Cadre de gestion sur la sécurité de l’information et la protection des renseignements personnels

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

MARS 2023

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

Table des matières

1 PRÉAMBULE

1.1 Définitions

Terme	Définition
AI - Accès à l'information	En vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, sauf exception et sous réserve de l'application d'une restriction légale au droit d'accès, toute personne qui en fait la demande a droit d'accès aux documents détenus par un organisme public dans l'exercice de ses fonctions. Ce droit s'exerce quelle que soit la forme de ces documents : écrite, graphique, sonore, visuelle, informatisée ou autre.
PRP - Protection des renseignements personnels	En vertu de différentes lois, la Commission des normes, de l'équité, de la santé et de la sécurité du travail (CNESST) a l'obligation d'assurer la protection des renseignements confidentiels qu'elle détient. Ceux-ci sont constitués de tous les renseignements personnels qui n'ont pas un caractère public ainsi que par l'ensemble des renseignements qu'elle détient et dont elle doit assurer la confidentialité. De plus, la *Loi sur les normes du travail* et la *Loi sur l'équité salariale* prévoient que la CNESST ne peut dévoiler pendant l'enquête l'identité du salarié concerné par une plainte, sauf si ce dernier y consent. Ces deux lois prévoient aussi qu'une personne nommée par la CNESST, responsable d'arriver à un accord et de régler la plainte à la satisfaction des parties, ne peut être contrainte de divulguer ce qui lui a été révélé ou ce dont elle a eu connaissance dans l'exercice de ses fonctions. Toute information, verbale ou écrite, recueillie par la personne visée doit demeurer confidentielle.
RPG - 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, sur la santé ou sur le bien-être des personnes, sur le respect de leurs droits fondamentaux à la protection des renseignements personnels qui les concernent et au respect de leur vie privée, sur l'image du gouvernement ou sur la prestation de services fournie par d'autres organismes publics.
IPG - Incident de sécurité de l'information à portée gouvernementale	Conséquence observable de la concrétisation d'un risque de sécurité de l'information à portée gouvernementale nécessitant une intervention concertée sur le plan gouvernemental.
Risque résiduel	Niveau de risque qui subsiste après la réponse au risque ou après l'application de mesures d'atténuation et de contrôle.
Actif informationnel	Un ensemble constitué d'information portée par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcriptibles sous l'une de ces formes ou en un autre système de symboles.

1.2 Encadrement légal, administratif et normatif

Le présent cadre de gestion s'inscrit dans une démarche visant à mettre en œuvre une gouvernance forte et intégrée de la sécurité de l'information gouvernementale. Le cadre légal, administratif et normatif sur lequel il s'appuie est le suivant :

- la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03);
- la Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;
- la Directive gouvernementale sur la sécurité de l'information (conseil du Trésor, décret numéro 1514-2021 du 8 décembre 2021);
- le 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);
- le Cadre de gestion des risques et des incidents à portée gouvernementale en matière de sécurité de l'information;
- les pratiques gouvernementales en matière de sécurité de l'information;
- les politiques et les directives relatives à la sécurité de l'information propres à la CNESST;
- la Loi sur la santé et la sécurité du travail;
- la Loi sur les accidents du travail et les maladies professionnelles;
- la Loi sur les normes du travail;
- la Loi sur l'équité salariale;
- la Loi concernant le cadre juridique des technologies de l'information (chapitre C-1.1);
- la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1);
- la norme internationale ISO/IEC 27001 :
    - ISO 27001 : 2013, Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences;
    - ISO 27002 : 2013, Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information.

1.3 Contexte

Le présent cadre est élaboré par la personne assumant le rôle de chef délégué de la sécurité de l'information (CDSI) en soutien à la mise en œuvre de la *Politique relative à la sécurité de l'information et à la protection des renseignements personnels* qui présente les orientations et les principes directeurs en matière de gestion de la sécurité de l'information. Le cadre de gestion vient donc préciser et départager les obligations et les responsabilités prévues à cette politique.

1.4 Objectifs du présent cadre de gestion

Le présent cadre de gestion s'appuie sur le 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). Ce dernier soutient la mise en œuvre des dispositions de la Directive gouvernementale sur la sécurité de l'information (conseil du Trésor, décret numéro 1514-2021 du 8 décembre 2021). Il précise l'organisation fonctionnelle de la sécurité de l'information gouvernementale ainsi que les rôles et les responsabilités requis pour une gouvernance forte et intégrée en la matière.

Les principaux objectifs sont :

1. attribuer et départager les rôles et les responsabilités des divers intervenants à tous les niveaux de l'organisation;

2. adopter une organisation fonctionnelle de la sécurité de l'information.

1.5 Principes directeurs

- La sécurité de l'information est un besoin d'affaires se traduisant par un ensemble de mesures et de processus dont l'amélioration continue est concrétisée dans un plan annuel de sécurité de l'information.

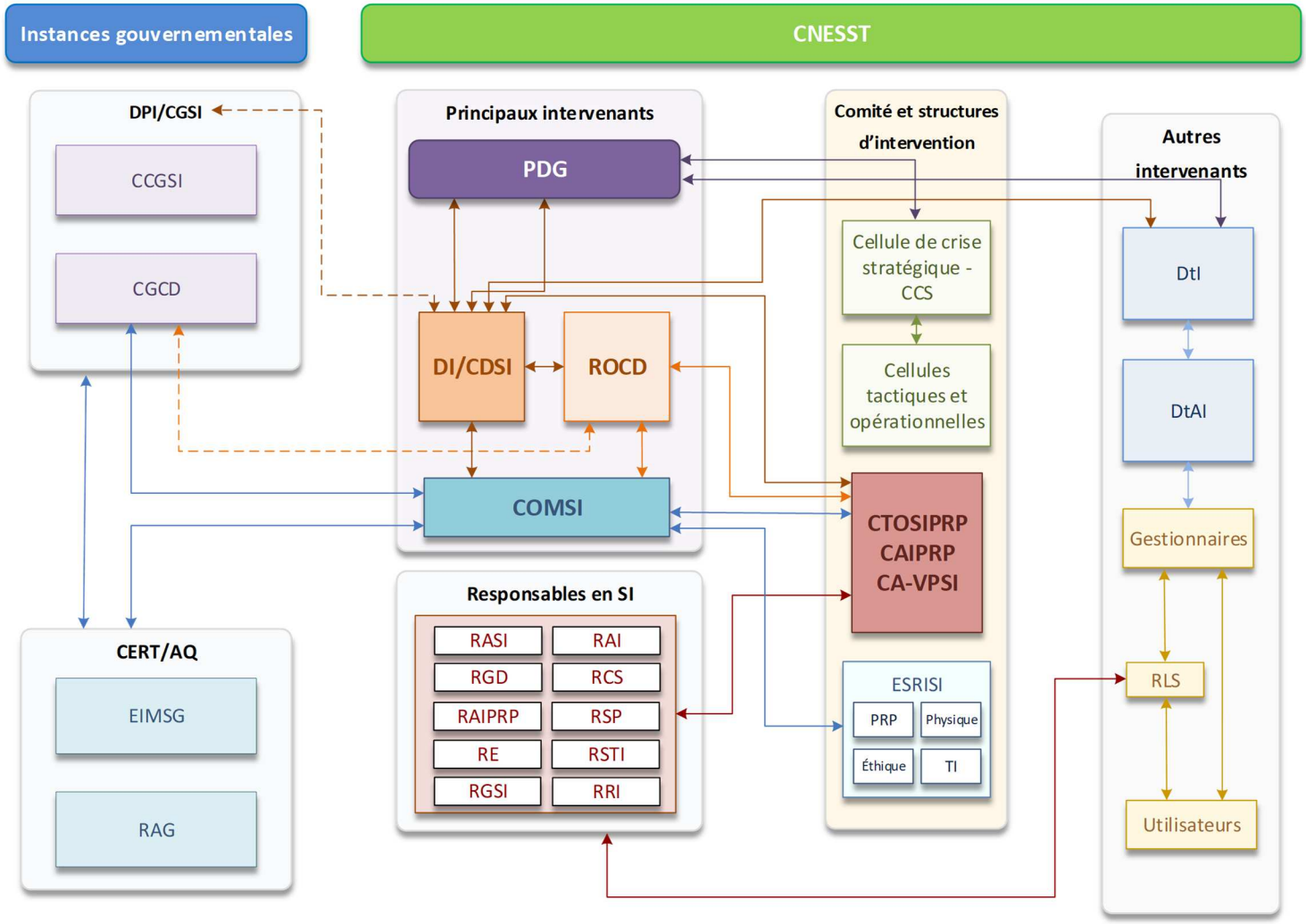
- La sécurité de l'information est prise en charge tout au long du cycle de vie des solutions et plus particulièrement en amont des changements importants et des projets.

- Tout actif informationnel se voit assigner un détenteur qui est responsable d'en assurer la sécurité et la protection des renseignements personnels.

- La cohérence des actions au chapitre de la gouvernance, de la conformité et de la gestion des risques est une responsabilité partagée par l'ensemble des unités de la CNESST.

1.6 Organisation fonctionnelle de la sécurité de l'information

La figure suivante présente les interactions entre les différentes parties prenantes du cadre de gestion.



CAIPRP	**Comité pour l'accès à l'information et la protection des renseignements personnels**
CA-VGSI	**Comité aviseur, volet gouvernance de la sécurité de l'information**
CCG	**Comité de crise gouvernemental**
CCGSI	**Comité de coordination gouvernementale de la sécurité de l'information**
CDSI	**Chef délégué de la sécurité de l'information**
CERT/AQ	**Computer Emergency Response Team de l'Administration québécoise**
CGCD	**Centre gouvernemental de cyberdéfense**
CGSI	**Chef gouvernemental de la sécurité de l'information**
COMSI	**Coordonnateur organisationnel des mesures de sécurité de l'information**
CTOSI	**Comité tactique et opérationnel en sécurité de l'information**
DI	**Dirigeant de l'information**
DtI	**Détenteur de l'information**
DtAI	**Détenteur adjoint de l'information**
DPI	**Dirigeant principal de l'information**
EIMSG	**Équipe intégrée sur les menaces à la sécurité de l'information gouvernementale**
ESRISI	**Équipes sectorielles de réponse aux incidents de la sécurité de l'information**
PDG	**Présidente directrice générale**
PRP	**Protection des renseignements personnels**
RAG	**Réseau d'alerte gouvernemental**
RAI	**Responsable de l'audit interne**
RAIPRP	**Responsable de l'accès à l'information et de la protection des renseignements personnels**
RASI	**Responsable de l'architecture de sécurité de l'information**
RCS	**Responsable de la continuité des services**
RE	**Responsable de l'éthique**
RGD	**Responsable de la gestion documentaire**
RGSI	**Responsable de la gouvernance SI**
RLS	**Répondant local de la sécurité**
ROCD	**Responsable opérationnel de la cyberdéfense**
RRI	**Responsable de la reprise des TI**
RSP	**Responsable de la sécurité physique**
RSTI	**Responsable de la sécurité des TI**
SI	**Sécurité de l'information**
TI	**Technologies de l'information**

Les rôles et les responsabilités en matière de gestion de la sécurité de l'information à la CNESST sont ainsi regroupés.

- Principaux intervenants en sécurité de l'information : font partie de ce groupe le dirigeant de la CNESST et les personnes devant obligatoirement être identifiées dans chacun des organismes publics.
- Responsables sectoriels en sécurité de l'information : ce groupe fait référence aux rôles des responsables de domaines connexes à la sécurité de l'information au sein de la CNESST.
- Autres intervenants : dans ce groupe se retrouvent tous les autres intervenants devant intervenir dans l'organisation pour une prise en charge de la sécurité de l'information.
- Comité et structures d'intervention : ce groupe fait référence aux différentes structures en place pour coordonner la sécurité de l'information aux divers paliers de gestion de la CNESST.

2 RÔLES ET RESPONSABILITÉS

2.1 Principaux intervenants

2.1.1 Présidente directrice générale

La personne qui assume ces fonctions doit :

- désigner une ou un coordonnateur organisationnel des mesures de sécurité de l'information (COMSI) pour la représenter auprès du réseau d'alerte gouvernemental et y participer activement;
- désigner un responsable de l'accès à l'information et de la protection des renseignements personnels (RAIPRP) pour assumer 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;
- désigner les détenteurs et les détentrices de l'information, personnel de l'organisation de niveau cadre qui ont pour responsabilités d'assurer la sécurité de l'information, et des ressources qui la sous-tendent, relevant de l'autorité de leur unité administrative;
- désigner un dirigeant de l'information afin d'assumer les responsabilités que lui attribue la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* et toute autre loi, règlement, politique ou directive en ces matières;
- veiller à l'élaboration et à la diffusion d'une politique ainsi que d'un cadre en matière de sécurité de l'information et en assurer l'approbation, la mise à jour ainsi que leur application;
- veiller au dépôt auprès du DPI, selon les modalités et le format fixés par ce dernier, d'une planification des actions de sécurité de l'information, des incidents et des risques de sécurité de l'information à portée gouvernementale, d'un bilan de sécurité de l'information ainsi que toute reddition de comptes en matière de sécurité de l'information jugée appropriée.

2.1.2 Dirigeant de l'information

La personne qui assume ces fonctions doit :

- veiller au suivi de la mise en œuvre des recommandations émises, à son endroit, par le Conseil du trésor ou par le DPI;
- définir, si nécessaire, des règles particulières en matière de gestion de l'information, incluant celles inhérentes à la sécurité de l'information;
- collaborer, au besoin, à la reddition de comptes en matière de sécurité de l'information auprès du Secrétariat du Conseil du trésor;

- veiller à la pérennité des actifs informationnels de la CNESST;
- agir à titre de chef délégué de la sécurité l'information (CDSI)

2.1.3 Chef délégué de la sécurité de l'information (CDSI)

La personne agissant à titre de chef délégué de l'information assume, sous le lien fonctionnel du chef gouvernemental de la sécurité de l'information (CGSI) les responsabilités découlant de la Loi et de ses textes d'application. [1] Elle veille à la coordination et à la cohérence des actions en sécurité de l'information menées par les autres intervenants au sein de la CNESST. Ses responsabilités sont les suivantes :

- mettre en œuvre les décisions émanant du chef gouvernemental de la sécurité de l'information (CGSI), notamment les indications d'application et les indications d'application particulières, en coordonner l'exécution et veiller à leur application;
- mettre en œuvre le cadre de gouvernance qui régit la sécurité de l'information au sein de son organisation;
- diriger le Centre opérationnel de cyberdéfense, l'opérationnaliser, faire évoluer l'offre de services du centre;
- désigner, parmi les membres du personnel d'encadrement sous sa direction et conformément aux indications d'application du chef gouvernemental de la sécurité de l'information, un responsable opérationnel de cyberdéfense (ROCD) dont le rôle est de voir au bon fonctionnement du Centre opérationnel de cyberdéfense;
- mettre en œuvre toute action requise pour la prise en charge d'un événement de sécurité;
- élaborer, au besoin et dans un souci d'efficacité et de gestion performante des ressources informationnelles, des processus de sécurité de l'information, déployer les mesures y afférentes et assurer le suivi de leur mise en œuvre;
- veiller à l'élaboration et à la diffusion d'un registre d'autorités en matière de sécurité de l'information;
- veiller à la coordination, à la cohérence et à la conformité des actions en sécurité de l'information menées au sein de la CNESST par les autres intervenants, dont les détenteurs et détentrices de l'information ainsi que les unités responsables des ressources informationnelles, de l'accès à l'information et de la protection des renseignements

1 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.

personnels, de la gestion documentaire, de la sécurité physique, de la continuité des services essentiels et de l'éthique;

- veiller à ce que la CNESST contribue aux processus de sécurité de l'information à portée gouvernementale;
- veiller à la définition et à la mise en œuvre de l'ensemble des directives et processus formels de sécurité de l'information portant, notamment, sur la gestion des risques, la gestion des identités et de l'accès à l'information, la gestion des vulnérabilités, la gestion des événements ainsi que la gestion des incidents;
- veiller à la prise en charge des exigences de sécurité de l'information, y compris celles liées au respect des exigences légales de protection des renseignements personnels, confidentiels et sensibles, lors de la réalisation d'un projet de développement ou lors de l'acquisition d'un système d'information;
- veiller à la réalisation récurrente d'audits de sécurité de l'information et de tests d'intrusion et de vulnérabilité;
- veiller à ce que les ententes de services et les contrats, conclus avec les prestataires de services, les partenaires et les mandataires, stipulent des clauses garantissant le respect des exigences de sécurité de l'information;
- veiller à la définition et à la mise en place d'un programme formel et continu de formation et de sensibilisation du personnel en matière de sécurité de l'information;
- veiller à la conception et au maintien d'une architecture décrivant la fonction, la structure et les interrelations des composantes de sécurité de l'information et à l'arrimage des solutions retenues aux processus organisationnels de sécurité de l'information;
- élaborer et mettre en œuvre une politique et un cadre de gestion en matière de sécurité de l'information;
- veiller à l'élaboration et à la mise en œuvre des orientations stratégiques afférentes en sécurité de l'information, dans le respect des lois, des directives et des approches gouvernementales.
- présider le Comité aviseur, volet gouvernance de la sécurité de l'information (CA-VGSI) et y soumettre les orientations, les politiques, les directives, les cadres de gestion, les priorités d'action, les éléments de reddition de comptes ainsi que tout événement ayant mis ou qui aurait pu mettre en péril la sécurité de l'information;
- transmet une copie du registre des évènements de sécurité sur demande du chef gouvernemental de la sécurité de l'information (CGSI) dans les délais qu'il indique;
- fournir les informations demandées par le chef gouvernemental de la sécurité de l'information (CGSI) relativement à la reddition de comptes, ou toute autre information requise par lui;

2.1.4 Responsable opérationnel de la cyberdéfense (ROCD)

Le responsable opérationnel de cyberdéfense (ROCD) assume, dans l'organisation fonctionnelle de la sécurité de l'information, les responsabilités suivantes:

- appuyer le chef délégué de la sécurité de l'information (CDSI) dans la direction, l'opérationnalisation et l'évolution de l'offre de service de son centre opérationnel de cyberdéfense (COCD);
- conseiller le chef délégué de la sécurité de l'information (CDSI) notamment, sur les orientations, les priorités d'action, les pratiques communes de cybersécurité, les mécanismes de reddition de comptes et sur l'optimisation des ressources pour son organisation;
- contribuer à la mise en œuvre des processus gouvernementaux normalisés en matière de cybersécurité;
- assurer, une prise en charge rapide et concertée des événements de sécurité pour son organisation;
- représenter son portefeuille ou son organisation auprès de la Cellule gouvernementale de cyberdéfense;
- maintenir un registre des répondants en matière de sécurité de l'information visés à l'article 23 et qui lui sont rattachés, pour participer au Réseau d'alerte gouvernemental;
- effectuer régulièrement les vérifications de sécurité des systèmes à l'égard des menaces et des vulnérabilités et, lorsque requis, recommander les correctifs nécessaires à l'organisme public concerné;
- assurer le maintien d'un registre des événements de sécurité qui relèvent de son organisation;
- assurer l'accompagnement nécessaire en sécurité opérationnelle aux organismes publics relevant de son organisation;
- exercer toute autre activité de sécurité de l'information que lui attribue le chef délégué à la sécurité de l'information (CDSI).

2.1.5 Responsable de la gouvernance de la sécurité de l'information (RGSI)

En matière de gouvernance de la sécurité de l'information, le ou la RGSI a les responsabilités suivantes :

- élaborer et mettre en œuvre des directives propres à assurer la sécurité de l'information;

- mettre en œuvre les orientations organisationnelles découlant des directives gouvernementales et définir des politiques internes et les pratiques généralement admises à cet égard;

- formuler des recommandations et veiller à l'intégration de dispositions garantissant le respect des exigences de sécurité de l'information dans le cadre de la négociation des ententes de services et des contrats;

- élaborer, maintenir et diffuser un registre d'autorités en matière de sécurité de l'information;

- assister les détenteurs de l'information dans la classification (anciennement la catégorisation) et dans l'analyse des risques de sécurité de l'information relevant de leur responsabilité et maintenir un registre de ces actifs et de leur classification;

- coordonner et contribuer à la réalisation d'analyses de risques de sécurité de l'information de façon récurrente pour les actifs critiques de la CNESST;

- planifier et coordonner la mise en œuvre d'un programme formel et continu de formation et de sensibilisation auprès de tout le personnel en matière de sécurité de l'information et de protection des renseignements personnels;

- planifier et réaliser des audits de sécurité de l'information;

- collaborer à la mise en œuvre des processus formels de sécurité de l'information au sein de l'organisation;

- recevoir et prendre acte de tout avis de sécurité produit à la CNESST;

- produire pour l'organisation tout bilan, évaluation, vérification, reddition de comptes en matière de sécurité de l'information et de protection des renseignements personnels;

- élaborer et mettre en œuvre un processus formel de gestion des risques en matière de sécurité de l'information et l'arrimer au processus de gestion des risques de sécurité de l'information à portée gouvernementale.

2.1.6 Responsable de la reprise informatique (RRI)

Le ou la responsable de la reprise informatique collabore étroitement avec le responsable organisationnel de la cyberdéfense (ROCD), le responsable de la continuité des services essentiels et le responsable de la sécurité des technologies de l'information. Il a notamment les responsabilités suivantes

- identifier les infrastructures et systèmes technologiques nécessaires à la réalisation des services essentiels identifiés dans le plan de la continuité des services essentiels,

- élaborer le plan de reprise des technologies de l'information selon divers scénarios, qu'ils soient de nature accidentelle (sinistre) ou malveillante (cyberattaque),

- pour chaque élément inscrit, le plan doit préciser l'objectif de point de reprise (RPO, return point objective) visé ainsi que l'objectif du temps de reprise (RTO, recovery time objective);

- coordonner la réalisation de tests initiaux et récurrents des activités prévues à ce plan, et en assurer la pérennité.

2.1.7 Coordonnateur organisationnel des mesures de sécurité de l'information

La ou le COMSI collabore étroitement avec le CDSI afin de lui fournir le soutien nécessaire à l'exercice de ses fonctions et a pour responsabilités notamment :

- d'élaborer et de mettre en œuvre un processus organisationnel de gestion des incidents de sécurité de l'information à la CNESST, l'arrimer au processus de gestion des incidents de sécurité de l'information à portée gouvernementale;

- d'assurer la coordination de la gestion des incidents de sécurité de l'information à la CNESST et d'assister les équipes sectorielles de gestion des incidents de sécurité de l'information dans la prise en charge de leurs responsabilités et dans la mise en œuvre des stratégies de réaction appropriées;

- de maintenir un registre organisationnel des incidents de sécurité de l'information ayant mis ou qui auraient pu mettre en péril la sécurité de l'information;

- de déclarer au ROCD, CDSI, et au PDG les incidents de sécurité de l'information majeurs.

- de déclarer au ROCD, CDSI, au PDG, au CGCD et au CGSI, selon les modalités fixées par ceux, les incidents de sécurité de l'information à portée gouvernementale.

De plus, le CGCD a émis un processus de gestion des menaces, des vulnérabilités et des incidents (MVI) dans lequel il confère les responsabilités suivantes au COMSI :

- représenter la Commission et participer activement au Réseau d'alerte gouvernemental, coordonné par le CERT/AQ;

- identifier les MVI touchant son OP, en tenir informé son CSIO et les faire remonter selon les conditions définies par le processus de gestion des MVI, si nécessaire;

- s'assurer de l'élaboration, de la mise à jour et de l'application d'un plan interne de réponse aux MVI;

- s'assurer de la réalisation d'analyses de risques de sécurité;

- collaborer étroitement avec son CDSI et son responsable opérationnel de cyberdéfense (ROCD) en leur fournissant, notamment, le soutien technique nécessaire à l'exercice de leurs responsabilités.

2.2 Responsables sectoriels

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

À ce titre, la ou le RAIPRP doit notamment :

- mettre en œuvre les actions répondant aux exigences découlant de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et du *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels*;

- collaborer, lorsque requis, à la formulation des recommandations quant à l'intégration de dispositions garantissant le respect des exigences de protection des renseignements personnels dans le cadre d'ententes de services et de contrats, conclus avec les prestataires de services, les partenaires et les mandataires;

- participer, lorsque requis, à la prise en charge des exigences à l'égard de la protection des renseignements personnels lors de la réalisation 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 tels renseignements;

- coordonner l'équipe de réponse aux incidents de sécurité propre à son secteur d'activité, s'assurer que celle-ci dispose des processus et des procédures nécessaires à la prise en charge des incidents de sécurité et assurer une reddition de comptes à cet effet, et ce, conformément au processus organisationnel de gestion des incidents de sécurité de l'information en vigueur à la CNESST.

2.2.2 Responsable de l'audit interne

La personne responsable de l'audit interne joue un rôle-clé dans la reddition de comptes en matière de protection et de sécurité de l'information. À ce titre, elle doit notamment :

- évaluer, examiner ou vérifier l'application, la validité et l'efficacité des règles, des mesures administratives et des moyens technologiques en matière de protection et de sécurité de l'information élaborés et mis en œuvre;

- évaluer, examiner ou vérifier l'adéquation de l'intégration de la protection et de la sécurité de l'information dans les processus d'affaires;

- exercer un rôle-conseil relatif à l'identification, l'évaluation et la gestion des risques en sécurité de l'information;

- collaborer à la définition et à la mise en place d'un processus de gestion des événements de sécurité de l'information;

- collaborer, au besoin, à la réalisation de tout bilan, évaluation, vérification, reddition de comptes en matière de sécurité de l'information et de protection des renseignements personnels pour le Conseil du trésor ou pour la CNESST.

2.2.3 Responsable de l'architecture de sécurité de l'information

La personne responsable de l'architecture de sécurité de l'information doit notamment :

- en s'appuyant sur le présent cadre de gestion et les autres documents organisationnels en sécurité de l'information, concevoir et mettre en œuvre l'axe sécurité de l'architecture d'entreprise décrivant la fonction, la structure et les interrelations des mesures de sécurité de l'information de la CNESST et arrimer les solutions retenues aux processus organisationnels de sécurité de l'information;
    - soutenir l'élaboration et la mise en œuvre des directives propres à assurer la sécurité de l'information;
    - concevoir et collaborer à la mise en œuvre des processus formels portant sur la gestion de la sécurité de l'information;
    - intégrer les exigences de sécurité de l'information tout au long du cycle de vie des solutions et plus particulièrement en amont des changements importants et des projets, incluant lors de la réalisation d'un projet de développement ou lors de l'acquisition d'un système d'information;
- collaborer à la conception et à l'évaluation des composantes et des fonctionnalités de sécurité de l'information, y compris celles liées au respect des exigences légales de protection des renseignements personnels sous la responsabilité de la RAIPRP, à intégrer aux solutions d'affaires développées ou acquises par la CNESST.

2.2.4 Responsable de la sécurité des technologies de l'information

La personne responsable de la gestion de la sécurité des technologies de l'information doit notamment :

- mettre en œuvre et gérer les mesures permettant d'assurer la sécurité de l'information numérique détenue par la CNESST;
- planifier et réaliser des tests d'intrusion et de vulnérabilité, annuellement ou à la suite d'un changement susceptible d'avoir des conséquences sur la sécurité de l'information, et en dégager les priorités d'action et les échéanciers afférents;
- mettre en œuvre les processus formels de gestion des vulnérabilités et des événements;
- élaborer et maintenir les guides, les procédures et les règles opérationnels portant sur les solutions de sécurité;

- assister les responsables locaux de la sécurité (RLS) dans leurs fonctions;

- coordonner l'équipe de réponse aux incidents de sécurité propre à son secteur d'activité et s'assurer que celle-ci dispose des processus et des procédures nécessaires à la prise en charge des incidents de sécurité, conformément au processus organisationnel de gestion des incidents de sécurité de l'information en vigueur à la CNESST et assurer la reddition de comptes à cet effet.

2.2.5 Responsable de l'éthique

La personne responsable de l'éthique est responsable notamment :

- de veiller 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;

- de coordonner l'équipe de réponse aux incidents de sécurité propre à son secteur d'activité, s'assurer que celle-ci dispose des processus et des procédures nécessaires à la prise en charge des incidents de sécurité, conformément au processus organisationnel de gestion des incidents de sécurité de l'information en vigueur à la CNESST et assurer la reddition de comptes à cet effet.

2.2.6 Responsable de la sécurité physique

La personne responsable de la sécurité physique doit :

- concevoir et mettre en œuvre les mesures de protection physique de l'information contre les sinistres, les pertes, les dommages, les accès non autorisés, le vol ainsi que l'interruption des activités, notamment lorsque les locaux abritent des systèmes et des installations technologiques stratégiques ou essentielles ou des supports contenant de l'information confidentielle;

- veiller à la mise au rebut ou au recyclage sécuritaire des supports de l'information;

- élaborer et mettre en œuvre des directives, des guides et des procédures propres à son domaine d'intervention;

- coordonner l'équipe de réponse aux incidents de sécurité propre à son secteur d'activité, s'assurer que celle-ci dispose des processus et des procédures nécessaires à la prise en charge des incidents de sécurité, conformément au processus organisationnel de gestion des incidents de sécurité de l'information en vigueur à la CNESST, et assurer la reddition de comptes à cet effet.

2.2.7 Responsable de la gestion documentaire

La personne responsable de la gestion documentaire doit notamment :

- collaborer à la conception des systèmes informatiques, administratifs ou autres et veiller à ce que ces systèmes possèdent les qualités nécessaires à une saine gestion des connaissances et du patrimoine informationnel, à la préservation des preuves ainsi qu'au respect des lois, et ce, à toutes les étapes du cycle de vie de l'information;

- collaborer étroitement avec les détenteurs de l'information, la ou le CDSI ainsi que la ou le ROCD en vue de déterminer, de gérer, de coordonner et de mettre en œuvre des mesures de sécurité de l'information relatives à la gestion documentaire, indépendamment de son support;

- veiller au respect de la *Loi sur les archives*, en collaboration avec le Service du courrier et des archives de la Direction des ressources matérielles de la CNESST;

- veiller au respect de l'intégrité et de la confidentialité des documents, notamment lors du transfert vers un autre support et rendre disponibles à l'organisation, lorsque requis, le matériel et les outils nécessaires afin d'assurer la valeur juridique des documents ainsi transférés vers un autre support.

2.2.8 Responsable de la continuité des services

La personne responsable de la continuité des services essentiels assure la gestion et la coordination du Plan de continuité des services essentiels de la CNESST. Plus particulièrement, elle doit notamment :

- coordonner l'élaboration du Plan de continuité des services essentiels, veiller à sa mise en œuvre et en assurer la pérennité;

- évaluer l'état de la situation initiale lors d'une catastrophe et suivre son évolution;

- assurer la planification et la coordination des tests initiaux et récurrents;

- convoquer le Comité de continuité des services si la situation le requiert;

- être porte-parole du Comité de continuité des services lorsque le comité de crise se réunit;

- coordonner les activités du Comité de continuité des services;

- assurer le suivi d'après sinistre lors du retour à la normale des opérations.

2.3 Autres intervenants

2.3.1 Détenteur de l'information

Le rôle de détenteur de l'information est attribué à une personne désignée par la présidente directrice générale. Cette personne soutient le CDSI en ce qui concerne la mise en œuvre des processus et des mesures de sécurité de l'information. Ses responsabilités sont les suivantes :

- désigner une ou plusieurs personnes à titre de détentrice ou détenteur adjoint de l'information pour l'assister dans la réalisation de ses tâches;
- veiller à la classification des actifs informationnels sous sa responsabilité à chaque modification apportée à la structure d'information, que ce soit en mode projet ou en continuité, et consigner cette classification dans le registre organisationnel des actifs;
- gérer les risques de sécurité de l'information pour les actifs informationnels sous sa responsabilité et s'assurer de la prise en charge des risques résiduels;
- veiller à la mise en œuvre et au respect des règles, des guides et des procédures en matière de protection et de sécurité de l'information relatifs aux actifs informationnels sous sa gouverne;
- veiller à ce que les mesures de sécurité appropriées par rapport aux risques encourus soient mises en place, appliquées et périodiquement vérifiées afin de protéger les actifs informationnels sous sa gouverne;
- veiller à l'octroi, à la gestion et à la révision des accès aux actifs informationnels dont il est responsable, dans le respect des règles applicables à la CNESST;
- collaborer à tout bilan, évaluation, vérification, reddition de comptes en matière de sécurité de l'information et de protection des renseignements personnels.

2.3.2 Détenteur adjoint de l'information

Sur nomination du détenteur ou de la détentrice de l'information, la personne détentrice adjointe est chargée de soutenir la ou le détenteur de l'information afin de protéger l'information sous sa responsabilité. À cette fin, elle doit notamment :

- réaliser la classification des informations sous sa responsabilité à chaque modification apportée à la structure d'information en mode projet ou en continuité;
- réaliser les analyses de risques sur les actifs informationnels sous sa gouverne, présenter les risques résiduels ainsi que le plan de traitement de ces derniers au détenteur de l'information afin d'obtenir son approbation;

- mettre en application les mesures de sécurité appropriées par rapport aux risques encourus et vérifier périodiquement leur fonctionnement;

- participer à la prise en charge des exigences de sécurité de l'information, y compris celles reliées au respect des exigences légales de protection des renseignements personnels, confidentiels et sensibles, lors de la réalisation d'un projet de développement ou lors de l'acquisition d'un système d'information sous sa gouverne;

- communiquer à la ou au CDSI, les risques, les problématiques et les préoccupations en lien avec la sécurité de l'information ou la protection des renseignements personnels, incluant les renseignements confidentiels ou sensibles.

2.3.3 Répondant local de la sécurité

Les RLS agissent à titre de personnes-ressources au sein de leur unité administrative en matière de sécurité de l'information. Ils doivent notamment :

- collaborer à la mise en œuvre et à l'application des règles, des mesures administratives et des moyens technologiques applicables à la CNESST en matière de sécurité;

- collaborer à l'octroi, à la gestion et à la révision des accès aux actifs informationnels dans le respect des règles applicables à la CNESST;

- assister son gestionnaire dans ses tâches relatives à la sécurité de l'information et à la protection des renseignements personnels;

- promouvoir les bonnes pratiques en sécurité de l'information auprès des utilisateurs des unités administratives qu'il soutient.

2.3.4 Gestionnaires

Les gestionnaires ont l'obligation d'assurer une protection adéquate de l'information dont ils sont responsables. Ils doivent notamment :

- appliquer les indications du chef délégué de la sécurité de l'information (CDSI) et de la responsable de l'accès à l'information et de la protection des renseignements personnels (RAIPRP), qu'elles émanent d'eux ou du chef gouvernemental de la sécurité de l'information;

- rendre compte au CDSI, selon leurs modalités sectorielles, du respect des obligations en matière de sécurité de l'information et répondre aux demandes que lui formule ce chef à cet égard;

- désigner un RLS pour son unité administrative;

- informer le personnel interne et externe dont ils sont responsables des dispositions de la *Politique relative à l'accès, la protection et la sécurité de l'information* et les informer des directives, des standards et des procédures en vigueur en matière de sécurité de

l'information ainsi que des modalités liées à leur mise en œuvre et les sensibiliser à la nécessité de s'y conformer;

- veiller à ce que tout consultant, partenaire ou fournisseur s'engage à respecter et respecte effectivement les règles de protection et de sécurité de l'information formulées dans tout contrat de services attribué par l'organisation et sous sa gouverne;
- octroyer, gérer et réviser périodiquement les accès du personnel aux actifs informationnels sous la gouverne des détenteurs de l'information en s'assurant du respect du principe du moindre privilège;
- veiller à ce que les arrivées, les départs et les mouvements de personnel soient signifiés le plus rapidement possible aux répondants technologiques afin d'assurer l'intégrité dans les identifiants et dans les accès;
- aviser la ou le détenteur adjoint de l'information de tout problème ou risque pouvant affecter la sécurité des actifs informationnels sous sa gouverne;
- veiller à ce que le personnel sous sa responsabilité bénéficie d'une formation adéquate et de séances de sensibilisation périodiques en matière de sécurité de l'information et de protection des renseignements personnels;
- veiller à l'application du calendrier de conservation;
- communiquer au détenteur adjoint de l'information les risques, les problématiques et les préoccupations en lien avec la sécurité de l'information ou la protection des renseignements personnels, incluant les renseignements confidentiels ou sensibles.

2.3.5 Utilisateurs

Les utilisateurs, qu'ils soient employés, partenaires ou fournisseurs de services, sont responsables des actions posées à l'aide de leur code d'usager, prennent tous les moyens à leur disposition pour assurer la sécurité de l'information des actifs informationnels de la CNESST mis à leur disposition et n'ont accès qu'aux seules données nécessaires à l'exercice de leurs fonctions. Ils doivent notamment :

- respecter et appliquer les orientations, les normes, les mesures administratives et les moyens technologiques mis en œuvre à la CNESST en matière de sécurité de l'information et de protection des renseignements personnels;
- aviser leur gestionnaire de toute situation portée à leur connaissance et susceptible de compromettre la protection des actifs informationnels de la CNESST;
- participer aux activités de formation et de sensibilisation requises.

2.4 Comités et structures d'intervention

2.4.1 Comités organisationnels

Il y a trois comités en sécurité de l'information et protection des renseignements personnels:

- 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.

Ces comités doivent notamment :

- examiner et formuler des recommandations concernant les orientations, les politiques, les directives, les cadres de gestion, les plans d'action, les processus et les bilans de l'organisation ainsi que toute proposition d'action ou état d'avancement de projets en sécurité de l'information;
- recommander, pour approbation auprès du comité de direction, le plan annuel de la sécurité de l'information, la mise à jour de la *Politique relative à l'accès, la protection et la sécurité de l'information* ainsi que le présent cadre de gestion;
- analyser et formuler des recommandations concernant les événements ayant mis ou qui auraient pu mettre en péril la sécurité de l'information de l'organisation;
- collaborer à la définition et à la mise en œuvre de l'ensemble des processus formels de sécurité de l'information;
- donner son avis sur les mesures particulières à respecter permettant la prise en compte des éléments visant à assurer la sécurité de l'information et la protection des renseignements personnels, confidentiels et sensibles, dès la conception, la planification, la réalisation ou la modification 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 tels renseignements.

Ces comités regroupent différentes personnes assumant une responsabilité en matière de sécurité de l'information et de protection des renseignements personnels.

2.4.2 Cellule de crise stratégique

En cas d'incident critique de sécurité de l'information, la cellule de crise stratégique (CCS) de la CNESST, constituée en vertu du Plan de continuité des services essentiels et du processus organisationnel de gestion des incidents de sécurité de l'information, est appelée à intervenir, lorsque les tentatives de rétablissement des activités n'ont pas apporté les résultats escomptés ou qu'aucune mesure palliative n'a pu assurer la continuité ou la reprise rapide des services. À ce titre, la CCS a pour rôle notamment :

- d'assurer la coordination stratégique avec les parties prenantes, organismes gouvernementaux et ministères;
- d'autoriser la mise en œuvre de stratégies permettant d'assurer la prise en charge des incidents critiques de sécurité de l'information;
- d'adopter la déclaration de sinistre proposée par le coordonnateur de la CCS et approuver les budgets spéciaux correspondants;
- de décider du déploiement ou non des stratégies de continuité des services;
- de proposer des orientations à suivre ou des actions à prendre en cas de sinistre;
- de formuler des recommandations concernant le délestage en totalité ou en partie des activités de l'organisation;
- de communiquer avec les médias.

2.4.3 Cellules tactiques et opérationnelles

Les cellules tactiques et opérationnelles, constituées en vertu du Plan de continuité des services essentiels, ont notamment pour mandat, lors d'un incident critique de sécurité de l'information :

- de procéder à l'évaluation des dommages;
- de recommander à la CCS l'adoption d'une déclaration de sinistre;
- d'assurer la mise en œuvre des stratégies de rétablissement des opérations;
- d'assurer la coordination avec les intervenants de l'extérieur de l'organisation, le cas échéant.

2.4.4 Équipes sectorielles de réponse aux incidents de sécurité de l'information

Ces équipes ont pour mission d'aider la CNESST dans la gestion des incidents affectant la sécurité de l'information. Cette aide se traduit par des gestes concrets de coordination, de prise en charge et de réponse aux incidents de sécurité. Les équipes de réponse aux incidents de sécurité de l'information doivent notamment :

- établir les relations avec les fournisseurs externes, lorsque requis, ainsi qu'avec les autres équipes de réponse aux incidents en sécurité de l'information;
- interpeller tous les spécialistes et les intervenants qui sont les plus susceptibles de détenir les connaissances fines permettant de cerner l'incident et de freiner sa propagation;
- collaborer étroitement avec la ou le COMSI et lui fournir le soutien technique nécessaire à l'exercice de ses responsabilités;
- collaborer à l'élaboration et à la mise en œuvre du processus organisationnel de gestion des incidents de sécurité de l'information et à son arrimage au processus à portée gouvernementale;
- assurer une reddition de comptes des événements qui auraient pu mettre en péril la sécurité de l'information;
- maintenir un registre sectoriel des incidents ayant mis en péril la sécurité de l'information, documenter ces incidents et en assurer la reddition de comptes à la ou le COMSI.

3 DISPOSITIONS FINALES

3.1 Entrée en vigueur

Le présent Cadre de gestion sur la sécurité de l'information et la protection des renseignements personnels est complémentaire à la Politique relative à l'accès, la protection et la sécurité de l'information de la CNESST. Cette version a été adoptée en mars 2023 et remplace toute version antérieure.