Ministère du Travail, de l'Emploi et de la Solidarité sociale
Québec

Politique ministérielle sur la gestion de la sécurité de l'information	
Émise le **2015-09-28**	Révisée le
Prochaine révision prévue le 2020-09-30	Codification RI-04-00-00

Politique ministérielle sur la gestion de la sécurité de l'information

Contexte

Dans l'exercice de ses fonctions, le Ministère offre des services à des clientèles diversifiées, notamment à des chercheurs d'emploi, des personnes démunies financièrement, des parents d'un nouvel enfant, des entreprises, des utilisateurs de services d'état civil, des spécialistes du domaine du travail, des organismes communautaires ainsi qu'aux citoyens désirant un accès simplifié à des services publics. Pour être en mesure d'offrir des services, le Ministère recueille, conserve, traite, diffuse et archive de l'information en grande quantité, laquelle augmente continuellement. Cette information est nécessaire à la réalisation de la mission du Ministère et requiert une protection tout au long de son cycle de vie.

La sécurité de l'information revêt une importance capitale au Ministère et fait l'objet d'un ensemble intégré de mesures qui s'articulent à l'intérieur d'une structure de gouvernance bien définie. La présente politique constitue l'assise de ces mesures et traduit la vision du Ministère en matière de sécurité de l'information. Elle exprime clairement ses objectifs, ses orientations, ses principes directeurs ainsi que les rôles et responsabilités de tous les acteurs.

L'atteinte d'un niveau de sécurité adéquat s'appuie sur une vision et une compréhension communes de la sécurité qui exigent l'implication constante de tous : gestionnaires, autres membres du personnel et clientèles. La présente politique établit des principes directeurs et des orientations qui tracent la ligne de conduite qui doit être suivie pour protéger adéquatement l'information et permettre au Ministère de s'acquitter de ses obligations et de s'assurer que ses employés maintiennent la confiance de ses partenaires, des citoyens et des entreprises à son égard.

Cette politique remplace la Politique de gestion de la sécurité de l'information en vigueur le 5 mars 2009.

Références

Lois, politiques ou documents concernant la sécurité de l'information :

- Loi sur le ministère de l'Emploi et de la Solidarité sociale et sur la Commission des partenaires du marché du travail (RLRQ, chapitre M-15.001);
- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, chapitre G-1.03);
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1);
- Loi sur l'administration publique (RLRQ, chapitre A-6.01);
- Loi concernant le cadre juridique des technologies de l'information (RLRQ, chapitre C-1.1);

- Loi sur les archives (RLRQ, chapitre A-21.1);
- 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 (directive du Conseil du trésor 198872, 1er octobre 2002);
- Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;
- Politique de la sécurité de l'information du Secrétariat du Conseil du trésor;
- Politique ministérielle sur la gestion des ressources informationnelles;
- Politique sur l'accès à l'information et sur la protection des renseignements personnels;
- Politique ministérielle en matière de vérification interne;
- Politique relative à la gestion documentaire;
- Politique de gestion du développement en milieu utilisateur;
- Politique ministérielle sur la sécurité physique dans les édifices du ministère de l'Emploi et de la Solidarité sociale;
- Directive administrative en matière de bris de confidentialité;
- Lignes directrices sur l'utilisation et la gestion du réseau Internet et du courriel;
- Guides et bulletins d'information sur les bonnes pratiques en matière de protection des renseignements personnels;
- Guide ministériel sur l'éthique, Agir avec intégrité;
- Protocole d'identification à appliquer lors de communications avec les clientèles (DOCU-MANI, chapitre 21.6);
- Directive ministérielle sur la réclamation lors de pertes subies par le Ministère et le personnel dans le cadre de leurs fonctions;

Cadre de gestion en matière de communication dans les réseaux sociaux.

Définitions

Assistance à la gestion des incidents gouvernementaux (CERT/AQ)

Service dont la mission est d'assister les ministères et organismes gouvernementaux (MO) dans la gestion d'incidents. Il coordonne le réseau d'alerte gouvernemental visant à améliorer la capacité des MO de prévoir les incidents et de se prémunir contre les attaques informatiques. Ce réseau d'alerte regroupe l'ensemble des spécialistes des MO et leur fournit les moyens techniques nécessaires pour échanger efficacement de l'information en situation de crise.

Authenticité

Caractère d'une entité qui est ce qu'elle revendique être.

Banque d'information

Information relative à un domaine défini, regroupée et organisée de façon à en permettre l'accès.

Cadre de gestion de la sécurité de l'information

Document décrivant exhaustivement l'organisation fonctionnelle de la sécurité de l'information dans un ministère ou organisme gouvernemental ainsi que les rôles et les responsabilités des intervenants en cette matière.

Catégorisation

Processus d'assignation d'une valeur à certaines caractéristiques de l'information, lesquelles définissent son degré de sensibilité relativement aux aspects de la disponibilité, de l'intégrité et de la confidentialité et, conséquemment, la protection à lui accorder. La catégorisation s'inscrit dans un processus de gestion de risques, car elle permet de définir clairement l'information pour laquelle un niveau de protection particulier est requis.

Cycle de vie de l'information

Ensemble des étapes que franchit l'information et qui vont, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, de sa création jusqu'à sa conservation ou sa destruction en conformité avec le calendrier de conservation établi par la Politique relative à la gestion documentaire du Ministère.

Détenteur ou détentrice de l'information

Gestionnaire de l'unité administrative responsable de la sécurité d'une ressource informationnelle ainsi que de la sécurité de l'ensemble des moyens, des objets et des lieux s'y rapportant. Le détenteur ou la détentrice d'une ressource informationnelle est le gestionnaire qui agit à titre de responsable de la protection de cette ressource informationnelle dans son unité.

Document

Information contenue sur un support. L'information y est délimitée et structurée, de façon tangible ou logique selon son support, 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 un système de symboles transcriptibles sous l'une de ces formes ou un autre système de symboles. Toute banque d'information est assimilée à un document si ses éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite.

Droit d'accès

Privilège accordé à un utilisateur d'accéder, de façon tangible ou logique, à de l'information.

Fiabilité

Caractéristique relative à un comportement et à des résultats prévus et cohérents.

Gestion de la continuité des services

Activité qui vise à atténuer les conséquences d'un incident majeur compromettant la disponibilité d'une information et ainsi à permettre le rétablissement des services essentiels dans un délai acceptable. La gestion de la continuité des services repose sur un plan de continuité des services, qui permet à une organisation de parer à des incidents majeurs. Le plan de continuité est un outil organisationnel qui est composé de plusieurs plans, dont un plan de sauvegarde, un plan de reprise et un plan de rétablissement.

Gestion des accès

Ensemble des activités qui ont pour objectif de limiter l'accès à l'information détenue par le Ministère aux seuls utilisateurs autorisés, en respectant le principe du moindre privilège et du besoin de savoir, soit ce qui correspond aux besoins d'information pour l'exécution d'une tâche ou d'une activité.

Gestion des risques

Ensemble des activités qui consistent à recenser les risques auxquels une ressource informationnelle est exposée, à définir et à mettre en place les mesures préventives appropriées en vue de supprimer ces risques ou d'atténuer les conséquences d'un incident.

Irrévocabilité

Impossibilité, pour une personne ou pour une entité engagée dans une communication par un moyen quelconque, de nier avoir reçu ou produit un message.

Incident de sécurité de l'information

Tout événement ou série d'événements susceptible de toucher la confidentialité, l'intégrité ou la disponibilité de l'information, y compris ses composantes, ou un événement ou une série d'événements qui peut enfreindre la loi, les politiques ou les directives relatives à la sécurité de l'information. Les incidents de sécurité incluent les atteintes à la vie privée, délibérées ou fortuites, à savoir la collecte, l'utilisation, la communication, l'accès, la conservation et l'élimination de renseignements personnels, lorsque ces actions ne sont pas autorisées.

Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement

Loi qui établit un cadre de gouvernance et de gestion en matière de ressources informationnelles et qui s'applique aux ministères et à la plupart des organismes publics, y compris à ceux du réseau de l'éducation et du réseau de la santé et des services sociaux.

Menace

Cause potentielle d'un incident indésirable qui peut nuire à un système ou à une organisation et qui est susceptible de compromettre la sécurité des ressources informationnelles. Une menace peut être caractérisée selon son type (naturel, humain, matériel ou technologique), selon sa cause (accidentelle ou délibérée) et selon le degré de perturbation des activités de l'organisation (partiel ou total).

Mesure de sécurité

Moyen organisationnel, technologique, humain ou juridique permettant d'assurer la réalisation des objectifs de disponibilité, d'intégrité et de confidentialité de l'information ainsi que d'authentification des personnes et des dispositifs et de l'irrévocabilité des actions que les personnes posent.

Plan de continuité

Planification stratégique, tactique et opérationnelle comportant de l'information et des procédures devant assurer la continuité des services d'une organisation.

Prestataire de services

Personne physique ou morale qui fait affaire avec un ministère ou organisme gouvernemental en vue de lui fournir des services ou des biens.

Registre d'autorité

Recueil où sont notamment consignés les noms des détenteurs ou détentrices de l'information, les systèmes d'information qui leur sont assignés ainsi que les noms des principaux intervenants en matière de sécurité de l'information.

Registre de catégorisation

Recueil où sont inscrites les évaluations de la sensibilité des renseignements relativement aux aspects de la disponibilité, de l'intégrité et de la confidentialité. Les évaluations sont utilisées pour établir le niveau de sécurité requis pour protéger ces renseignements.

Renseignement confidentiel

Renseignement dont l'accès est assorti d'une ou plusieurs restrictions prévues par la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels. 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

Renseignements dans un document qui concernent une personne physique et qui permettent de la reconnaître.

Renseignement sensible

Tout renseignement considéré comme confidentiel, stratégique, essentiel, critique, indispensable ou vital pour les opérations et dont la divulgation, l'altération, la perte ou la destruction est susceptible de porter un préjudice à l'organisation détentrice ou à sa clientèle, à ses partenaires ou aux prestataires de services.

Ressource informationnelle

Ressource utilisée par une entreprise ou une organisation, dans le cadre de ses activités de traitement de l'information, pour mener à bien sa mission, pour faciliter la prise de décision ou encore la résolution de problèmes. Une ressource informationnelle peut être une ressource humaine, matérielle ou financière directement affectée à la gestion, à l'acquisition, au développement, à l'entretien, à l'exploitation, à l'accès, à l'utilisation, à la protection, à la conservation et à la destruction d'éléments d'information. Une ressource peut être une personne, un fichier ou un système informatique.

Risque de sécurité de l'information à portée gouvernementale

Risque d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information gouvernementale et qui peut avoir des conséquences sur la prestation de services à la population, sur la vie, la santé ou le bien-être des personnes, sur l'image du gouvernement ou sur la prestation de services fournie par d'autres organismes publics.

Risque résiduel

Risque qui subsiste après la réponse au risque ou après l'application de mesures d'atténuation du risque.

Sécurité de l'information

Ensemble de moyens technologiques, humains, organisationnels, juridiques et éthiques permettant d'assurer la réalisation des objectifs de disponibilité, d'intégrité et de confidentialité de l'information, tout en contrôlant les accès avec des principes d'authentification et d'irrévocabilité.

Services communs de sécurité de l'information

Services utilisés par plusieurs ministères et organismes gouvernementaux dont la gestion est centralisée.

Système

Ensemble d'éléments et de relations entre ces éléments considéré comme un tout.

Système d'information

Système constitué des ressources humaines, des ressources matérielles et des procédures permettant de collecter, de détenir, de traiter et de transmettre les éléments d'information pertinents pour l'organisation, sa clientèle et ses partenaires.

Utilisateur

Toute personne morale ou physique qui utilise une ressource informationnelle de l'organisation ou y a accès.

Portée

La présente politique s'applique à l'information détenue ou utilisée par le Ministère, peu importe sa nature, le support sur lequel elle se trouve ou sa localisation, qu'elle se trouve dans les locaux du Ministère ou dans les locaux d'un prestataire de services, et ce, durant tout son cycle de vie.

Cette politique doit être prise en considération lors de la conception ou de la mise en œuvre d'un processus lié à un système d'information ou d'un développement en milieu utilisateur de même que lors de l'élaboration d'ententes ou de l'acquisition d'une solution technologique.

Enfin, la présente politique s'applique à tout le personnel du Ministère, notamment les détenteurs et détentrices de ressources informationnelles, les fournisseurs ou les prestataires de services qui ont accès à une ressource informationnelle ou à un lieu dont la sécurité est sous la responsabilité du Ministère.

Un cadre de gestion complémente cette politique.

Orientations et principes directeurs

Dans le cadre de ses activités, la sécurité de l'information est une préoccupation constante du Ministère. En ce sens, il en reconnaît l'importance et vise à bien l'encadrer en se donnant les **orientations** suivantes :

Maintenir une relation basée sur le respect et la confiance avec les clientèles et le personnel

La sécurité de l'information, notamment la protection des renseignements détenus sur les citoyens, les entreprises et le personnel, est indissociable de la prestation de services du Ministère. Elle contribue à maintenir une relation basée sur le respect et la confiance avec ses clientèles et son personnel. La sécurité de l'information vise également à assurer la pérennité de la fiabilité de l'information.

Renforcer l'encadrement relatif à la sécurité de l'information

Un encadrement adéquat relatif à la sécurité de l'information du Ministère et les orientations internes en cette matière appuient les valeurs organisationnelles. Le renforcement de l'encadrement doit passer par la définition d'une structure organisationnelle où les rôles et les responsabilités des intervenants de tous les niveaux sont précisés et par une saine gestion des risques.

Agir de manière concertée et valoriser la collaboration

Il est nécessaire que les membres du personnel de tous les niveaux collaborent à la sécurité de l'information du Ministère. L'efficacité de cette collaboration passe par une communication adéquate avec les partenaires, les citoyens et les utilisateurs de l'information et par la mise en place de processus de gestion de la sécurité de l'information assurant la saine gestion de celle-ci et permettant une reddition de comptes conforme au cadre légal et gouvernemental.

Responsabiliser les utilisateurs de l'information

La sécurité de l'information doit être une préoccupation constante de l'ensemble des membres du personnel ainsi que des utilisateurs des actifs informationnels du Ministère, notamment les citoyens, les entreprises et les fournisseurs de services. Chaque utilisateur doit assumer ses actions par rapport à l'information obtenue.

Atteindre et maintenir un niveau de maturité adéquat en matière de sécurité de l'information

Un niveau de maturité convenable en matière de sécurité de l'information est atteint, notamment, lorsque les processus de sécurité de l'information sont normalisés, intégrés, répertoriés, mis en œuvre et ajustés périodiquement. La sécurisation de l'information détenue par le Ministère conformément aux meilleures pratiques[1] influence également le niveau de maturité du Ministère relativement à la sécurité de l'information.

1. En ce qui concerne les meilleures pratiques en matière de sécurité de l'information, le Ministère se base sur la famille des normes ISO27XXX concernant la sécurité de l'information et les documents publiés par le Secrétariat du Conseil du trésor sur le sujet.

Connaître les risques et les menaces et s'y adapter

Les mesures de sécurité sont établies en fonction des risques existants, de leur probabilité d'occurrence, du degré d'exposition à ces risques et des conséquences d'un incident. Elles doivent être proportionnelles à la valeur de l'information à protéger.

S'adapter pour mieux répondre aux besoins des clientèles et aux exigences des partenaires gouvernementaux et des partenaires d'affaires

Les mesures de sécurité de l'information adoptées par le Ministère sont réévaluées continuellement afin qu'elles tiennent compte des changements législatifs, organisationnels et technologiques ainsi que de l'évolution des menaces et des risques de sécurité. De plus, la gestion de la sécurité de l'information s'appuie sur le respect des exigences et des obligations des partenaires gouvernementaux et des partenaires d'affaires.

Ces orientations se traduisent dans les **principes directeurs** qui suivent :

Assurer la disponibilité de l'information

- Toute information nécessaire aux activités courantes du Ministère doit être accessible et utilisable en temps voulu par une personne autorisée;
- En cas de sinistre ou d'incident majeur compromettant la disponibilité de l'information, le Ministère doit disposer d'un plan de continuité des services, qui permet le rétablissement des processus jugés essentiels dans un délai acceptable. Ce plan doit être testé et mis à jour régulièrement.

Assurer l'intégrité de l'information

- Des mesures de sécurité doivent permettre de maintenir l'intégrité de l'information de manière à ce qu'elle ne soit pas détruite ni altérée de quelque façon que ce soit sans autorisation et que son support lui procure la stabilité et la pérennité voulues;
- L'intégrité de tout document servant à l'établissement de la preuve d'un acte ou d'un fait doit être assurée tout au long de sa vie afin de préserver sa valeur juridique.

Assurer la confidentialité de l'information

- Des mesures de sécurité doivent permettre de protéger la confidentialité de l'information, notamment les renseignements personnels, en limitant aux personnes autorisées son accessibilité et sa divulgation. Elles garantissent ainsi une utilisation stricte et contrôlée de l'information;
- Des mesures de sécurité doivent assurer la traçabilité des actions accomplies relativement à l'information détenue par le Ministère, notamment sa destruction.

Gérer les accès physiques et logiques des utilisateurs

- La gestion des accès doit limiter l'accès à l'information détenue par le Ministère aux seules personnes autorisées, en respectant le principe du moindre privilège et du besoin de savoir;

- Les règles concernant la gestion des accès physiques et logiques ainsi que les rôles et responsabilités des personnes autorisées doivent être bien définis;
- L'accès aux locaux doit être contrôlé;
- L'infrastructure technologique et le milieu dans lequel se trouve l'information doivent être sécurisés adéquatement;
- Une journalisation des accès aux renseignements confidentiels et personnels détenus par le Ministère doit être conservée de manière à ce qu'une vérification des accès puisse être faite**.**

Catégoriser l'information et gérer les risques

- Les systèmes d'information, les développements en milieu utilisateur et la grande collection documentaire sont catégorisés par leur détenteur ou détentrice et répertoriés dans le registre de catégorisation;
- L'information que détient et traite le Ministère doit être soumise à une analyse de risques basée sur sa catégorisation et des mécanismes de repérage et d'évaluation continue des risques en matière de sécurité de l'information;
- Une analyse des risques doit être réalisée dès le début des études menant à tout changement pouvant compromettre la sécurité de l'information. Les résultats de cette analyse sont utilisés pour définir les mesures de protection adéquates durant tout le cycle de vie de l'information.

Gérer la sécurité lors d'un développement informatique

- Les exigences découlant d'une analyse de risques en matière de sécurité de l'information doivent être prises en considération dès le début des études menant à l'acquisition ou au développement d'un système d'information;
- Les mesures de protection des renseignements personnels doivent être appliquées tout au long du processus de conception et de développement du système;
- Tout nouveau système d'information ou tout développement en milieu utilisateur doit se voir assigner un détenteur ou une détentrice et être catégorisé. Un exercice d'analyse de risques en matière de sécurité de l'information doit être réalisé relativement au DMU.

Gérer les contrats, les ententes et les échanges

- Des clauses garantissant le respect des exigences du Ministère en matière de sécurité de l'information doivent figurer dans les contrats et les ententes;
- Au besoin, des mécanismes de validation seront mis en place par le Ministère pour veiller au respect de cette politique;
- Les fournisseurs et les partenaires ayant accès aux ressources informationnelles du Ministère doivent offrir une protection semblable à celle du Ministère. La responsabilité de chacun et de chacune doit être clairement établie.

Sensibiliser et former

- Le Ministère doit communiquer les principes directeurs et les orientations internes concernant la sécurité de l'information à l'ensemble des utilisateurs afin d'assurer leur application et sensibiliser les utilisateurs à l'importance du sujet;
- Le Ministère doit communiquer à toutes et à tous leurs rôles et responsabilités;

- Chaque gestionnaire doit sensibiliser le personnel sous sa responsabilité à la sécurité de l'information et s'assurer qu'il suive et comprenne bien la formation préparée par le Ministère sur le sujet.

Gérer les incidents de sécurité de l'information

- Un processus de gestion des incidents touchant l'information détenue par le Ministère doit être en place afin que les intervenants désignés puissent réagir adéquatement et limiter les conséquences que ces incidents pourraient avoir sur les personnes et les services.
- Les incidents doivent être répertoriés, analysés et classifiés selon leur gravité. Ils peuvent donner lieu à l'adoption et la mise en place de mesures correctives.

Assurer la gestion des documents et leur disposition

- Conformément à la Politique relative à la gestion documentaire, les documents sont inventoriés et classés de manière à en permettre le repérage et l'accessibilité;
- Le Ministère doit planifier et encadrer la création, l'utilisation, la conservation et la destruction des documents, et ce, peu importe leur support, notamment des documents comportant des renseignements confidentiels et personnels;
- L'archivage ou la destruction des documents qui ne sont plus nécessaires doit être fait selon le calendrier de conservation des documents du Ministère.

Gérer la conformité aux normes et aux standards

- Le Ministère a l'obligation de se conformer aux normes et aux standards qu'il a acceptés dans le cadre d'une entente ou d'un contrat;
- Le Ministère effectue des transactions requérant l'utilisation de cartes de paiement (cartes de crédit ou cartes de débit) dans le cadre de sa prestation de services. Il doit donc se conformer aux normes de sécurité des données de cartes de paiement en vigueur afin d'assurer la sécurité de l'information associée aux titulaires de carte.

Droit de regard et sanctions

- Le Ministère a un droit de regard sur l'utilisation de l'information qu'il détient et des moyens, objets et lieux qui permettent d'avoir accès à cette information ou d'en assurer la sécurité;

Ce droit de regard doit être exercé conformément au cadre légal et gouvernemental applicable au Ministère, et ce, dans le respect de la protection des renseignements personnels.

Objectifs

La présente politique a pour objectifs

- d'affirmer l'engagement du Ministère à s'acquitter pleinement de ses responsabilités à l'égard de la sécurité de l'information;
- d'établir les grands principes et les orientations qui doivent guider son action en cette matière;
- de diffuser les orientations et les principes directeurs qu'il a adoptés en matière de sécurité de l'information pour en permettre l'intégration dans son cadre de gestion, ses règles de gestion, ses pratiques, ses guides et ses procédures;
- de faire appliquer par le personnel, dans la mesure du possible, les normes et les standards internationaux en matière de sécurité de l'information et de le faire

	adhérer aux bonnes pratiques qui ont cours dans ce domaine dans les secteurs public et privé, lorsqu'elles s'appliquent; - d'intégrer la sécurité de l'information dans la culture organisationnelle en renforçant la responsabilisation individuelle et en soutenant une démarche globale de gestion des risques.
Rôles et responsabilités	**Dirigeante principale ou dirigeant principal de l'information** La dirigeante principale ou le dirigeant principal de l'information (DPI) fournit aux organismes publics les outils et l'assistance leur permettant de prendre en charge les exigences en matière de sécurité de l'information et conseille le Secrétariat du Conseil du trésor dans sa fonction de gouverne de la sécurité de l'information gouvernementale. À cette fin et selon une périodicité bisannuelle, elle ou il est informé de la planification des actions et du bilan de sécurité de l'information du Ministère. **Sous-ministre** La ou le sous-ministre est la ou le premier responsable de la sécurité de l'information du Ministère. Elle ou il doit s'assurer du respect des lois et des règles applicables en matière de sécurité de l'information. Il ou elle veille à ce que la sécurité de l'information au Ministère soit gérée conformément à la Directive sur la sécurité de l'information gouvernementale. Plus précisément, elle ou il - adopte une politique et un cadre de gestion de la sécurité de l'information, voit à leur mise en œuvre, les maintient à jour et assure leur application; - remet à la ou au DPI, selon les modalités et le format fixés par ce dernier, i. une planification des actions de sécurité de l'information bisannuelle, qui inclut les priorités d'action et les échéanciers découlant des exercices d'audits et de tests d'intrusion, ii. un bilan de sécurité de l'information bisannuel; - s'assure de la mise en œuvre des processus formels de sécurité de l'information permettant, notamment, d'assurer la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents; - déclare à la ou au DPI, selon les modalités fixées par cette dernière ou ce dernier, les risques de sécurité de l'information à portée gouvernementale; - déclare au CERT/AQ, selon les modalités fixées par ce dernier, les incidents de sécurité de l'information à portée gouvernementale; - s'assure de la réalisation d'un audit de sécurité de l'information, selon une périodicité bisannuelle ou à la suite d'un changement majeur susceptible d'avoir des conséquences sur la sécurité de l'information gouvernementale, et en dégage les priorités d'action ainsi que les échéanciers s'y rapportant; - s'assure de la réalisation de tests d'intrusion et de vulnérabilité, annuellement ou à la suite d'un changement majeur susceptible d'avoir des conséquences sur la sécurité de l'information gouvernementale, et en dégage les priorités d'action et les échéanciers s'y rapportant; - s'assure de la mise en place d'un registre d'autorité de la sécurité de l'information. Sont notamment consignés dans ce registre les noms des détenteurs ou détentrices de l'information, les systèmes d'information qui leur sont assignés ainsi que les rôles et les responsabilités des principaux intervenants en matière de sécurité de l'information;

- s’assure que les ententes de services et les contrats, conclus avec les prestataires de services, les partenaires et les mandataires, comprennent des clauses garantissant le respect des exigences en matière de sécurité de l’information;
- favorise l’utilisation des services communs de sécurité de l’information déterminés par le Secrétariat du Conseil du trésor;
- définit et met en place un programme formel et continu de formation et de sensibilisation du personnel en matière de sécurité de l’information;
- désigne une ou un responsable organisationnel de la sécurité de l’information (ROSI) pour le représenter en matière de sécurité de l’information auprès de son organisation et auprès du ou de la DPI. Ce responsable doit être une employée permanente ou un employé permanent du Ministère et appartenir à la classe d’emploi de niveau cadre ou à une classe d’emploi de niveau supérieur;
- désigne une coordonnatrice organisationnelle ou un coordonnateur organisationnel de gestion des incidents (COGI) pour le représenter auprès du réseau d’alerte gouvernemental et y participer activement. Cette coordonnatrice ou ce coordonnateur doit être une employée permanente ou un employé permanent du Ministère et appartenir à la classe d’emploi de niveau professionnel ou à une classe d’emploi de niveau supérieur.

Comité ministériel sur la protection des renseignements personnels et sur l’accès et la sécurité de l’information

Le comité ministériel sur la protection des renseignements personnels et sur l’accès et la sécurité de l’information (CMPRPASI) est chargé de soutenir la ou le sous-ministre dans l’exercice de ses responsabilités et obligations. Il est par ailleurs présidé par la ou le sous-ministre. En vertu de la directive et du cadre de gestion sur la sécurité de l’information gouvernementale, le comité est la principale instance de concertation en matière de sécurité de l’information. En ce sens, il

- examine et formule des recommandations concernant les orientations, les politiques, les directives, les cadres de gestion, les plans d’action et les bilans de l’organisation ainsi que les propositions d’action ou les états d’avancement de projets en matière de sécurité de l’information;
- analyse et formule des recommandations concernant les événements qui ont mis ou auraient pu mettre en péril la sécurité de l’information de l’organisation.

La composition du comité est précisée dans la Politique sur l’accès à l’information et sur la protection des renseignements personnels.

Dirigeante sectorielle ou dirigeant sectoriel de l’information

La dirigeante sectorielle ou le dirigeant sectoriel de l’information (DSI) est désigné par la ou le sous-ministre 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, elle ou il

- veille à l'application par le Ministère des règles de gouvernance et de gestion établies en matière de sécurité de l’information;
- examine les plans d’action et conseille le Ministère sur les modifications à y apporter;

- contribue, conjointement avec la ou le DPI et le CERT/AQ, à la définition et à la mise en œuvre du processus de gestion des incidents à portée gouvernementale;

- définit, si nécessaire, dans le respect des règles établies conformément à la loi, des règles particulières en matière de gestion de l'information, incluant celles inhérentes à la sécurité de l'information, qui, après approbation du Secrétariat du Conseil du trésor, seront applicables au Ministère.

Responsable organisationnel de la sécurité de l'information

Désigné par la ou le sous-ministre, le responsable organisationnel ou la responsable organisationnelle de la sécurité de l'information (ROSI) joue le rôle de porte-parole de la ou du DPI auprès du Ministère et l'informe des orientations et des priorités d'intervention gouvernementales en matière de sécurité de l'information. Il ou elle assiste la ou le sous-ministre dans la détermination des orientations stratégiques et des priorités d'intervention et le ou la représente en matière de déclaration des incidents de sécurité de l'information à portée gouvernementale. En ce sens, il ou elle

- soumet à la consultation du Comité ministériel sur la protection des renseignements personnels et sur l'accès et la sécurité de l'information les orientations, les politiques, les directives, les cadres de gestion, les priorités d'action, les éléments de reddition de comptes ainsi que tout événement qui a mis ou aurait pu mettre en péril la sécurité de l'information;
- assure la coordination et la cohérence des actions de sécurité de l'information menées au sein du Ministère par d'autres intervenants, notamment par les détenteurs ou détentrices de l'information, les unités responsables des ressources informationnelles, de l'accès à l'information, de la protection des renseignements personnels, de la gestion documentaire, de la sécurité physique, de la continuité des services et de l'éthique;
- s'assure de la contribution du Ministère au processus de gestion des risques et des incidents de sécurité de l'information à portée gouvernementale;
- définit et met 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 qui ont mis ou auraient pu mettre en péril la sécurité de l'information gouvernementale;
- s'assure de la prise en charge des exigences de sécurité de l'information lors de la réalisation de projets de développement de systèmes d'information ou de l'acquisition de systèmes d'information;
- coordonne 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.

Responsable de l'accès à l'information et de la protection des renseignements personnels

Le ou la responsable de l'accès à l'information et de la protection des renseignements personnels (RAIPRP) joue un rôle d'expert-conseil et assiste la ou le sous-ministre dans l'application de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels. À ce titre, il ou elle

- communique au ou à la ROSI les problématiques et les préoccupations de sécurité en rapport avec la protection des renseignements personnels ou sensibles;

- contribue à assurer la cohérence et l'harmonisation des interventions liées à la sécurité de l'information, l'accès aux documents et la protection des renseignements personnels en tout temps, y compris lors de la mise en œuvre du processus de gestion des risques;
- détermine les risques qui peuvent menacer la protection des renseignements personnels;
- produit des avis relatifs à la protection des renseignements personnels et transmet une copie de ces avis à la ou au ROSI lorsque les avis comportent des aspects liés à la sécurité de l'information.

Conseillère organisationnelle ou conseiller organisationnel de la sécurité de l'information

La conseillère organisationnelle ou le conseiller organisationnel de la sécurité de l'information (COSI) apporte son soutien au ou à la ROSI sur le plan tactique, notamment en ce qui a trait à la mise en œuvre des mesures d'atténuation des risques et à la mise en place des processus officiels de sécurité de l'information. Au-delà de son rôle de soutien auprès du ou de la ROSI, la ou le COSI

- met en œuvre les orientations internes découlant des directives gouvernementales, des politiques internes et des pratiques généralement admises en matière de sécurité de l'information;
- produit les bilans et les plans d'action de sécurité de l'information;
- participe aux négociations des ententes de services et des contrats et formule des recommandations quant à l'intégration de dispositions garantissant le respect des exigences de sécurité de l'information;
- tient à jour le registre d'autorité de la sécurité de l'information;
- assiste les détenteurs ou détentrices de l'information pour ce qui est de la catégorisation de l'information relevant de leur responsabilité et de la réalisation des analyses de risques de sécurité de l'information;
- contribue à la mise en œuvre des processus officiels de sécurité de l'information du Ministère.

Conseillère organisationnelle ou conseiller organisationnel en sécurité de l'information des projets

La conseillère organisationnelle ou le conseiller organisationnel en sécurité de l'information des projets (COSIP) apporte son soutien au ou à la ROSI sur le plan de la prise en charge des exigences de sécurité de l'information lors de la réalisation de projets de développement ou d'acquisition de systèmes d'information. À ce titre et dans ces contextes précis, elle ou il

- contribue à la mise en place du cadre normatif de développement assurant la prise en charge des exigences de sécurité de l'information lors de la réalisation d'un projet de développement;

- produit des avis relatifs à la sécurité de l'information et transmet une copie de ces avis au ou à la responsable de l'accès à l'information et de la protection des renseignements personnels lorsque les avis comportent des aspects liés à la protection des renseignements personnels;
- contribue à la mise en œuvre du processus de catégorisation des ressources informationnelles du Ministère;
- met à jour le registre de catégorisation;
- assiste les détenteurs ou détentrices de l'information pour ce qui est de la catégorisation de l'information relevant de leur responsabilité et de la réalisation des analyses de risques de sécurité de l'information.

Coordonnatrice organisationnelle ou coordonnateur organisationnel de gestion des incidents

La coordonnatrice ou le coordonnateur organisationnel de gestion des incidents (COGI) est désigné par la ou le sous-ministre en vertu de la Directive sur la sécurité de l'information gouvernementale. Ses tâches concernent la prévention des incidents, la réaction aux incidents et l'amélioration de la sécurité informatique. Elle ou il est appelé à travailler en étroite collaboration avec le ou la ROSI et le ou la COSI dans l'exécution de ses tâches. Outre sa participation active au réseau d'alerte gouvernementale, la ou le COGI

- contribue à la mise en place du processus de gestion des incidents de sécurité de l'information de son organisation;
- assure la coordination des membres du CERT/AQ qui sont assignés à son organisation et met en œuvre les stratégies de réaction appropriées;
- contribue aux analyses de risques de sécurité de l'information, au repérage des menaces et des situations de vulnérabilité et à la mise en œuvre des solutions appropriées;
- contribue à la mise en œuvre du processus gouvernemental de gestion des incidents de sécurité de l'information;
- élabore et tient à jour les guides portant sur la sécurité opérationnelle des systèmes et des réseaux de télécommunications;
- collabore étroitement avec le ou la ROSI et lui fournit le soutien technique nécessaire à l'exercice de ses responsabilités.

Comité de crise

Le comité de crise est un groupe décisionnel appelé à intervenir lorsqu'un événement paralyse totalement ou partiellement les activités du Ministère et qu'aucune mesure prévue n'a pu assurer la continuité des services ou la reprise rapide des activités. Ce comité est présidé par la ou le sous-ministre ou son représentant. À ce titre, il

- autorise la mise en œuvre de stratégies permettant d'assurer la prise en charge des incidents majeurs de sécurité de l'information;
- adopte la déclaration de sinistre proposée par la ou le responsable de la continuité des services et approuve les budgets spéciaux correspondants;
- décide du déploiement ou non du plan de continuité des services;
- propose des orientations à suivre ou des actions à poser en cas de sinistre;
- formule des recommandations concernant le délestage, en totalité ou en partie, des activités de l'organisation;

- communique avec les médias par le représentant des communications siégeant au comité.

Le noyau permanent de ce comité est composé de représentants de la haute direction, notamment du ou de la DSI, du ou de la ROSI, du responsable de la protection des renseignements personnels, du responsable de la sécurité physique et du responsable de la continuité des services.

Ce comité peut s'adjoindre toute autre personne en mesure de lui assurer le soutien adéquat dans le cadre de ses prises de décision. Citons, à titre d'exemple, les détenteurs ou détentrices de l'information, des conseillers pour les volets juridiques, technologiques et de communication avec les médias et les ressources humaines.

Détenteurs ou détentrices de ressources informationnelles

Les détenteurs ou détentrices de ressources informationnelles sont des gestionnaires nommément désignés par la ou le sous-ministre. Ils sont responsables de la gestion et de la protection des ressources informationnelles qui ont été confiées à leur unité administrative. En ce sens, ils sont habilités à prendre toute décision concernant ces ressources et les risques auxquels celles-ci sont exposées en vue d'assurer leur sécurité pendant tout le cycle de vie. Ils

- participent aux mécanismes de coordination et de concertation en matière de sécurité de l'information. Au besoin, ils assistent le ou la ROSI dans l'exercice de ses fonctions en participant à l'élaboration des orientations stratégiques, des politiques, des directives, des bilans, des plans d'action et des cadres de gestion concernant la sécurité de l'information;
- catégorisent l'information relevant de leur responsabilité selon sa valeur en ce qui a trait à la disponibilité, l'intégrité et la confidentialité;
- veillent à ce que les mesures de sécurité de l'information, y compris celles liées à la continuité des services et celles liées au respect des exigences légales de protection des renseignements personnels, soient adoptées et appliquées;
- s'assurent de l'adéquation des mesures de sécurité de l'information en vigueur par rapport aux risques encourus;
- agissent comme maîtres d'œuvre des analyses de risques et s'assurent de la prise en charge des risques résiduels;
- gèrent les droits d'accès relatifs aux ressources informationnelles qu'ils détiennent;
- prennent les actions nécessaires à la résolution de tout incident touchant la sécurité de l'information qu'ils détiennent.

Responsable de la vérification interne et des enquêtes administratives

Le ou la responsable de la vérification interne et des enquêtes administratives soutient la haute direction quant aux contrôles sur les systèmes, processus et activités. Il ou elle peut notamment

- vérifier l'efficacité des contrôles de la sécurité de l'information au Ministère;
- exercer un rôle-conseil à l'égard de la sécurité de l'information auprès du Ministère et des détenteurs ou détentrices de ressources informationnelles;
- effectuer des enquêtes à la demande des gestionnaires ou à la suite de la détection d'un usage illicite ou abusif de données informationnelles ou des outils informatiques mis à la disposition du personnel;

- répondre aux demandes de vérification de sécurité avant la nomination d'un nouvel employé dont le poste est considéré à risque relativement à la sécurité de l'information du Ministère.

Responsable de l'architecture de sécurité de l'information

En collaborant étroitement avec le conseiller en architecture d'entreprise du Ministère, le ou la responsable de l'architecture de sécurité de l'information (RASI)

- conçoit et met en œuvre l'architecture décrivant la fonction, la structure et les interrelations des composantes de sécurité de l'information;
- arrime les solutions retenues aux processus organisationnels de sécurité de l'information;
- participe à la conception et à l'évaluation des composantes de sécurité de l'information des programmes, logiciels ou applications développés ou acquis par son organisation.

Responsable de la sécurité physique

Le ou la responsable de la sécurité physique (RSP) 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. Plus particulièrement, la ou le RSP

- gère le volet de la sécurité physique du cadre normatif ministériel relatif à la sécurité de l'information, incluant la Politique ministérielle sur la sécurité physique dans les édifices du Ministère;
- conçoit et met en œuvre les mesures de protection physique des biens et des personnes;
- s'assure de la mise au rebut sécuritaire des documents sur support physique;
- élabore et met en œuvre des directives, des guides et des procédures propres à son domaine d'intervention;
- traite les incidents relatifs à la sécurité physique et participe à l'élaboration et au suivi de l'application de la procédure de déclaration systématique des incidents touchant la protection des renseignements personnels et la sécurité de l'information.

Coordonnatrice ministérielle ou coordonnateur ministériel en éthique

La coordonnatrice ou le coordonnateur ministériel en éthique a pour mandat de contribuer à l'implantation et au développement de la culture éthique organisationnelle. En ce sens, il ou elle

- veille à l'intégration de l'éthique aux processus de gestion de la sécurité de l'information, afin d'assurer la régularisation des conduites et la responsabilisation individuelle;
- participe aux mécanismes de coordination et de concertation en matière de sécurité et assiste le ou la ROSI dans l'exercice de ses fonctions, au besoin.

Responsable de la gestion documentaire

Le ou la responsable de la gestion documentaire assiste, en matière de sécurité de la gestion documentaire, le ou la ROSI. À cette fin, il ou elle

- collabore à la conception d'outils de gestion documentaire et s'assure qu'à toutes les étapes du cycle de vie de l'information, ces outils ont les qualités nécessaires pour permettre une saine gestion des connaissances et du patrimoine informationnel, la préservation des preuves et le respect des lois;
- collabore étroitement avec les détenteurs ou les détentrices de l'information ainsi qu'avec le ou la ROSI ou le ou la 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.

Gestionnaires

En collaboration avec le ou la ROSI, les gestionnaires assument des responsabilités en matière de sécurité au sein de leur unité administrative. À cette fin, les gestionnaires

- respectent les processus de sécurité de l'information du Ministère, notamment ceux portant sur la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents;
- agissent comme détenteurs ou détentrices de l'information propre à leur unité administrative et informent le ou la RAIPRP de l'existence de cette information lorsqu'elle contient des renseignements personnels;
- s'assurent d'intégrer dans les ententes avec les partenaires et les fournisseurs les clauses garantissant le respect des exigences de sécurité du Ministère.

Utilisateurs

Les utilisateurs doivent prendre connaissance de la présente politique, la respecter et protéger convenablement l'information mise à leur disposition en évitant notamment de l'exposer à des risques indus. De plus, ils doivent

- prendre connaissance des directives, normes et règles qui découlent de cette politique et les respecter;
- protéger l'information mise à leur disposition en l'utilisant avec discernement, aux seules fins autorisées et conformément aux privilèges d'accès qui leur ont été accordés dans l'exercice de leurs fonctions;
- utiliser le matériel mis à leur disposition de manière à protéger l'accès à l'information et l'accès aux locaux du Ministère;
- aviser sans tarder leur gestionnaire de tout acte susceptible de représenter une violation des règles de sécurité.

CERT/AQ

Le CERT/AQ assure, conjointement avec la ou le DPI, la coordination de la gestion des incidents de sécurité de l'information à portée gouvernementale.

Personne-ressource	La gestion de la présente politique et le soutien nécessaire à son application sont assurés par le Secteur des services à la gestion et ressources informationnelles. Pour toutes questions relatives à l'application ou à l'interprétation des dispositions de la politique, veuillez-vous référer au responsable organisationnel de la sécurité de l'information, M. Louis-Philippe Pelletier, de la Direction des services communs.

Approbation

_____ _____

Sous-ministre Date

ANNEXE 1

Historique

Ministère du Travail, de l'Emploi et de la Solidarité sociale
Québec

Politique ministérielle sur la gestion de sécurité de l'information	
Émise le **2015-09-28**	Révisée le
Prochaine révision prévue le 2020-09-30	Codification RI-04-00-00

Description du changement	Approbation	Date
Adoption de la Politique ministérielle sur la gestion de la sécurité de l'information, qui remplace la Politique de gestion de la sécurité de l'information en vigueur depuis le 5 mars 2009.	Sous-ministre	2015-09-28