Politique relative à la sécurité de l’information et à la protection des renseignements personnels

Commission des normes, de l’équité, de la santé et de la sécurité du travail (CNESST)

Mars 2023

Commission des normes, de l’équité,
de la santé et de la sécurité du travail
cnesst.gouv.qc.ca

CNESST

CONTEXTE

La Commission des normes, de l'équité, de la santé et de la sécurité du travail (Commission) fait la promotion des droits et des obligations en matière de travail et en assure le respect, et ce, tant auprès des travailleuses et travailleurs que des employeurs du Québec.

Pour ce faire, elle :

- favorise des relations et des conditions de travail justes et équilibrées;
- assure l'implantation et le maintien de l'équité salariale;
- vise la prise en charge de la santé et de la sécurité par les milieux de travail, indemnise les victimes de lésions professionnelles et veille à leur réadaptation.

L'objectif de la Commission est de simplifier l'accès aux services en créant une porte d'entrée unique en matière de travail pour la population du Québec.

La Commission est dirigée par un conseil d'administration paritaire formé d'un(e) président(e) et d'un nombre égal de représentants des travailleurs et des employeurs. Comptant près de 5000 employé(e)s, elle assure sa présence sur tout le territoire québécois par l'intermédiaire de ses bureaux régionaux, son centre administratif à Montréal et son siège social à Québec. Elle offre une gamme de produits et de services à sa clientèle, ses partenaires et à ses fournisseurs notamment par le biais de la prestation électronique de services (PES), laquelle permet de faciliter et d'accélérer l'échange d'information. Depuis quelques années, la PES prend d'ailleurs une place grandissante dans la livraison de ses services.

Afin de réaliser sa mission, la Commission recueille, détient, utilise et communique une masse d'informations. Une partie de celles-ci provient d'un réseau d'organisations, de professionnels et d'organismes partenaires avec lesquels la Commission collabore régulièrement.

Consciente de la valeur de cette information, la Commission a la responsabilité d'en assurer la protection. Cela nécessite donc la mise en place de directives et de mesures de protection soutenues par une Politique relative à la sécurité de l'information et à la protection des renseignements personnels. La sécurité de l'information et la protection des renseignements personnels requièrent l'engagement et la collaboration de l'ensemble du personnel de la Commission. Les responsabilités qui en découlent doivent être portées par la haute direction, qui a la responsabilité d'assurer le respect de cette politique.

CADRE NORMATIF

La Commission doit respecter un cadre normatif s'appliquant à l'information et aux documents qu'elle détient. Plusieurs lois, règlements ou autres documents normatifs encadrent l'accès et la protection des renseignements personnels ainsi que la sécurité de l'information à la Commission. Une liste de ces documents se retrouve en annexe.

Ce cadre normatif impose des obligations en matière d'accès aux documents, de diffusion de l'information et de protection des renseignements confidentiels. Ces renseignements confidentiels sont constitués de tous les renseignements personnels, à l'exclusion de ceux à caractère public, ainsi que de l'ensemble des renseignements que détient la Commission et dont elle doit assurer la confidentialité, la disponibilité et l'intégrité.

Notamment, la Commission doit permettre à toute personne, physique ou morale, qui en fait la demande, d'avoir accès aux documents administratifs qu'elle détient, sous réserve de l'application d'une restriction légale au droit d'accès. Elle doit également permettre à toute personne physique d'avoir accès aux renseignements personnels qui la concernent.

La Commission doit divulguer, de manière proactive, certains documents et renseignements d'intérêt pour l'information du public, dans le but de permettre aux citoyens d'être mieux informés et de répondre à la volonté gouvernementale d'instaurer une plus grande transparence.

La Commission doit assurer la confidentialité des renseignements contenus dans les dossiers de sa clientèle (travailleurs, employeurs), des fournisseurs de services et des employé(e)s. Elle doit aussi protéger les renseignements de nature confidentielle fournis par un tiers et qui portent sur un renseignement industriel, financier, commercial, scientifique, technique ou syndical.

Finalement, la Commission doit assurer la préservation de la valeur juridique ou patrimoniale des documents qu'elle détient, peu importe leur support, et assurer la sécurité de l'information, c'est-à-dire sa disponibilité, sa confidentialité et son intégrité. La présente politique met en place une vision intégrée des différents aspects de la gestion de l'information.

OBJECTIFS

Cette politique témoigne de l'engagement de la Commission à l'égard de la sécurité de l'information et de la protection des renseignements personnels. Elle vise les objectifs suivants :

- Maintenir une vision et une compréhension communes de la protection des renseignements confidentiels et de la sécurité de l'information par l'implication continue de tous les gestionnaires et employé(e)s de la Commission;
- Protéger et sécuriser l'information tout au long de son cycle de vie;
- Assurer le respect des cadres législatifs, réglementaires et administratifs applicables en matière de sécurité de l'information et en matière d'accès et de protection des renseignements confidentiels;
- Protéger l'information de nature confidentielle contre la consultation, l'utilisation ou la divulgation non autorisée;
- Assurer la qualité de l'information et la protéger contre toute atteinte à son intégrité ou à sa disponibilité susceptible de causer des torts à la population ou au gouvernement.

PORTÉE

La Politique relative à la sécurité de l'information et à la protection des renseignements personnels porte sur l'information détenue ou utilisée par la Commission, peu importe la nature de l'information, sa localisation ou le support sur lequel elle se trouve, et ce, durant tout son cycle de vie. Elle détermine notamment les orientations et les principes directeurs qui doivent être considérés dès l'étape de conception d'un processus ou d'un système d'information, ou lors de l'élaboration d'ententes ou de l'acquisition d'une solution technologique. Cette politique s'applique à tout le personnel de la Commission, à ses mandataires et à ses fournisseurs ainsi qu'à ceux qui interviennent pour leur compte.

ORIENTATIONS

Cette section définit les orientations que la Commission entend poursuivre en matière de sécurité de l'information et de protection des renseignements personnels.

Soutenir l'encadrement de la sécurité de l'information

Un encadrement adéquat de la sécurité de l'information passe par la définition d'une structure organisationnelle où les rôles et les responsabilités sont attribués à tous les niveaux de l'organisation. Il est également nécessaire d'avoir une gestion rigoureuse des risques, particulièrement ceux dont les effets peuvent être préjudiciables à la clientèle que dessert la Commission.

Favoriser une gestion intégrée de la protection des renseignements confidentiels et de la sécurité de l'information

La protection des renseignements détenus sur la clientèle de la Commission, les fournisseurs et le personnel contribue au développement d'une relation basée sur le respect et la confiance. Les directives et les mesures de protection doivent donc contribuer à renforcer cette confiance tout en permettant aux clientèles, aux fournisseurs et au personnel d'avoir accès aux renseignements qui les concernent. Pour contribuer à relever le niveau de protection des informations détenues par la Commission, il faut favoriser un modèle de gouvernance qui soutient la gestion intégrée de la protection des renseignements confidentiels et de la sécurité de l'information.

Maintenir un niveau de maturité adéquat en sécurité de l'information

Pour permettre l'atteinte du niveau de maturité en sécurité de l'information[1] convenable pour l'organisation, il faut normaliser, intégrer, documenter et implanter les processus de sécurité de l'information. La Commission doit également s'assurer que l'information détenue est sécurisée, conformément aux bonnes pratiques de sécurité de l'information. À la suite d'une analyse de maturité des systèmes effectuée périodiquement, l'application de mécanismes de coordination et de contrôle permet alors de faire évoluer la gestion de la sécurité de l'information vers le niveau de maturité souhaité pour la Commission.

Perfectionner les compétences en sécurité de l'information et en protection des renseignements confidentiels

L'efficacité des mesures de sécurité et de protection des renseignements confidentiels déployées par une organisation est en grande partie tributaire du degré de sensibilisation du personnel quant à leur mise en œuvre**.** L'adoption de bonnes pratiques par le personnel contribue efficacement à protéger l'information.

Outre la sensibilisation du personnel, la Commission doit également s'assurer, par des actions de formation, que celui-ci dispose de l'expertise et du savoir-faire nécessaires à la mise en œuvre de bonnes pratiques de sécurité de l'information et de protection des renseignements confidentiels. La préoccupation à l'égard de la protection des renseignements confidentiels et de la sécurité de l'information doit être partagée par le personnel, les partenaires et les fournisseurs.

1 Le modèle CMMI *(Capability Maturity Model + Integration)* définit une échelle de mesure de la *maturité* à cinq niveaux. La maturité d'une organisation est le degré auquel celle-ci a déployé explicitement et de façon cohérente des processus qui sont documentés, gérés, mesurés, contrôlés et continuellement améliorés.

PRINCIPES DIRECTEURS

La Commission assure la sécurité de l'information et la protection des renseignements confidentiels conformément aux principes directeurs ci-dessous.

1. Classifier l'information et évaluer les risques

1.1. Dès l'étape de la conception d'un processus ou d'un système d'information, les informations sont classifiées par leur détenteur(trice) et sont protégées selon le besoin en matière de confidentialité, de disponibilité et d'intégrité, de façon à considérer les principes et les règles applicables en sécurité de l'information.

1.2. À moins qu'il ne s'agisse d'une exigence légale, le choix des mesures de sécurité de l'information s'appuie sur une analyse des risques auxquels l'information peut être exposée. Une évaluation des risques est effectuée avant de procéder à tout changement significatif au système d'information, à l'infrastructure ou avant d'acquérir une solution technologique.

1.3. Une évaluation des facteurs relatifs à la vie privée doit être faite de tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels.

2. Respecter les mesures assurant la protection des renseignements confidentiels

2.1. Les renseignements confidentiels sont recueillis et utilisés seulement s'ils sont nécessaires à l'exercice de la mission de la Commission.

2.2. L'architecture des processus d'affaires et des systèmes d'information qui les sous-tendent tient compte des principes et des règles applicables à la protection des renseignements confidentiels.

3. Assurer la disponibilité de l'information

3.1. L'information doit être accessible en temps voulu et de la manière requise par une personne autorisée.

3.2. La lisibilité des documents technologiques est assurée pendant toute leur période de conservation.

3.3. En tenant compte du Plan des services essentiels, en cas de sinistre, des plans visant à assurer la disponibilité de l'information nécessaire sont établis, testés et maintenus à jour.

4. Assurer l'intégrité de l'information

4.1. L'information n'est pas détruite ou altérée de quelque façon sans autorisation et le support de cette information lui procure la stabilité et la pérennité voulues.

4.2. Des mesures de sécurité physiques et logiques protègent l'information contre la perte ou le dommage accidentel ou délibéré.

4.3. La collecte de l'information est effectuée auprès de sources fiables afin de garantir la qualité de cette information.

4.4. L'intégrité des documents est assurée tout au long du cycle de vie de ces documents de manière à préserver leur valeur, et ce, en fonction de leur catégorisation et de l'évaluation des risques.

5. Gérer le patrimoine informationnel

5.1. Les documents sont inventoriés et classés de manière à en assurer le repérage et l'accessibilité.

5.2. Les mesures de protection sont prises en fonction de la valeur particulière du document et des besoins d'accès, conformément à la loi.

5.3. L'archivage ou la destruction des documents qui ne sont plus nécessaires est fait selon la nature de l'information à détruire et le calendrier de conservation des documents.

6. Contrôler les accès des utilisateurs

6.1. L'organisation forme son personnel sur ses rôles et responsabilités à l'égard de la protection des renseignements confidentiels et de la sécurité de l'information à laquelle il a accès et le sensibilise à ce sujet.

6.2. L'accès à l'information est autorisé uniquement aux personnes dont les tâches le requièrent et en fonction de leur catégorisation. Des mécanismes appropriés assurent la gestion des permissions et des autorisations d'accès.

6.3. L'identité d'une personne est validée avant tout accès à certaines informations, en fonction de leur catégorisation. Le moyen employé pour établir l'identité d'une personne procure une assurance raisonnable qu'il s'agit bien de la bonne personne.

6.4. Les meilleures pratiques en matière de journalisation des accès sont mises en place afin de permettre la vérification des accès aux informations en fonction de leur catégorisation.

7. Contrôler l'accès physique à l'information

7.1. Contrôler l'accès aux lieux de la Commission afin que seules les personnes autorisées puissent pénétrer dans les locaux appropriés.

7.2. Garder les documents physiques confidentiels sous clé (pratique « bureau propre ») lorsqu'ils ne sont pas utilisés.

7.3. Lorsque des renseignements confidentiels sont discutés ou affichés, utiliser un espace de travail et des moyens technologiques appropriés afin d'en protéger la confidentialité.

8. Donner accès aux renseignements confidentiels en toute sécurité

8.1. Les bénéficiaires, les employeurs ainsi que les membres du personnel peuvent accéder à leur dossier selon les conditions prévues par la loi. Toute personne doit établir son identité avant d'accéder à son dossier. Le moyen utilisé pour établir l'identité fournit une assurance raisonnable qu'il s'agit de la bonne personne.

8.2. La communication de renseignements confidentiels à la personne qui en fait la demande est effectuée en fonction d'une juste appréciation des risques et de façon à protéger la confidentialité, l'intégrité et la disponibilité de ces renseignements.

PARTAGE DES RESPONSABILITÉS

La présente section expose sommairement les rôles des principaux intervenants et des comités, tandis que l'ensemble des rôles et responsabilités, ainsi que la composition des comités sont décrits en détail dans le Cadre de gestion sur la sécurité de l'information et la protection des renseignements personnels.

Présidente directrice générale (PDG)

La présidente directrice générale (PDG) nomme les personnes qui occuperont les fonctions suivantes :

- dirigeant de l'information (qui agit à titre de chef délégué de la sécurité de l'information), après recommandation du dirigeant principal de l'information;
- coordonnateur organisationnel des mesures de sécurité de l'information;
- détenteurs de l'information;
- responsable de l'accès à l'information et de la protection des renseignements personnels.

Ces personnes assurent la mise en œuvre de cette politique conformément aux responsabilités qui leur sont confiées.

La présidente directrice générale doit également approuver plusieurs documents stratégiques en sécurité de l'information, dont certains à l'occasion d'un comité de direction.

Comités organisationnels en sécurité de l'information

Il y a trois comités organisationnels en sécurité de l'information :

- le comité sur l'accès à l'information et la protection des renseignements personnels (CAIPRP), présidé par la présidente directrice générale;
- le comité aviseur – volet gouvernance en sécurité de l'information (CA-VGSI), présidé par le chef délégué de la sécurité de l'information;
- le comité tactique et opérationnel en sécurité de l'information (CTOSI), présidé conjointement par la responsable de l'accès à l'information et la protection des renseignements personnels et par le responsable opérationnel de cyberdéfense.

Ces comités sont les principales instances de concertation en matière de sécurité de l'information, d'accès à l'information et de protection des renseignements personnels. Ils regroupent les différentes personnes assumant des responsabilités en sécurité de l'information et ils coordonnent les différentes activités qui y sont liées.

Dirigeant de l'information

Le ou la dirigeante de l'information veille à l'application des règles de gouvernance et de gestion établies en matière de sécurité de l'information. Cette personne contribue, conjointement avec le dirigeant principal de l'information et le CERT/AQ (Équipe de réponse aux incidents de sécurité de l'information de l'Administration québécoise), à la définition et à la mise en œuvre du processus de gestion des incidents à portée gouvernementale.

Le dirigeant de l'information agit à titre de chef délégué de la sécurité de l'information (CDSI).

Chef délégué de la sécurité de l'information (CDSI)[2]

Le ou la CDSI assure la gouvernance de la sécurité de l'information. Cette personne détermine les orientations stratégiques et les priorités d'intervention. De plus, elle représente la Commission en matière de gestion des risques et des incidents de sécurité de l'information à portée gouvernementale.

Responsable opérationnel en cyberdéfense (ROCD)

Le ou la ROCD apporte son soutien au CDSI au niveau tactique et stratégique, notamment en ce qui a trait à la mise en œuvre des mesures de réduction des risques et à la mise en place des processus formels de sécurité de l'information.

Coordonnateur organisationnel des mesures de sécurité de l'information (COMSI)

Le ou la COMSI collabore étroitement avec le CDSI et le ROCD et leur fournit le soutien technique nécessaire à l'exercice de leurs responsabilités. Cette personne participe activement au réseau d'alerte gouvernemental et contribue à la mise en place du processus de gestion des incidents au sein de son organisation et du processus de gestion des incidents à portée gouvernementale.

Détenteur(trice) de l'information

Le ou la détenteur(trice) est responsable d'assurer la sécurité de l'information qui lui est confiée.

Détenteur(trice) adjoint(e) de l'information

Cette personne est chargée de soutenir le ou la détenteur(trice) de l'information dans l'exercice de ses fonctions.

Responsable de l'audit interne (RAI)

Le ou la RAI joue un rôle-clé dans la reddition de comptes en matière de protection et de sécurité de l'information.

Responsable de la sécurité des technologies de l'information (RSTI)

Le ou la RSTI contribue à l'élaboration et à la mise en œuvre de mesures propres à assurer la sécurité de l'information numérique détenue par son organisation.

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

Le ou la RAIPRP assure la gouvernance de l'accès aux documents et de la protection des renseignements confidentiels, incluant les renseignements personnels.

Cette personne assume les responsabilités que lui attribue la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et toute autre loi, règlement, politique ou directive en ces matières. Elle assure le lien avec la Commission d'accès à l'information et les instances gouvernementales responsables de l'application de cette loi.

2 Toute organisation gouvernementale doit avoir un chef de la sécurité de l'information organisationnelle (CSIO) qui se rapporte à un CDSI. Le CDSI est responsable de la sécurité pour un portefeuille d'organisations. Aucune autre organisation ne fait partie du portefeuille de la Commission, donc ici le CDSI cumule le rôle de CSIO. Ainsi, le rôle de CSIO n'est pas mentionné dans ce document.

Responsable de la gestion documentaire (RGD)

Le ou la RGD développe et met à jour les diverses composantes du système de gestion documentaire en vue de faciliter la classification et la conservation de l'information.

Responsable de l'éthique

Le ou la responsable de l'éthique veille notamment à l'intégration de l'éthique dans les processus de gestion de la sécurité de l'information afin d'assurer la régulation des conduites et la responsabilisation individuelle.

Responsable de la sécurité physique (RSP)

Le ou la RSP met notamment en place les mesures de protection physiques des locaux et sécurise leurs accès.

Gestionnaires

Les gestionnaires sont responsables de l'application et du respect de cette politique au sein de leur unité administrative. Ces personnes doivent informer et sensibiliser leur personnel aux dispositions de la présente politique et s'assurer que celui-ci n'accède qu'à l'information nécessaire à l'exercice de ses fonctions.

Le personnel

Le personnel, qu'il soit de l'interne ou de l'externe, est responsable d'appliquer et respecter les orientations, les normes, les mesures administratives et les moyens technologiques mis en œuvre à la Commission en matière de sécurité de l'information et de protection des renseignements personnels.

DROIT DE REGARD ET SANCTIONS

La Commission a un droit de regard sur l'utilisation de ses informations par les utilisateurs, notamment par le contrôle de l'utilisation de leurs droits d'accès à l'information.

Toute contravention aux règles de sécurité de l'information est passible de mesures administratives ou disciplinaires pouvant aller jusqu'au congédiement, selon la nature et la gravité de la contravention.

La Commission peut aussi prendre, contre tout fournisseur ou sous-traitant qui ne respecte pas les règles de sécurité de l'information, des mesures pouvant aller jusqu'à la cessation de la relation d'affaires; ou le remboursement à la Commission du montant que celle-ci pourrait être tenue de verser à titre de dommages et intérêts, en raison d'un acte ou d'une omission qui serait imputable à celui-ci, par son fait, ou celui de ses préposés; ou les deux.

Enfin, la Commission peut prendre des mesures pour des clients qui ne respectent pas ses règles de sécurité allant jusqu'à retirer les droits d'accès.

MISE EN APPLICATION ET SUIVI DE LA POLITIQUE

La responsabilité de l'application et de la mise en œuvre de la présente politique appartient à la personne nommée par la présidente directrice générale à titre de chef délégué de la sécurité de l'information.

DATE D'ENTRÉE EN VIGUEUR ET APPROBATION

La présente version de la politique entre en vigueur à la date de son approbation par le comité directeur.

ANNEXE

La liste des principales lois que la Commission administre ainsi que les autres lois et règlements à portée générale se retrouve ci-dessous :

- Loi sur les accidents du travail et les maladies professionnelles (chapitre A-3.001);
- Loi sur la santé et la sécurité du travail (chapitre S-2.1);
- Loi sur les normes du travail (chapitre N-1.1)
- Loi sur l'équité salariale (chapitre E-12.001)
- Charte des droits et des libertés de la personne (chapitre C-12);
- Code civil du Québec (L.Q. 1991, c. 64);
- Loi sur la fonction publique (chapitre F-3.1.1, a. 126);
- Loi sur le droit d'auteur (L.R.C. 1985, c. C-42);
- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03);
- Loi concernant le cadre juridique des technologies de l'information (chapitre C-1.1)
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1);
- Lois sur les archives (chapitre A-21.1);
- Règlement sur l'éthique et la discipline dans la fonction publique (chapitre F-3.1.1, r. 3);
- Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (chapitre A-2.1, r.0.2).

Autres documents normatifs **:**

- Calendrier de conservation de la Commission (conformément à la Loi sur les archives);
- Directive gouvernementale sur la sécurité de l'information (conseil du Trésor, décret numéro 1514-2021 du 8 décembre 2021);
- Cadre gouvernemental de gestion de la sécurité de l'information (arrêté 2022-04 du ministre de la Cybersécurité et du Numérique en date du 26 juillet 2022)
- Guide sur l'éthique et la discipline de la Commission de la santé et de la sécurité du travail;
- ISO 27001 : 2013, Spécifications pour la gestion de la sécurité dans les systèmes d'information;
- ISO 27002 : 2013, Code de bonne pratique pour la gestion de la sécurité de l'information.