ROSI)

- En collaboration avec les autres intervenants du Ministère, fait un bilan annuel au CMSI sur l'application de la présente politique et, s'il y a lieu, formule des recommandations ou en propose des modifications à la sous-ministre.

6.8. Le conseiller organisationnel à la sécurité de l'information (COSI)

- Élabore un rapport de vérification de l'utilisation des réseaux informatiques du Ministère et, le cas échéant, communique au ROSI les recommandations de redressement de situation;
- S'assure de la mise en place des contrôles de sécurité nécessaires pour assurer la confidentialité et l'intégrité du journal d'utilisation des réseaux informatiques du Ministère.

6.9. Le gestionnaire

- Veille à la participation de son personnel aux séances de sensibilisation ou d'information quant à l'utilisation des services des réseaux informatiques du Ministère;
- Veille, par la supervision de son personnel, à ce que les services des réseaux informatiques soient utilisés en conformité avec la présente politique;
- S'adresse à la DCA pour évaluer la pertinence d'une enquête administrative portant sur le respect de l'application de la présente politique. Le cas échéant, il adresse une demande d'autorisation d'enquête administrative auprès d'un membre désigné par les hautes autorités pour qu'il y ait une telle enquête à l'égard d'un utilisateur ciblé;
- S'assure, pour toute personne qui ne fait pas partie du personnel du Ministère et à laquelle il a permis l'accès aux services des réseaux informatiques, que la présente politique est respectée par l'entremise d'un engagement contractuel.

6.10 L'utilisateur

- Prend connaissance de la présente politique sur l'utilisation des services des réseaux informatiques et veille à s'y conformer;
- Prend des mesures raisonnables pour contrôler l'utilisation de son mot de passe ou tout autre mécanisme de contrôle d'accès qu'il est autorisé à utiliser en conformité

avec les exigences de sécurité du Ministère;

- Participe aux séances de sensibilisation ou d'information quant à l'utilisation des services des réseaux informatiques du Ministère;
- Utilise les équipements et les services des réseaux informatiques de manière à éviter, dans la mesure du possible, l'encombrement que peuvent produire notamment les envois massifs, le téléchargement de fichiers volumineux ou l'écoute en continu;
- En regard de ses fonctions et du temps à y consacrer, évalue la pertinence avant d'adhérer à un forum de discussions et en avise son gestionnaire. Il informe ses interlocuteurs que son opinion n'engage que lui-même, sauf s'il a pour mandat d'agir comme représentant du Ministère;
- Communique avec son gestionnaire lorsqu'il désire consulter les informations le concernant contenues au journal d'utilisation des services des réseaux informatiques du Ministère;
- S'il possède un compte à privilèges élevés, s'assure de ne pas utiliser ce compte pour naviguer sur Internet.

7. EXIGENCES EN MATIÈRE DE SURVEILLANCE

Toute information conservée ou transigeant sur l'équipement ministériel, au moyen des services des réseaux informatiques, est réputée constituer une information à laquelle le Ministère a accès. À cet égard, le Ministère possède les outils technologiques permettant de déchiffrer les communications initiées ou destinées à son réseau.

L'analyse des journaux d'utilisation des services des réseaux informatiques du Ministère est effectuée périodiquement afin de s'assurer du respect de la présente politique, conformément aux pratiques usuelles du MCN, dans le cadre de l'entente de services informatiques.

L'enquête administrative prévue à l'article 6.3 est effectuée lorsqu'il y a des motifs raisonnables de soupçonner qu'il y a une utilisation des services des réseaux informatiques qui n'est pas conforme à la présente politique. La lecture du contenu d'un courriel peut être effectuée uniquement dans le cadre d'une telle enquête et ne doit pas aller au-delà de ce qui est requis.

La mise en œuvre des mesures de contrôle prévues dans la présente section doit être faite conformément à la loi, notamment à l'égard de la protection de la vie privée, des renseignements personnels et confidentiels.

8. DISPOSITIONS PARTICULIÈRES

Le ROSI est chargé de la mise en application, du suivi et de la révision de la présente politique.

9. SANCTION

Lorsqu'un utilisateur contrevient aux dispositions de la présente politique de même qu'aux dispositions énoncées au cadre légal et administratif de l'Annexe 1, il s'expose à des mesures disciplinaires, administratives ou légales selon la faute commise. Ces mesures peuvent inclure la suspension des privilèges informatiques, la réprimande, la suspension, le congédiement ou autre, et ce, conformément aux dispositions des conventions collectives, des ententes ou des contrats.

10. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur à sa signature par la sous-ministre.

Original signé

Juliette Champagne
Sous-ministre de la Langue française

2023-03-10
Date

ANNEXE 1

CADRE LÉGAL ET ADMINISTRATIF

CANADA

- Charte canadienne des droits et libertés de la Loi constitutionnelle de 1982;
- Code criminel, L.R., 1985, c. C-46;
- Loi sur le droit d'auteur, L.R., 1985, c. C-42.

QUÉBEC

Lois et règlements

- Code civil du Québec, RLRQ c. CCQ-1991;
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ, c. A-2.1 :
  - ✓ Règlement sur la diffusion de l'information et sur la protection des renseignements personnels, RLRQ, c. A-2.1, r. 2;
- Loi concernant le cadre juridique des technologies de l'information, RLRQ, c. C-1.1;
- Charte des droits et libertés de la personne, RLRQ, c. C-12;
- Loi sur la fonction publique, RLRQ, c. F-3.1.1 :
  - ✓ Règlement sur l'éthique et la discipline dans la fonction publique, RLRQ, c. F-3.1.1, r. 3;
- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, RLRQ, c. G-1.03;
- Loi sur le directeur des poursuites criminelles et pénales, RLRQ, c. D-9-1-1;
- Loi sur les archives, RLRQ, c. A-21.1

Directives et politiques

- Directive sur l'utilisation du courriel, d'un collecticiel et des services d'Internet par le personnel de la fonction publique;
- Directive sur la sécurité de l'information gouvernementale;
- Directive sur la communication de renseignements confidentiels en vue d'assurer la protection des personnes;
- Politique ministérielle de sécurité de l'information;
- Politique ministérielle de gestion documentaire;
- Politique ministérielle sur l'éthique.

ANNEXE II

DÉFINITIONS

Chiffrement : opération par laquelle est substitué à un texte en clair, un texte inintelligible et inexploitable pour quiconque ne possède pas la clé permettant de le ramener à sa forme initiale.

Collecticiel : logiciel qui permet à des utilisateurs reliés par un réseau de travailler en collaboration sur un même projet.

Message électronique : document informatisé qu'un utilisateur saisit, envoie ou consulte par l'intermédiaire d'un réseau. Comprends notamment le courriel, la messagerie instantanée, le forum de discussion, la publication sur un fil d'actualité, etc.

Courriel : service de correspondance sous forme d'échange de messages électroniques, à travers un réseau informatique. Par extension, message transmis par un utilisateur vers un ou plusieurs destinataires, d'ordinateur à ordinateur, par l'intermédiaire d'un réseau informatique.

Fichier : collection d'informations consignée et stockée comme une entité unique et spécifique sur un support de stockage.

Internet : réseau informatique mondial constitué d'un ensemble de réseaux nationaux, régionaux et privés, qui sont reliés par le protocole de communication TCP-IP et qui coopèrent dans le but d'offrir une interface unique à leurs utilisateurs.

Renseignement personnel : renseignement qui concerne une personne physique et qui permet de l'identifier.

Renseignement confidentiel : renseignement dont la divulgation aurait des incidences néfastes, notamment sur les relations intergouvernementales, les négociations entre organismes publics, l'économie, les tiers relativement à leurs secrets industriels, l'administration de la justice et la sécurité publique, les décisions administratives ou politiques et la vérification.

Réseau : système de transmission interconnectant tous les clients et les services ainsi que tout le matériel et les logiciels afférents.

Compte à privilèges élevés : compte réseau dont les droits octroyés permettent de gérer d'autres utilisateurs, d'installer des applications, d'administrer des serveurs ou des postes de travail, etc.

Équipement ministériel : appareil permettant la mise en réseau d'information et dont l'acquisition et la configuration est réalisée par le Ministère. Comprends notamment les ordinateurs, les téléphones intelligents, les tablettes, etc.