

Politique sur l'accès à l'information et sur la protection des renseignements personnels	
---	--

Émise le 2014-03-31	Révisée le
-------------------------------	-------------------

Prochaine révision prévue le 2019-03-31	Codification PR-01-00-00
---	------------------------------------

1. Contexte

Le ministère de l'Emploi et de la Solidarité sociale offre des services à des clientèles très diversifiées : chercheurs d'emploi, personnes démunies financièrement, parents d'un nouvel enfant, entreprises, utilisateurs des services d'état civil, organismes communautaires ainsi que tout citoyen désirant un accès simplifié à des services publics. L'organisation des services y est fortement décentralisée et les trois quarts des ressources humaines œuvrent en région en partenariat avec le milieu. Pour accomplir sa mission, le Ministère recueille, produit et utilise une information abondante à l'égard de ses clientèles, renseignements souvent sensibles.

Ainsi, dans un environnement technologique offrant des possibilités sans cesse croissantes de circulation d'information, le Ministère reconnaît l'importance d'assurer la protection des renseignements personnels qui lui sont confiés par sa clientèle, ses partenaires et ses employés. Par ailleurs, des appels à une plus grande ouverture et transparence exercent une pression croissante sur les gouvernements afin que ceux-ci facilitent l'accès à l'information. Le Ministère souhaite donc jouer son rôle en promouvant une divulgation plus proactive et en facilitant l'exercice du droit d'accès reconnu par la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (Loi sur l'accès).

Le respect des obligations de la Loi sur l'accès et du Règlement sur la diffusion et sur la protection des renseignements personnels (Règlement sur la diffusion) est une responsabilité partagée qui exige la participation active de tous les employés du Ministère. C'est donc dans une approche de mobilisation du personnel qu'est adoptée la présente politique.

2. Références

Les renseignements détenus par le Ministère, ses contractants et son personnel doivent être protégés, traités et diffusés conformément aux

principes énoncés dans la Loi sur l'accès (L.R.Q., c. A-2.1), dans la Charte des droits et libertés de la personne (L.R.Q., c. C-12), dans le Code civil du Québec et dans le Règlement sur la diffusion (c. A-2.1, r. 2). D'autres fondements légaux encadrent également les activités reliées à l'accès à l'information et à la protection des renseignements personnels (cf. annexe I).

3. Définitions¹

Bris de confidentialité : toute divulgation illégale de renseignements confidentiels, et ce, peu importe le support sur lequel ils se trouvent (papier, clé USB, ordinateur portable, tablette numérique, disquette, téléphone intelligent, etc.) et tout accès non autorisé à des renseignements personnels. Les situations les plus courantes surviennent lorsque des renseignements personnels sur la clientèle ou sur des membres du personnel sont volés ou perdus, communiqués ou consultés illégalement. Ces bris peuvent être intentionnels ou accidentels. Ils peuvent résulter d'une erreur humaine ou de la défaillance d'un système.

Contractant : toute personne morale (à but lucratif ou non lucratif), une société ou une personne physique qui conclut un contrat d'approvisionnement ou un contrat de services ou réalisant des travaux de construction pour le Ministère.

Cycle de vie d'un renseignement (cycle de vie de l'information) : l'ensemble des étapes que franchit un renseignement qui vont de sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation du ministère ou de l'organisme.

Détenteur de l'information : un employé désigné par son organisme public, appartenant à la classe d'emploi de niveau cadre ou à une classe d'emploi de niveau supérieur, et dont le rôle est, notamment, de s'assurer de la sécurité de l'information et des ressources qui la sous-tendent, relevant de la responsabilité de son unité administrative.

Document : un document est constitué d'information portée par un support (numérique, papier, électronique, bande magnétique, vidéo ou autre). L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles réinscriptibles sous l'une de ces formes ou en un autre système de symboles. Est assimilée au document toute

¹ Les définitions inscrites dans ce glossaire sont extraites de diverses sources ou en sont largement inspirées dont la Directive sur la sécurité de l'information gouvernementale, la Loi concernant le cadre juridique des technologies de l'information, la politique de gestion de la sécurité de l'information (MESS) et le grand dictionnaire terminologique de l'Office québécois de la langue française (OQLF).

banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite.

Incident de sécurité de l'information : conséquence observable de la concrétisation d'un risque de sécurité de l'information nécessitant une intervention.

Personnel : toute personne à l'emploi du ministère de l'Emploi et de la Solidarité sociale.

Protection des renseignements personnels : la protection des renseignements personnels englobe les droits et les obligations des personnes et des organisations en ce qui a trait à la collecte, à l'utilisation, à la communication et à la conservation des renseignements personnels.

Renseignement confidentiel : renseignement dont l'accès est assorti d'une ou plusieurs restrictions prévues par la Loi sur l'accès, notamment un renseignement ayant une incidence sur les relations intergouvernementales, sur l'économie, sur l'administration de la justice et la sécurité publique, sur les décisions administratives ou politiques ou sur la vérification. Est également confidentiel un renseignement fourni par un tiers et qui constitue un secret industriel ou un renseignement financier, commercial, scientifique, technique ou syndical. Sont également confidentiels les renseignements personnels, sauf dans les cas prescrits par la Loi.

Renseignement personnel : renseignement qui concerne une personne physique et qui permet de l'identifier, notamment, mais non limitativement, les renseignements relatifs à l'identité (le nom, le prénom, la date de naissance, le numéro d'assurance sociale, le numéro de permis de conduire, le numéro d'assurance maladie), les renseignements à caractère financier (information sur les comptes bancaires, dossier de crédit), les caractéristiques d'une personne (origine ethnique, religion, expérience de travail, scolarité, état de santé), la photographie, la vidéo d'une personne, les données biométriques (empreintes digitales, iris, voix).

Renseignement sensible : tout renseignement portant sur les allégeances individuelles ou protégé par la Charte des droits et libertés de la personne, dont les renseignements sur la religion, l'orientation sexuelle et les allégeances politiques. Un renseignement peut être à la fois personnel, confidentiel et sensible, par exemple un renseignement médical ou fiscal.

Registre : banque d'informations qui recense les dossiers, les fichiers, les réalisations, les activités ou les événements relatifs à l'accès et à la protection des renseignements personnels, peu importe le support sur lequel elle est conservée.

Sécurité de l'information : ensemble des moyens technologiques, humains, organisationnels, juridiques et éthiques permettant d'assurer la réalisation des objectifs de disponibilité, d'intégrité et de confidentialité de l'information.

4. Portée

Cette politique s'applique à tout le personnel du Ministère, ses gestionnaires et ses dirigeants ainsi qu'aux contractants ayant accès à des renseignements du Ministère. Elle s'applique à tout renseignement détenu par le Ministère ou par un tiers pour son compte, et ce, durant tout son cycle de vie.

Cette politique s'applique également aux renseignements détenus par le Directeur de l'état civil (DEC), sauf en ce qui concerne les actes et les registres de l'état civil, qui sont régis par le Code civil du Québec et dont les mesures d'accès et de protection doivent être déterminées et assumées par le directeur de l'état civil en tant qu'officier public. Les renseignements détenus par le DEC sont donc soumis à un régime mixte de protection.

La politique énonce les principes directeurs et établit le partage des responsabilités à l'égard de sa mise en œuvre.

5. Énoncé de la politique

Prenant appui sur les valeurs importantes de la société québécoise que sont la transparence et l'ouverture entre l'État et les citoyens et le respect de la vie privée, le Ministère s'engage à :

- protéger les renseignements personnels qui lui sont confiés, par l'application des mesures nécessaires, durant tout le cycle de vie de l'information;
- favoriser la diffusion des documents administratifs d'intérêt qui ne sont pas confidentiels, en adoptant un mode de divulgation davantage proactif;
- faciliter l'exercice du droit d'accès en prêtant assistance aux demandeurs et en s'assurant de transmettre, dans les meilleurs délais, des réponses précises et complètes;
- favoriser, chaque fois que cela est envisageable, la communication des documents faisant l'objet d'une demande d'accès dans la mesure prévue par la Loi sur l'accès.

6. Principes directeurs

- **Le respect et la confiance des personnes**

L'accessibilité de l'information et la protection des renseignements personnels détenus par le Ministère au sujet de ses employés, de ses partenaires et de ses clientèles contribuent au développement d'une relation de service basée sur le respect et la confiance.

- **La réalisation de la mission du Ministère**

L'information est un actif essentiel à la réalisation de la mission du Ministère. Les mesures prises en matière d'accès et de protection des renseignements personnels doivent concourir à l'atteinte des objectifs du plan stratégique ministériel.

- **L'instauration de mesures préventives et proactives**

En matière de protection des renseignements personnels, une approche préventive est privilégiée. Elle consiste à prévenir les risques d'atteinte à la vie privée, notamment par la formation et la sensibilisation, par une démarche continue d'identification et d'évaluation des risques et par des mesures de protection qui sont réévaluées régulièrement afin de tenir compte des changements organisationnels et technologiques.

En matière d'accès à l'information, une divulgation proactive de l'information est adoptée afin de favoriser la transparence et de maintenir le lien de confiance des différentes clientèles envers la gestion du Ministère.

- **La mise en place d'une approche intégrée**

La protection des renseignements personnels est prise en compte dès la conception de nouvelles mesures, de nouveaux programmes ou du développement de systèmes d'information.

La communication de l'information non confidentielle est prévue dès l'élaboration de documents de façon à optimiser la diffusion proactive de l'information.

- **La valorisation de la collaboration**

L'accès à l'information et la protection des renseignements personnels sont des responsabilités partagées, individuellement par chaque membre du personnel et par chaque contractant, et collectivement par l'organisation. La collaboration de chacun assure l'efficacité, l'uniformité et la conformité de l'application des règles en ces domaines.

- **L'imputabilité et la responsabilité**

Le respect de la présente politique exige l'attribution claire de responsabilités à tous les niveaux, une imputabilité des personnes selon leur niveau de responsabilité et une reddition de comptes régulière, notamment dans le rapport annuel de gestion.

7. Objectifs

La présente politique a pour objectifs :

- de favoriser une application efficace et uniforme de la Loi sur l'accès et du Règlement sur la diffusion au sein du Ministère, selon les responsabilités définies par la présente politique;
- de responsabiliser l'ensemble du personnel en matière d'accès aux documents et de protection des renseignements personnels.

8. Rôles et responsabilités

L'action concertée des divers intervenants est nécessaire afin d'assurer le respect de la présente politique. Le partage de leurs responsabilités en la matière est le suivant :

- **La ou le sous-ministre**

La personne assumant la fonction de sous-ministre est la première responsable de l'accès à l'information et de la protection des renseignements personnels. En outre, cette personne :

- s'assure du respect de la loi et des règlements ainsi que de la présente politique et des cadres normatifs, tant gouvernementaux que ministériels, en matière d'accès à l'information et de protection des renseignements personnels;
- approuve les orientations ministérielles en matière d'accès à l'information et de protection des renseignements personnels;
- rend compte, dans le rapport annuel de gestion, de la diffusion des documents visés par le Règlement sur la diffusion ainsi que du traitement des demandes d'accès et des activités relatives à l'accès à l'information et à la protection des renseignements personnels;
- veille à la sensibilisation et à la formation des membres du personnel et du personnel d'encadrement sur les obligations et les pratiques en matière d'accès à l'information et en protection des renseignements personnels;
- désigne une personne responsable de l'accès et de la protection des renseignements personnels et son substitut.

○ **Le comité ministériel sur la protection des renseignements personnels et sur l'accès et la sécurité de l'information**

Le comité est chargé de soutenir la ou le sous-ministre dans l'exercice de ses responsabilités et obligations. Il est présidé par la ou le sous-ministre et est composé, notamment, de la responsable ou du responsable de l'accès aux documents et de la protection des renseignements personnels, de la dirigeante sectorielle ou du dirigeant sectoriel de l'information², de la responsable organisationnelle ou du responsable organisationnel de la sécurité de l'information, de la conseillère organisationnelle ou du conseiller organisationnel en sécurité de l'information, des détentrices ou des détenteurs de l'information, d'une représentante ou d'un représentant de la Direction des communications, d'une représentante ou d'un représentant de la Direction générale adjointe des ressources humaines, d'une représentante ou d'un représentant de la Direction des affaires juridiques ainsi que des personnes responsables de la gestion des technologies de l'information, de la vérification interne, de la gestion documentaire, de la sécurité physique et de la coordination ministérielle en éthique.

En matière d'accès et de protection des renseignements personnels, le comité a comme principales responsabilités :

- de soutenir et conseiller la sous-ministre dans l'exercice de ses responsabilités et obligations en matière d'accès à l'information et de protection des renseignements personnels;
- de s'assurer que tout projet d'acquisition de biens et services en technologie de l'information, tout projet de développement et/ou de refonte de système d'information ou de prestation électronique de services, qui recueille, utilise, conserve, communique ou détruit des renseignements personnels comportent les mesures particulières suivantes en matière de protection des renseignements personnels;
- d'être informé de tout projet de sondages et établir les mesures à respecter en matière de protection des renseignements personnels comprenant une évaluation de la nécessité de recourir à un sondage à l'évaluation de son aspect éthique;
- d'être informé de tout projet de vidéosurveillance et établir les mesures particulières à respecter.

○ **La ou le responsable de l'accès et de la protection des renseignements personnels**

La personne responsable de l'accès et de la protection des renseignements personnels est désignée par la ou le sous-ministre. Elle coordonne les actions

² Cette personne, désignée en application de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03), veille à l'application, par les organismes publics qui lui sont rattachés, des règles de gouvernance et de gestion établies en matière de sécurité de l'information.

ministérielles nécessaires à l'application de la Loi sur l'accès. Elle doit notamment :

- conseiller la ou le sous-ministre dans l'exercice de ses responsabilités en matière d'accès et de protection des renseignements personnels;
- veiller au respect des obligations du Ministère en matière de collecte, d'utilisation, de conservation, de communication et de destruction des renseignements personnels et, à ce titre, émettre des avis relatifs à l'accès et à la protection des renseignements personnels;
- proposer et mettre en place les mesures nécessaires dans toutes les unités administratives du Ministère afin d'assurer la protection des renseignements personnels et faciliter l'accès à l'information;
- participer au comité ministériel sur la protection des renseignements personnels et sur l'accès et la sécurité de l'information et soumettre les problématiques nécessitant des orientations;
- traiter les demandes relatives à l'accessibilité des documents administratifs et des renseignements personnels détenus par le Ministère et rendre les décisions afférentes;
- rendre les décisions quant à la rectification d'un renseignement personnel détenu par le Ministère;
- s'assurer du respect des règles adoptées par le Ministère en matière de gestion des bris de confidentialité;
- agir comme témoin auprès de la Commission d'accès à l'information (CAI) lors de la contestation d'une décision;
- exercer un rôle-conseil dans la rédaction d'une entente d'échange de renseignements personnels et de son approbation par la CAI, le cas échéant;
- planifier et réaliser, en collaboration avec la Direction des communications et la Direction générale adjointe des ressources humaines, la tenue d'activités régulières de sensibilisation et de formation;
- tenir les registres ministériels prévus par la Loi sur l'accès;
- attester de la conformité des sondages en matière de protection des renseignements personnels lorsqu'ils nécessitent la collecte, l'utilisation, la communication ou la conservation de tels renseignements.

○ **La responsable organisationnelle ou le responsable organisationnel de la sécurité de l'information (ROSI)**

Cette personne joue le rôle de porte-parole de la dirigeante ou du dirigeant principal de l'information auprès de son organisation et lui relaie les informations et les priorités d'intervention gouvernementales en sécurité de l'information. La ou le ROSI assiste la personne dirigeant l'organisme public dans la détermination des orientations stratégiques et des priorités d'intervention et la représente en matière de déclaration des incidents de sécurité de l'information à portée gouvernementale. La ou le ROSI a en outre pour responsabilités :

- de soumettre à la consultation du comité, chargé de la sécurité de l'information de son organisation, les orientations, les politiques, les directives et les cadres de gestion, les priorités d'actions, les éléments de reddition de comptes ainsi que tout événement ayant mis ou qui aurait pu mettre en péril la sécurité de l'information;
- d'assurer la coordination et la cohérence des actions de sécurité de l'information menées au sein de son organisation par d'autres intervenants dont, notamment, les détentrices et les détenteurs de l'information, 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;
- de s'assurer de la contribution de son organisation au processus de gestion des risques et des incidents de sécurité de l'information à portée gouvernementale;
- de définir et mettre en œuvre les processus formels de sécurité de l'information portant sur la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents ayant mis ou qui auraient pu mettre en péril la sécurité de l'information gouvernementale;
- de s'assurer de la prise en charge des exigences de sécurité de l'information lors de la réalisation de projets de développement ou de l'acquisition de systèmes d'information;
- de coordonner l'élaboration et la mise en œuvre d'un programme formel et continu de formation et de sensibilisation en matière de sécurité de l'information.

○ **La conseillère organisationnelle ou le conseiller organisationnel en sécurité de l'information (COSI)**

La ou le COSI apporte son soutien au ROSI au niveau tactique, notamment en ce qui a trait à la mise en œuvre des mesures de mitigation des risques et à la mise en place des processus formels de sécurité de l'information. Au-delà de son rôle de soutien au ROSI, la ou le COSI est notamment chargé :

- de mettre en œuvre les orientations internes découlant des directives gouvernementales, des politiques internes et des pratiques généralement admises à cet égard;
- de produire les bilans et les plans d'action de sécurité de l'information;
- de participer aux négociations des ententes de service et des contrats et de formuler des recommandations quant à l'intégration de dispositions garantissant le respect des exigences de sécurité de l'information;
- de tenir à jour le registre d'autorité de la sécurité de l'information;
- d'assister les détentrices et les détenteurs de l'information dans la catégorisation de l'information relevant de leur responsabilité et dans la réalisation des analyses de risques de sécurité de l'information;
- de contribuer à la mise en œuvre des processus formels de sécurité de l'information de son organisation.

○ **La responsable ou le responsable de la gestion des technologies de l'information**

La personne responsable de la gestion des technologies de l'information veille à :

- contribuer à l'élaboration et à la mise en œuvre de directives propres à assurer la sécurité de l'information numérique;
- mettre en œuvre les mesures permettant d'assurer la sécurité de l'information numérique détenue par le Ministère, dont les plans de reprise informatique en cas de sinistre;
- mettre en place un cadre normatif de développement assurant la sécurité de l'information, y compris celles reliées au respect des exigences légales de protection des renseignements personnels, lors de la réalisation d'un projet de développement ou lors de l'acquisition d'un système d'information.

○ **Les détentrices et les détenteurs de l'information**

Les personnes détentrices de l'information, désignées par la dirigeante ou le dirigeant d'un organisme public, sont responsables d'assurer la protection des renseignements personnels et la sécurité de l'information des renseignements qu'ils détiennent ou qu'ils utilisent. Les personnes ainsi désignées figurent au registre d'autorité de la sécurité. Celui-ci inventorie les systèmes d'information et leurs détenteurs. Ceux-ci sont notamment chargés :

- de participer à l'élaboration des orientations stratégiques, des politiques, des directives, des cadres de gestion, des guides, des plans d'action et des bilans;
- de catégoriser l'information relevant de leur responsabilité selon la valeur en termes de disponibilité, d'intégrité et de confidentialité;
- de 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;
- de s'assurer de l'adéquation des mesures de sécurité de l'information en vigueur par rapport aux risques encourus;
- d'agir comme maîtres d'œuvre des analyses de risques et de s'assurer de la prise en charge des risques résiduels.

○ **La responsable ou le responsable de la vérification interne**

La personne responsable de la vérification interne joue un rôle dans la reddition de comptes en matière d'accès à l'information et de protection de renseignements personnels, plus particulièrement en regard de l'identification, de l'évaluation et de la gestion des risques d'atteinte à la

protection des renseignements personnels. À ce titre, elle évalue, examine ou vérifie, notamment :

- l'application, la validité et l'efficacité des règles, des mesures administratives et des moyens en matière de protection des renseignements personnels élaborés et mis en œuvre;
- la pertinence et l'efficacité des politiques, des pratiques et des mesures de contrôle du Ministère qui appuient la conformité du Ministère à la Loi sur l'accès, à ses politiques et directives connexes.

○ **La responsable ou le responsable de la gestion documentaire**

La personne responsable de la gestion documentaire a pour responsabilités, notamment, de :

- collaborer à la conception des systèmes informatiques, administratifs ou autres et de s'assurer qu'à toutes les étapes du cycle de vie de l'information, ces systèmes ont les qualités nécessaires à une saine gestion des connaissances et du patrimoine informationnel, à la préservation des preuves et au respect des lois;
- collaborer étroitement avec les détenteurs de l'information, la ou le ROSI ou la conseillère organisationnelle ou le conseiller organisationnel en sécurité de l'information (COSI) en vue de déterminer, de gérer, de coordonner et de mettre en œuvre des mesures de sécurité de l'information, indépendamment de son support.

○ **La responsable ou le responsable de la sécurité physique**

La personne responsable de la sécurité physique met en place les mesures de protection physique des locaux et de sécurisation de leurs accès, notamment lorsqu'ils abritent des systèmes et des installations technologiques stratégiques ou essentielles ou des supports de l'information confidentielle. Elle s'assure également de la mise au rebut sécuritaire des supports de l'information.

○ **La coordonnatrice ministérielle ou le coordonnateur ministériel en éthique**

La personne assumant la coordination ministérielle en éthique est chargée de promouvoir les valeurs éthiques adoptées par le Ministère, dont l'une est la confidentialité. En outre, cette personne :

- participe au comité ministériel sur la protection des renseignements personnels et sur l'accès et la sécurité de l'information;

- évalue l'aspect éthique des sondages utilisant des renseignements sensibles;
- planifie la tenue d'activités régulières de sensibilisation et de formation en matière éthique.

○ **La Direction des communications**

La Direction des communications a pour responsabilité notamment de :

- collaborer à la planification d'activités régulières de sensibilisation;
- jouer un rôle-conseil en matière de communication dans l'ensemble du processus de résolution de bris de confidentialité;
- assurer la coordination des communications auprès de la population et des médias ainsi qu'à l'interne auprès des gestionnaires et du personnel du Ministère.

○ **La Direction générale adjointe des ressources humaines**

La Direction générale adjointe des ressources humaines a pour responsabilité notamment de :

- collaborer, au besoin, à l'élaboration d'activités régulières de formation;
- mettre à la disposition de tous les nouveaux employés du Ministère l'information leur permettant d'assumer leur responsabilité en matière d'accès à l'information et de protection des renseignements personnels;
- veiller à la mise en place de mesures, mécanismes, normes et procédures assurant la sécurité des renseignements personnels et de l'information confidentielle concernant les employés du Ministère.

○ **Les gestionnaires**

Les gestionnaires assument les responsabilités en matière d'accès aux documents et de protection des renseignements personnels au sein de leur unité administrative. Ces personnes doivent notamment :

- s'assurer du respect de la Loi sur l'accès, de la présente politique, des orientations, des normes et des directives en ces matières par leur unité administrative;
- s'assurer que les droits des citoyennes et des citoyens sont respectés;
- s'assurer que le personnel sous leur responsabilité, dont les nouveaux employés, bénéficie d'une formation adéquate en ces domaines;
- s'assurer que le personnel n'ait accès qu'aux renseignements nécessaires à l'exercice de leurs fonctions;

- déclarer tout bris de confidentialité susceptible de compromettre la protection de renseignements personnels à la personne responsable de l'accès et de la protection des renseignements personnels;
 - désigner, lorsque requis, une répondante ou un répondant de l'accès et de la protection des renseignements personnels et s'assurer que cette information est connue de leur personnel;
 - transmettre tous les documents relatifs à une demande d'accès, dans les délais requis, à la personne responsable de l'accès et de la protection des renseignements personnels;
 - collaborer à tout bilan, évaluation, vérification ou reddition de compte à cet égard.
- **La répondante ou le répondant de l'accès et de la protection des renseignements personnels**

La répondante ou le répondant exerce un rôle-conseil en matière de respect de la Loi sur l'accès au sein de son unité administrative. De plus, cette personne assure la liaison avec l'équipe ministérielle coordonnée par la ou le responsable de l'accès et de la protection des renseignements personnels. En outre, la répondante ou le répondant doit :

- assurer la formation et la sensibilisation du personnel de son unité administrative;
- assurer le soutien-conseil auprès de son gestionnaire et du personnel de son unité administrative et, au besoin, consulter la personne responsable de l'accès et de la protection des renseignements personnels;
- coordonner le repérage des documents nécessaires au traitement des demandes d'accès formulées à la personne responsable de l'accès et de la protection des renseignements personnels et lui transmettre tous les documents dans les délais;
- s'assurer que les suites appropriées sont données aux demandes de documents reçues par l'unité administrative;
- informer les demandeurs de leur droit de déposer une demande d'accès auprès de la personne responsable de l'accès et de la protection des renseignements personnels;
- inscrire dans les registres appropriés les communications de renseignements personnels effectuées sans le consentement des personnes concernées ou les transmettre à la personne responsable de l'accès et de la protection des renseignements personnels lorsque ces communications relèvent de son ressort;
- s'assurer que les bris de confidentialité soient déclarés;
- procéder au sein de son unité, avec l'accord du gestionnaire, à l'exercice périodique d'autoévaluation des pratiques en matière d'accès et de protection des renseignements personnels.

○ **Les membres du personnel du Ministère**

Tous les membres du personnel sont concernés par l'application de la Loi sur l'accès. Ainsi, dans le cadre de leurs fonctions, chacune et chacun doit notamment :

- respecter les exigences légales et réglementaires portant sur l'accès et sur la protection des renseignements personnels;
- respecter la présente politique, les normes et les directives en ces matières;
- participer aux activités de sensibilisation et de formation portant sur ces sujets;
- consulter et n'utiliser que les renseignements nécessaires à leurs fonctions;
- prendre tous les moyens à leur disposition pour assurer la confidentialité des renseignements dont ils disposent pour exercer leur fonction;
- inscrire dans le registre approprié, lorsque requis, les communications de renseignements personnels faites à des tiers sans le consentement de la personne concernée;
- aviser, avec diligence, leur gestionnaire de bris de confidentialité susceptible de compromettre la protection de renseignements personnels;
- informer la clientèle de son droit d'accès aux documents et aux renseignements personnels ainsi que de son droit de rectification des renseignements personnels.

○ **Les contractants**

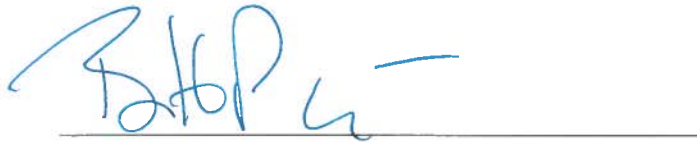
Tous les contractants du Ministère sont concernés par l'application de la Loi sur l'accès. Ainsi, dans le cadre de leurs contrats ceux-ci doivent :

- respecter les exigences légales et réglementaires portant sur l'accès et sur la protection des renseignements personnels;
- respecter la présente politique, les normes et les directives en ces matières;
- prendre tous les moyens à leur disposition pour assurer la confidentialité des renseignements dont ils disposent pour exercer leur fonction;
- ne recueillir, pour le compte du Ministère, que les renseignements nécessaires à l'exécution du contrat;
- accéder uniquement aux renseignements nécessaires à l'exercice de leurs fonctions, selon les accès qui leur sont attribués par le Ministère, et n'utiliser ces renseignements que pour la réalisation de leurs contrats.

9. Personne-ressource au Ministère

Pierrette Brie
Responsable ministérielle de l'accès
et de la protection des renseignements personnels
Ministère de l'Emploi et de la Solidarité sociale
tél.: (418) 643-4820
télééc.: (418) 643-1226
pierrette.brie@mess.gouv.qc.ca

Approbation :



Brigitte Pelletier
Sous-ministre

31 MARS 2014

Date

Historique

Ministère de l'Emploi
et de la Solidarité
sociale

Québec 

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

Émise le

2014-03-31

Révisée le

Prochaine révision prévue le

2019-03-31

Codification

PR-01-00-00

Description du changement	Approbation	Date
Adoption de la politique ministérielle concernant l'accès à l'information et la protection des renseignements personnels	Sous-ministre	2014-03-31

ANNEXE I

CADRE NORMATIF GOUVERNEMENTAL

Loi concernant le cadre juridique des technologies de l'information (L. R.Q. c. C-1.1);

Directive sur la sécurité de l'information gouvernementale (Décret 7-2014, 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 (1er octobre 2002).

CADRE NORMATIF MINISTÉRIEL

Politique de gestion de la sécurité de l'information;

Directive administrative en matière de bris de confidentialité;

Cadre de gestion relatif à la conduite d'études ou de recherche nécessitant la collecte, l'utilisation, la communication et la conservation de renseignements personnels ou sensibles par sondage ou par le recours à des méthodes qualitatives.