POLITIQUE

DE SÉCURITÉ DE L'INFORMATION

MARS
2018

MINISTÈRE DE L'AGRICULTURE,
DES PÊCHERIES
ET DE L'ALIMENTATION

TABLE DES MATIÈRES

CONTEXTE

Le ministère de l'Agriculture, des Pêcheries et de l'Alimentation (MAPAQ) intervient dans des domaines d'activité variés, soit la production agricole, la pêche et l'aquaculture commerciales, la transformation des aliments et des boissons, la commercialisation des aliments (distribution en gros et au détail), de même que dans le réseau de l'hôtellerie, de la restauration et des institutions, aussi connu sous le nom de « réseau HRI ». Il a aussi la responsabilité de contribuer à la protection de la santé publique et à l'amélioration de la santé animale en exerçant une surveillance de toute la chaîne bioalimentaire. Enfin, par l'entremise de l'Institut de technologie agroalimentaire, il est présent dans le domaine de la formation collégiale et professionnelle.

Ministère

La mission du Ministère est d'appuyer une offre alimentaire de qualité et de promouvoir l'essor du secteur bioalimentaire dans une perspective de développement durable, pour le mieux-être de la société québécoise.

Pour remplir sa mission, le Ministère recueille, produit, utilise, conserve ou détruit une information abondante qui concerne les citoyens, les entreprises et le personnel, ainsi que la gestion ministérielle ou gouvernementale. Elle peut revêtir une importance stratégique pour le Ministère comme pour l'État et avoir une valeur légale, administrative, économique ou patrimoniale. En conséquence, l'information, c'est-à-dire l'actif informationnel, constitue une ressource essentielle qu'il convient de protéger durant tout son cycle de vie, quel qu'en soit le support ou l'emplacement.

La présente politique assure aussi le respect des obligations du Ministère en vertu de la Directive sur la sécurité de l'information gouvernementale et prend en considération les meilleures pratiques reconnues mondialement, par exemple celles qui sont colligées dans le référentiel COBIT[MD]. La mise en œuvre de cette politique sera notamment soutenue par un cadre de gestion ministériel de la sécurité de l'information.

OBJECTIFS DE LA POLITIQUE

La Politique de sécurité de l'information a pour objet de munir le Ministère de manière adéquate pour exercer une saine gouvernance de la sécurité de l'information. Elle constitue le premier plan du cadre organisationnel et vise les objectifs suivants :

1. Protéger l'information tout au long de son cycle de vie, quel qu'en soit le support ou l'emplacement;
2. Assurer la disponibilité de l'information gouvernementale de façon qu'elle soit accessible en temps voulu et de la manière requise par une personne autorisée;
3. Assurer l'intégrité de l'information de manière que celle-ci ne soit pas détruite ni altérée de quelque façon sans autorisation et au moyen d'un support qui lui procure la stabilité et la pérennité nécessaires;
4. Limiter la divulgation de l'information confidentielle aux seules personnes autorisées à en prendre connaissance;
5. Permettre de confirmer, lorsque cela est nécessaire, l'authenticité d'un document ou l'identité d'une personne ou d'un dispositif qui accède à l'information;
6. Se prémunir contre le refus d'une personne de reconnaître sa responsabilité à l'égard d'un document ou d'un autre objet, notamment au regard d'un dispositif d'identification avec lequel elle a un lien;
7. Assurer l'archivage ou la destruction des documents en fonction de leur valeur légale, administrative, économique ou patrimoniale dans le respect du calendrier de conservation du Ministère et conformément aux normes en vigueur en matière de gestion documentaire.

CHAMP D'APPLICATION

Actif informationnel

Cette politique porte sur l'actif informationnel que détient ou utilise le Ministère, peu importe sa nature, sa localisation et le support sur lequel il se trouve, et ce, durant tout son cycle de vie, c'est-à-dire depuis sa collecte ou sa création jusqu'à son versement à Bibliothèque et Archives nationales du Québec ou sa destruction en conformité avec le calendrier de conservation du Ministère.

Personnes visées

Cette politique s'applique à l'ensemble du personnel du Ministère, aux clients, visiteurs, étudiants, mandataires, partenaires et fournisseurs ainsi qu'aux personnes qui interviennent pour leur compte. Elle concerne également l'information confiée à des tiers et toute forme d'échange ou de communication de renseignements, y compris la prestation électronique de services.

Activités

Cette politique doit être prise en considération dès la conception d'un processus ou d'un système d'information, de même qu'au moment de la préparation d'ententes, de contrats ou de conventions ou de l'acquisition d'une solution technologique.

PRINCIPES DIRECTEURS

Responsabilité et imputabilité

L'atteinte des objectifs de sécurité de l'information exige l'attribution claire des responsabilités à tous les échelons de l'organisation et l'adoption de processus de gestion de la sécurité assurant une reddition de comptes appropriée. Ainsi, la sécurité de l'information représente une responsabilité collective et chaque personne a l'obligation de rendre des comptes en fonction de son rôle particulier. Il s'ensuit que la sensibilisation et la formation à la sécurité de l'information s'avèrent des éléments essentiels.

Le détenteur a la responsabilité de voir au bon usage de l'information et des systèmes qui lui sont confiés. Il doit rendre compte de la mise en œuvre de mesures destinées à réduire les risques touchant la sécurité de l'information à un degré acceptable pour le Ministère.

Évolution

Les pratiques et les solutions retenues en matière de sécurité de l'information doivent être évaluées périodiquement afin de tenir compte des changements juridiques, organisationnels, technologiques, physiques ou environnementaux ainsi que de l'évolution des menaces et des risques.

Universalité

Les pratiques et les solutions retenues en matière de sécurité de l'information doivent correspondre, dans la mesure du possible, à des façons de faire reconnues et généralement utilisées à l'échelle nationale ou internationale, par exemple celles qui sont colligées dans le référentiel COBIT[MD].

Éthique

Les processus de gestion de la sécurité de l'information doivent être soutenus par une démarche d'éthique visant à assurer la régulation des conduites et à favoriser la responsabilisation individuelle.

Gestion des incidents

Le processus de la gestion des incidents permet de préparer l'organisation en vue de la prise en charge d'incidents susceptibles de compromettre la sécurité de l'information, depuis cette prise en charge jusqu'au retour à la normale. Il prévoit, le cas échéant, l'escalade jusqu'aux autorités ministérielles ou gouvernementales. Il prévoit également l'arrimage avec d'autres processus du Ministère, dont le plan des mesures d'urgence et le plan de continuité de services.

RÔLES ET RESPONSABILITÉS DES PRINCIPAUX ACTEURS

Sous-ministre

Le sous-ministre est le premier responsable de la protection et de la sécurité de l'information ainsi que de la gouvernance de ces aspects. Il approuve la présente politique.

Il nomme une personne pour agir comme responsable organisationnel de la sécurité de l'information (ROSI) qui voit à la mise en œuvre de cette politique. Il désigne les membres du Comité de gouvernance de la sécurité de l'information, approuve la charte de ce comité et statue sur les avis et recommandations du même comité. Il désigne également les détenteurs de l'information. Enfin, il approuve le plan d'action en matière de sécurité et autorise les budgets correspondants.

Comité de gouvernance de la sécurité de l'information

Le Comité de gouvernance de la sécurité de l'information (CGSI) examine et formule ses recommandations au sous-ministre à l'égard des orientations, des politiques, des directives, des cadres de gestion, des plans d'action et des bilans de sécurité de l'organisation, de même qu'il met en avant toute proposition d'action. Il reçoit en outre les éléments de reddition de comptes relativement à la sécurité de l'information et, le cas échéant, il formule la ou les recommandations sur les suites à donner.

Les membres du comité doivent s'assurer de la diffusion et de la reddition de comptes à l'égard de la sensibilisation et de la formation en sécurité et de la mise en œuvre des processus de sécurité dans leur secteur respectif.

Ils contribuent à la détermination des priorités annuelles en matière de sensibilisation de même qu'à la révision annuelle des risques à portée gouvernementale. Ils doivent également assurer l'arrimage entre le CGSI et leur secteur respectif pour tous les enjeux et toutes les initiatives concernant la sécurité.

Le CGSI, présidé par la secrétaire générale du Ministère[1], est notamment composé des personnes suivantes :

- Responsable organisationnel de la sécurité de l'information (ROSI);
- Détenteurs des actifs informationnels stratégiques ou critiques ou gestionnaire désigné pour les représenter;
- Directeur général de l'administration;
- Dirigeant sectoriel de l'information;
- Responsable de la gestion documentaire;
- Secrétaire du CGSI.

De plus, la personne responsable de la vérification interne participe au CGSI à titre d'observateur.

Le CGSI invite d'autres personnes en tant que collaborateurs selon les besoins.

1 La secrétaire générale du Ministère est également responsable de l'application de la Loi sur l'accès aux documents dans les organismes publics et sur la protection des renseignements personnels et responsable de la continuité des services en cas de sinistre.

Responsable organisationnel de la sécurité de l'information

Le responsable organisationnel de la sécurité de l'information (ROSI) représente le Ministère auprès du dirigeant principal de l'information (DPI) et il relaie les orientations et les priorités d'intervention gouvernementales relatives à la sécurité de l'information. Il assiste le sous-ministre dans la détermination des orientations stratégiques et des priorités d'intervention et le représente en ce qui a trait à la déclaration des risques et des incidents de sécurité de l'information à portée gouvernementale.

En outre, il assure la coordination et la cohérence des actions de sécurité de l'information menées au Ministère par les différents acteurs et il établit les partenariats internes à ces fins. Il assure également la coordination de la reddition de comptes du Ministère en matière de sécurité auprès du DPI et du Secrétariat du Conseil du trésor. De plus, il représente le Ministère auprès de toute autre organisation externe au chapitre de la sécurité de l'information, participe aux comités de sécurité gouvernementaux et développe les partenariats externes à ces fins.

Enfin, il représente le sous-ministre dans la gestion des situations ayant mis ou susceptibles d'avoir mis en péril la sécurité de l'information du Ministère.

Comité tactique de sécurité

Le Comité tactique de sécurité assure un suivi des risques, des incidents, des enjeux, des tendances, des projets et des initiatives en matière de sécurité.

Il est présidé par le ROSI et comprend les coordonnateurs organisationnels de la gestion des incidents (COGI), la conseillère organisationnelle en sécurité de l'information (COSI), le responsable du plan des mesures d'urgence du Ministère, la responsable de la continuité des services en cas de sinistre ou son adjointe, ainsi que le responsable de la sécurité physique ou son représentant.

Le ROSI peut inviter à se joindre au comité toute personne possédant une expertise jugée nécessaire.

Le comité se réunit sur une base régulière.

Coordonnateur organisationnel de la gestion des incidents

Le coordonnateur organisationnel de la gestion des incidents (COGI) voit à la mise en œuvre du processus de la gestion des incidents de sécurité de l'information au Ministère et il coordonne le volet technologique de la gestion des incidents. Il participe en outre au réseau d'alerte gouvernemental.

Le COGI contribue à la réalisation des analyses de risques de sécurité de l'information, à l'identification des menaces et des situations de vulnérabilité, puis il met en œuvre les solutions appropriées. Il collabore étroitement avec le ROSI et lui fournit le soutien technique nécessaire à l'exercice de ses responsabilités. Il participe également au comité tactique de sécurité.

Conseiller organisationnel en sécurité de l'information

Le conseiller organisationnel en sécurité de l'information (COSI) apporte son soutien au ROSI sur le plan tactique, notamment pour l'intégration de dispositions garantissant le respect des exigences de sécurité de l'information dans les ententes, les conventions et les contrats, pour la catégorisation des actifs informationnels, pour la réalisation des analyses de risques, de même que pour la tenue du registre d'autorité. Il collabore à l'élaboration et à la mise en œuvre de procédures officielles en matière de sécurité de l'information au Ministère.

Détenteur de l'information

Administrateur d'État ou gestionnaire désigné par le sous-ministre, le détenteur de l'information a la responsabilité de la catégorisation des actifs informationnels du Ministère ainsi que de la mise en œuvre des mesures de sécurité propres à assurer la protection de l'information stratégique ou critique qui est collectée, utilisée, communiquée, conservée ou détruite, mesures qui s'avèrent raisonnables compte tenu, notamment, de la sensibilité, de la finalité de l'utilisation, de

la quantité, de la répartition et du support de l'information. Il collabore étroitement avec le ROSI, le COSI et les COGI, notamment pour la catégorisation des actifs informationnels du Ministère, la détermination des exigences de sécurité, la gestion des incidents et la reddition de comptes en matière de sécurité.

Directeur des ressources informationnelles

Le directeur des ressources informationnelles recommande les moyens et les mécanismes de sécurité nécessaires pour assurer la protection des technologies de l'information et des communications ainsi que la relève des services informatiques nécessaires à la continuité des services essentiels en cas de sinistre. Il s'assure de l'intégration de la sécurité de l'information et de la protection des renseignements personnels au moment de bâtir, d'acquérir ou d'implanter des systèmes ou des technologies de l'information.

Il détermine l'équipement et les logiciels qui sont autorisés et assure la mise en œuvre des mesures de sécurité qui sont appropriées et conformes aux attentes des détenteurs de l'information. Enfin, il collabore étroitement avec le ROSI et lui fournit le soutien nécessaire à l'exercice de ses responsabilités.

Gestionnaire

Le gestionnaire est responsable de l'application et du respect de la présente politique au sein de son unité administrative, de même que de l'application des directives touchant la sécurité de l'information et des bonnes pratiques en cette matière. Il sensibilise chaque année les membres de son personnel à la protection de l'information, aux conséquences d'une atteinte à la sécurité de l'information ainsi qu'à leurs responsabilités en la matière.

Il veille à ce que les employés sous sa gouverne utilisent correctement les actifs informationnels. Il voit également à inclure les clauses sur la sécurité et la protection de l'information dans les contrats et les ententes. Il collabore étroitement avec le ROSI, les COGI et la COSI et il leur fournit le soutien nécessaire à l'exercice de leurs responsabilités.

Utilisateur

Tout utilisateur, y compris les employés, les étudiants, les visiteurs, les mandataires, les partenaires, les fournisseurs et ceux qui agissent pour leur compte, a l'obligation de protéger l'information mise à sa disposition. L'utilisateur a notamment les responsabilités suivantes :

- S'assurer de l'intégrité et de la confidentialité de l'information du Ministère;
- Suivre les directives et de respecter les consignes qui lui sont présentées;
- Utiliser l'information, quel que soit le support sur lequel elle se trouve, avec discernement, aux seules fins auxquelles elle est destinée et selon les droits qui lui sont accordés;
- Imprimer les documents sensibles avec les fonctionnalités d'impression protégée;
- Assurer, le moment venu, la destruction sécuritaire des documents sensibles;
- Utiliser uniquement l'équipement et les logiciels fournis par la Direction des ressources informationnelles ou autorisés par le directeur des ressources informationnelles;
- Agir avec précaution, notamment en s'abstenant d'utiliser l'information s'il a des doutes sur les règles applicables;
- Respecter les droits de propriété intellectuelle au moment de l'utilisation des produits et des documents;
- Signaler sans tarder à son supérieur immédiat toute situation ou tout incident susceptible de compromettre la sécurité de l'information.

DISPOSITIONS FINALES

Droit de regard et sanctions

Le Ministère a un droit de regard sur l'emploi de ses actifs informationnels par les utilisateurs, notamment par le contrôle de leurs droits d'accès à l'information. De ce fait, toute expectative de l'utilisateur en matière de protection de la vie privée s'en trouve restreinte.

Toute personne qui enfreint sciemment une règle applicable à la protection ou à la sécurité de l'information est passible notamment de l'une des sanctions suivantes :

- Les membres du personnel s'exposent à des mesures administratives ou à des sanctions disciplinaires pouvant aller jusqu'au congédiement;
- Les étudiants s'exposent aux sanctions prévus au Règlement institutionnel relatif aux conditions de vie des étudiants de l'Institut de technologie agroalimentaire;
- Les partenaires, les mandataires et les fournisseurs sont passibles de mesures administratives, par exemple la résiliation du contrat ou l'expulsion de la personne qui travaille pour son compte.

Enfin, des poursuites criminelles ou pénales pourraient être entreprises contre toute personne qui enfreindrait l'une de ces règles.

Mesure 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 ou au Comité de gouvernance de la sécurité de l'information après avoir pris soin d'évaluer les risques associés à la mesure d'exception.

En cas d'urgence, la mesure d'exception peut être autorisée par le gestionnaire responsable du domaine visé. Ce gestionnaire en fait rapport au ROSI.

Toute mesure d'exception est prise avec précaution.

Mise en œuvre, suivi et révision

Cette politique remplace la Politique de sécurité de l'information du Ministère qui a été adoptée en juillet 2015.

La mise en œuvre de la présente politique est soutenue par l'assignation des responsabilités définies dans le cadre de gestion de la sécurité de l'information du Ministère et par la mise en œuvre progressive des processus et des procédures particulières en matière de sécurité.

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

Approbation et date d'entrée en vigueur

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

Le sous-ministre,

ORIGINAL SIGNÉ

_____

Marc Dion
Le 29 mars 2018

ANNEXE 1 – DÉFINITIONS

Actif informationnel

Ce terme désigne tant l'information consignée dans un document que le système qui permet de la prendre en charge. L'actif informationnel peut être constitué de documents technologiques ou de documents papier ou encore d'une banque de données. Il peut s'agir aussi d'une technologie de l'information, d'une installation, d'un bien informatique ou d'un ensemble de ces éléments.

Catégorisation des actifs informationnels

La catégorisation des actifs informationnels en matière de sécurité de l'information est un processus qui permet d'évaluer le degré de sensibilité des renseignements que détient le Ministère, dans le but d'en déterminer le niveau de protection, eu égard aux risques potentiels aux chapitres de la disponibilité, de l'intégrité, de la confidentialité, de l'authentification et de l'irrévocabilité (DICAI).

Le Ministère peut ainsi tenir compte du degré de sensibilité déterminé de ses actifs informationnels pour mettre en œuvre les mesures lui permettant de se conformer à ses obligations légales, d'éviter des pertes financières, d'atteindre ses objectifs en ce qui a trait à la prestation de services et de rehausser la confiance des citoyens et des entreprises à l'égard de ses services et des services publics, en général.

La catégorisation d'un actif informationnel sert donc de base pour sécuriser le support sur lequel les renseignements sont conservés : papier, numérique (système informatique, clé USB, portable, etc.), enregistrement, audiovisuel, etc.

Continuité des services en cas de sinistre

La continuité des services repose sur un ensemble de processus et de procédures documentés qui permettent à l'organisation de continuer ou de rétablir ses processus d'affaires essentiels à un niveau minimal acceptable et à l'intérieur de délais acceptables préétablis pour l'organisation. L'organisation est ainsi en mesure de reprendre ses activités rapidement et efficacement à la suite d'incidents ou de perturbations (aléas), quelle qu'en soit la taille ou la cause.

Cycle de vie de l'information

Le cycle de vie de l'information consiste en l'ensemble des étapes que franchit une information depuis 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 de l'organisme public.

Document

Ce terme désigne un ensemble constitué d'information qui se trouve sur un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support, et est intelligible sous forme de mots, de sons ou d'images. Elle peut être communiquée au moyen de quelque mode d'écriture que ce soit, y compris un système de symboles transcrits sous l'une de ces formes. Est assimilée à un document toute 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.

Document technologique

Ce type de document s'appuie sur un support qui fait appel à une technologie de l'information, qu'elle soit électronique, magnétique, optique, sans fil ou autre. Toute banque de données qui permet la création de documents est assimilée à un document technologique (Loi concernant le cadre juridique des technologies de l'information).

Éthique

L'éthique fait référence à des valeurs partagées pour guider les actions. Elle implique une appropriation de règles déontologiques. Dans une situation donnée, la personne se fonde sur ces valeurs pour former son jugement et prendre une décision. Elle est amenée à réfléchir aux conséquences de ses actes avant de les poser. L'éthique fait ainsi appel au jugement de la personne et vise une action préventive.

Gestion des incidents

Le processus de la gestion des incidents permet de préparer l'organisation en vue de la prise en charge d'incidents susceptibles de compromettre la sécurité de l'information, depuis cette prise en charge jusqu'au retour à la normale. Il prévoit, le cas échéant, l'escalade jusqu'aux autorités ministérielles ou gouvernementales. Il prévoit également l'arrimage avec d'autres processus du Ministère, dont le plan des mesures d'urgence et le plan de continuité de services.

Gestion des risques

La gestion des risques fait partie de tout processus intégré de gestion de la sécurité de l'information au sein d'une organisation. Elle tient compte de l'analyse de la probabilité et des répercussions de différents scénarios de risque pour déterminer la stratégie à mettre en œuvre ainsi que le niveau requis des mesures de sécurité.

Incident touchant la sécurité de l'information à portée gouvernementale

Ce terme désigne une conséquence observable de la concrétisation d'un risque quant à la sécurité de l'information à portée gouvernementale. Une intervention concertée sur le plan gouvernemental est alors nécessaire.

Règle

Sous ce terme général sont compris la présente politique, les cadres de gestion et directives à venir ainsi que les lois et les règlements en vigueur, notamment la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et le Code criminel.

Renseignements personnels et confidentiels

L'article 54 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1) indique ce qui suit : « Dans un document, sont personnels les renseignements qui concernent une personne physique et permettent de l'identifier ». La Commission d'accès à l'information du Québec a précisé les trois critères énoncés dans cet article et permettant d'établir qu'un renseignement est personnel ou non :

- Il doit s'agir d'un « renseignement » (l'information doit faire connaître quelque chose);
- Le renseignement doit « concerner » (avoir trait à) une personne physique;
- Il doit permettre d'« identifier » cette personne (de la reconnaître par rapport à quelqu'un d'autre ou à différentes classes ou catégories d'individus, ou encore de reconnaître sa nature).

Par ailleurs, tout renseignement qui porte sur le secret industriel d'un tiers ou tout renseignement industriel, financier, commercial, scientifique, technique ou syndical est confidentiel.

Risque touchant la sécurité de l'information à portée gouvernementale

Ce type de risque porte atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information gouvernementale et peut avoir des conséquences sur la prestation de services à la population, sur la vie, la santé ou le bien-être des personnes, sur leur droit fondamental à la protection des renseignements qui les concernent, sur le respect de leur vie privée, sur l'image du gouvernement ou sur la prestation de services des autres organismes publics.

Sécurité physique

La sécurité physique concerne la protection de l'accès physique à des lieux, à de l'équipement, à du matériel, à des documents et à des personnes.

ANNEXE 2 – CADRE LÉGAL ET ADMINISTRATIF

Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, (RLRQ, chapitre G-1.03, art. 20).

Directive sur la sécurité de l'information gouvernementale (décret 7-2014 du 15 janvier 2014).

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 l'administration publique (RLRQ, chapitre A-6.01).

Lois administrées, politiques et directives du Ministère.

Loi sur le vérificateur général (RLRQ, chapitre V-5.01).

Charte canadienne des droits et libertés, partie 1 de la Loi constitutionnelle de 1982 (annexe B de la Loi de 1982 sur le Canada [1982, R.-U., chapitre 11]), art. 5 et 44.

Charte des droits et libertés de la personne (RLRQ, chapitre C-12).

Code civil du Québec (LQ, 1991, chapitre 64, art. 35 à 41).

Code criminel (LRC [1985], chapitre C-46).

Loi sur la sécurité civile (RLRQ, chapitre S-2.3).

Loi sur la fonction publique (RLRQ, chapitre F-3.1.1).

Loi sur les archives (RLRQ, chapitre A-21.1).

Loi sur le droit d'auteur (LRC [1985], chapitre C-42).

ANNEXE 3 – POSTES COMPORTANT DES RESPONSABILITÉS PARTICULIÈRES EN MATIÈRE DE SÉCURITÉ

Responsable de l'architecture en matière de sécurité de l'information

Cette personne conçoit l'architecture décrivant la fonction, la structure et les interrelations des composantes liées à la sécurité de l'information et veille à la mise en œuvre de cette architecture. Elle harmonise les solutions retenues avec les processus organisationnels en matière de sécurité de l'information. Elle participe également à la conception et à l'évaluation des composantes liées à la sécurité de l'information en ce qui concerne les solutions d'affaires élaborées ou acquises par son organisation.

Responsable de la continuité des services en cas de sinistre

Cette personne assure la gestion et la coordination du plan de continuité des services de son organisation. Plus particulièrement, elle en coordonne l'élaboration, veille à sa mise en œuvre et en assure la mise à jour. Elle élabore et mettre en place la politique de continuité des services du Ministère ainsi que les processus et les procédures nécessaires à sa réalisation. Elle s'occupe également de l'élaboration et de la mise en œuvre du programme de maintenance, du programme d'exercice et du programme de formation et de sensibilisation en matière de continuité des services en cas de sinistre. Enfin, elle s'assure de l'arrimage du plan de continuité des services du Ministère avec les principaux acteurs internes et externes des mesures d'urgence et de la sécurité civile.

Responsable de la sécurité physique

Cette personne met en place les mesures de protection physique des locaux de son organisation et de sécurisation de leurs accès, notamment lorsqu'ils abritent des systèmes et des installations technologiques stratégiques ou essentiels ou encore des supports où se trouve de l'information confidentielle. Plus particulièrement, elle s'occupe de la conception et de la mise en œuvre des mesures de protection physique des biens contre les sinistres, les pertes, les dommages ou le vol ainsi qu'au moment de l'interruption des activités de l'organisation. Elle s'assure également d'une mise au rebut sécuritaire des supports de l'information. Enfin, elle élabore des directives, des guides et des procédures propres à son domaine d'intervention et veille à leur mise en œuvre.

Responsable de la gestion des technologies de l'information

Cette personne contribue à l'élaboration et à la mise en œuvre de directives propres à assurer la sécurité de l'information numérique détenue par son organisation. Elle veille à l'application des mesures permettant d'assurer la sécurité de cette information, dont les plans de reprise informatique pour les cas de sinistre. Elle veille également à l'instauration d'un cadre normatif de développement qui permet la prise en charge des exigences en matière de sécurité de l'information, y compris les exigences légales pour la protection des renseignements personnels, et ce, dans la réalisation d'un projet de développement ou l'acquisition d'un système d'information.

Responsable de la vérification interne

Cette personne joue un rôle clé dans la reddition de comptes en matière de sécurité de l'information, plus particulièrement au regard de la détermination, de l'évaluation de la gestion des risques d'atteinte à la sécurité de l'information. À ce titre, elle examine ou vérifie, notamment, l'application, la validité et l'efficacité des règles, des mesures administratives et des moyens technologiques liés à la sécurité de l'information. Elle vérifie également que la sécurité de l'information est intégrée correctement dans les processus d'affaires.

Responsable de la gestion documentaire

Cette personne collabore à la conception des systèmes informatiques, administratifs ou autres. Elle s'assure qu'à toutes les étapes du cycle de vie de l'information, ces systèmes permettent une saine gestion des connaissances et du patrimoine informationnel, la préservation des preuves et le respect des lois en vigueur. Elle collabore étroitement avec les détenteurs de l'information et le responsable ou le conseiller organisationnel en matière de sécurité de l'information en vue de déterminer, de gérer, de coordonner et de mettre en œuvre des mesures de sécurité, quel qu'en soit le support.

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

Cette personne 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, elle communique au responsable organisationnel en matière de sécurité de l'information toute problématique ou préoccupation eu égard à la protection des renseignements personnels ou sensibles. Elle contribue à assurer la cohérence et l'harmonisation des interventions qui concernent la sécurité de l'information, l'accès aux documents et la protection des renseignements personnels, notamment au cours de la mise en œuvre du processus de la gestion des risques et des incidents touchant la sécurité de l'information à portée gouvernementale.

Responsable du développement ou de l'acquisition de systèmes d'information

Cette personne conçoit, met en œuvre et documente les fonctionnalités de sécurité à intégrer dans les systèmes d'information, y compris celles liées au respect des exigences légales en matière de protection des renseignements personnels. Elle s'assure également de leur bon fonctionnement.

Répondant ministériel en matière d'éthique

Cette personne veille au respect de l'éthique dans les processus de gestion de la sécurité de l'information pour assurer la régulation des conduites et la responsabilisation individuelle.

Agriculture, Pêcheries et Alimentation
Québec

18-0062