Commission
d'accès à l'information
du Québec

CADRE DE GESTION DE LA SÉCURITÉ DE L'INFORMATION

Juin 2016

Table des matières

1 PRÉAMBULE

Le présent cadre de gestion de la sécurité de l'information est un complément à la politique de sécurité de l'information de la Commission d'accès à l'information (la Commission). Il vise à renforcer la gouvernance de la sécurité de l'information à la Commission, par la mise en place d'une structure organisationnelle de la sécurité de l'information et la définition des rôles et responsabilités à tous les niveaux de l'organisation.

Ce cadre est adopté en application de l'article 7 de la *Directive sur la sécurité de l'information gouvernementale* du Conseil du trésor.

2 CADRE LÉGAL ET ADMINISTRATIF

Le cadre de gestion est assujetti, entres autres, aux cadres légaux et administratifs suivants :

- la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, chapitre A-2.1);
- le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* (RLRQ, chapitre A-2.1, r. 02);
- la *Loi concernant le cadre juridique des technologies et l'information* (RLRQ, chapitre C-1.1);
- la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, chapitre G-1.03);
- la *Directive sur la sécurité de l'information gouvernementale*;
- le *Cadre gouvernemental de gestion de la sécurité de l'information*;
- le *Cadre de gestion des risques et incidents à portée gouvernementale en matière de sécurité de l'information*;
- *l'Approche stratégique gouvernementale 2014-2017 en sécurité de l'information gouvernementale*;
- la *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics*;
- la *Politique de sécurité de l'information de la Commission*.

3 DÉFINITIONS

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

Système d'information : Système constitué des ressources humaines (le personnel), des ressources matérielles (l'équipement) et des procédures permettant d'acquérir, de stocker, de traiter et de diffuser les éléments d'information pertinents pour le fonctionnement d'une entreprise ou d'une organisation. [1]

[1] Source : OQLF – Grand dictionnaire terminologique

4 ORGANISATION FONCTIONNELLE DE LA SÉCURITÉ DE L'INFORMATION

Le *Cadre gouvernemental de gestion de la sécurité de l'information* définit l'organisation fonctionnelle de la sécurité de l'information au gouvernement du Québec.

Cette organisation fonctionnelle s'articule autour des deux axes suivants :

1. La structure horizontale, constituée des instances gouvernementales ayant un rôle d'encadrement et de soutien pour les organismes publics;
2. La structure verticale, constituée des organismes publics responsables de la prise en charge des exigences de la sécurité de l'information qui leur incombe.

Voici une description de l'organisation fonctionnelle de la sécurité de l'information au niveau gouvernemental puis au niveau de la Commission.

4.1 AU NIVEAU GOUVERNEMENTAL

Le dirigeant principal de l'information appuie le Conseil du trésor dans sa fonction de gouverne de la sécurité de l'information gouvernementale et fournit aux organismes publics les outils et l'assistance leur permettant de prendre en charge les exigences de la sécurité de l'information au sein de leur organisation. Des organismes publics à portée horizontale comme le Centre de services partagés du Québec (CSPQ), le Secrétariat à l'accès à l'information et à la réforme des institutions démocratiques (SAIRID) du Ministère du Conseil exécutif et le Ministère de la Justice du Québec jouent un rôle d'encadrement et de soutien pour les organismes publics. Des instances de concertation comme la table des responsables organisationnels de la sécurité de l'information facilitent les échanges entre les organismes publics.

Le schéma suivant présente une vue d'ensemble de l'organisation fonctionnelle de la sécurité de l'information au gouvernement du Québec.

Pour plus de détails, veuillez consulter le Cadre gouvernemental de gestion de la sécurité de l'information.

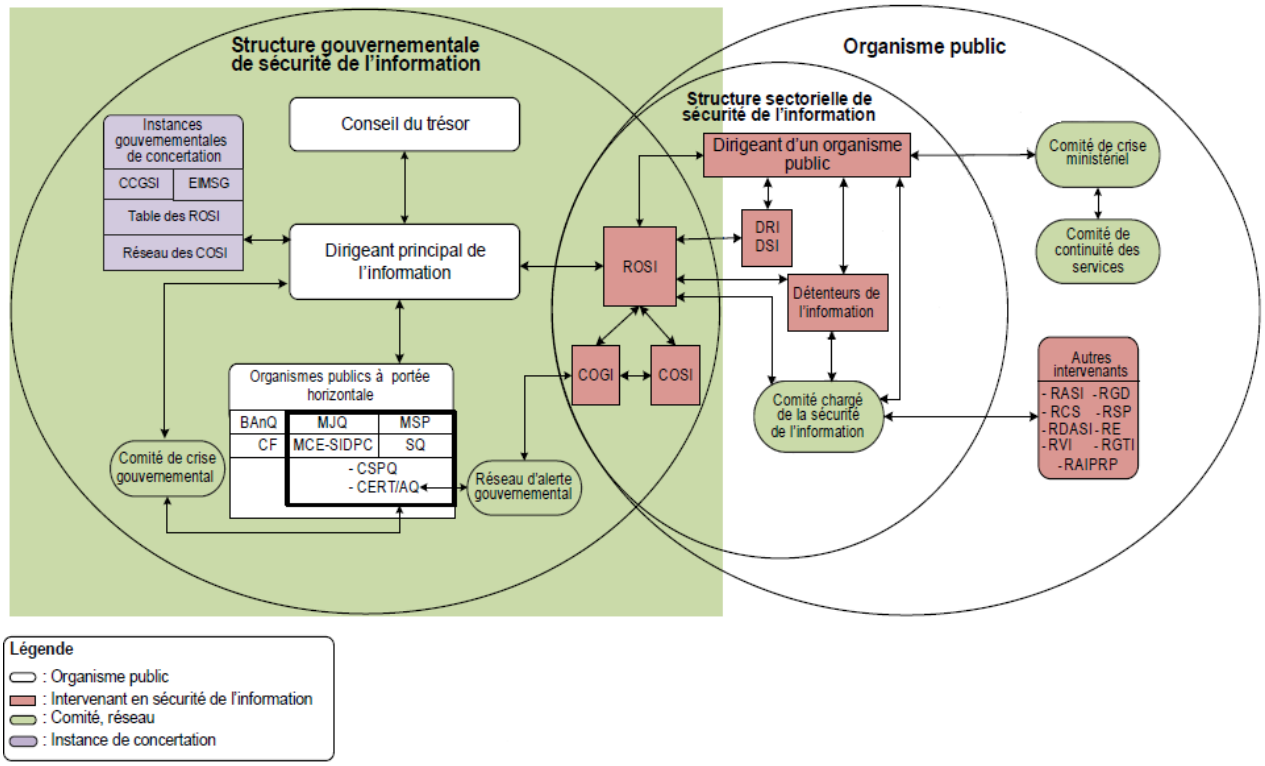

Figure 1 - Vue d'ensemble de l'organisation fonctionnelle de la sécurité de l'information au gouvernement du Québec

Acronymes

Organismes publics

BAnQ	Bibliothèque et Archives nationales du Québec
CERT/AQ	Équipe de réponse aux incidents de sécurité de l'information de l'administration québécoise
CF	Contrôleur des finances
CSPQ	Centre de services partagés du Québec
MCE – SIDPC	Ministère du Conseil exécutif – Secrétariat aux institutions démocratiques et à la participation citoyenne
MJQ	Ministère de la Justice du Québec
MSP	Ministère de la Sécurité publique
SQ	Sûreté du Québec

Instances gouvernementales de concertation

CCGSI	Comité de coordination gouvernementale de la sécurité de l'information
EIMSIG	Équipe intégrée sur les menaces à la sécurité de l'information gouvernementale

Intervenants en sécurité de l'information

COGI	Coordonnateur organisationnel de gestion des incidents
COSI	Conseiller organisationnel en sécurité de l'information
DPI	Dirigeant principal de l'information
DRI	Dirigeant réseau de l'information
DSI	Dirigeant sectoriel de l'information
RASI	Responsable de l'architecture de sécurité de l'information
RCS	Responsable de la continuité des services
RDASI	Responsable du développement ou de l'acquisition des systèmes d'information
RE	Responsable de l'éthique
RGD	Responsable de la gestion documentaire
RGTI	Responsable de la gestion des technologies de l'information
ROSI	Responsable organisationnel de la sécurité de l'information
RAIPRP	Responsable de l'accès à l'information et de la protection des renseignements personnels
RSP	Responsable de la sécurité physique
RVI	Responsable de la vérification interne

4.2 Au niveau de la Commission

Le président est le premier responsable de la sécurité de l'information à la Commission. À ce titre, il désigne les intervenants en sécurité de l'information. Les principaux intervenants sont le dirigeant sectoriel de la sécurité de l'information (DSI), le responsable organisationnel de la sécurité de l'information (ROSI), le conseiller organisationnel de la sécurité de l'information (COSI), le coordonnateur organisationnel de gestion des incidents (COGI) et les détenteurs de l'information. Il met également en place un comité chargé de la sécurité de l'information, un comité de crise en réponse aux incidents et un comité de continuité des services. Les autres intervenants comme le responsable de l'éthique ou de la sécurité physique sont également nommés par le président.

Une description détaillée des rôles et responsabilités des intervenants en sécurité de l'information est présentée à la section 5 – Rôles et responsabilités.

Pour un organisme de la taille de la Commission, un même intervenant pourra assumer plus d'un rôle et siéger à plus d'un comité. Pour faciliter les échanges avec les autres organismes publics et par souci de cohérence avec le *Cadre gouvernemental de gestion de la sécurité de l'information,* la Commission a décidé d'attribuer tous les rôles proposés par le cadre gouvernemental.

Les personnes désignées, la composition des comités et la liste des actifs principaux et leurs détenteurs sont présentés à l'Annexe A – Registre d'autorité.

Le schéma suivant présente l'organisation fonctionnelle de la sécurité de l'information au niveau de la Commission.

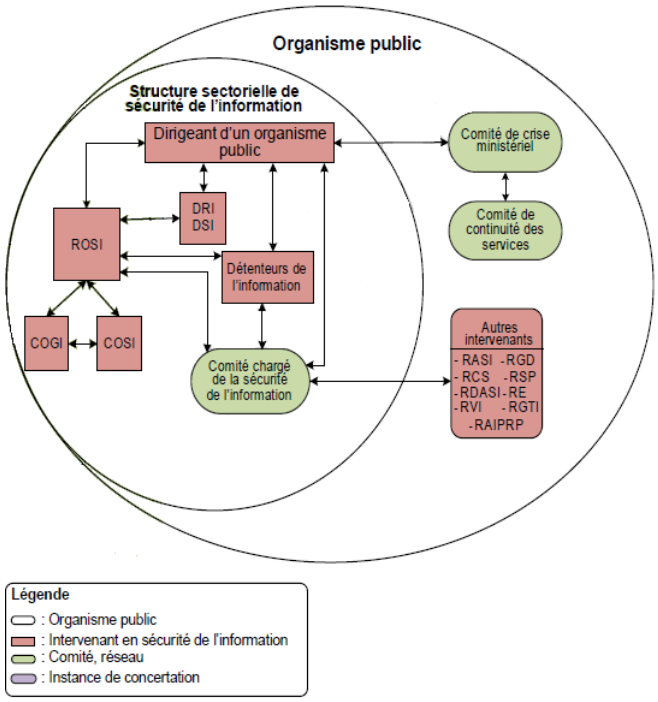

Figure 2 - Organisation fonctionnelle de la sécurité de l'information au niveau de la Commission

Acronymes

Organismes publics	
BAnQ	Bibliothèque et Archives nationales du Québec
CERT/AQ	Équipe de réponse aux incidents de sécurité de l'information de l'administration québécoise
CF	Contrôleur des finances
CSPQ	Centre de services partagés du Québec
MCE – SIDPC	Ministère du Conseil exécutif – Secrétariat aux institutions démocratiques et à la participation citoyenne
MJQ	Ministère de la Justice du Québec
MSP	Ministère de la Sécurité publique
SQ	Sûreté du Québec
Instances gouvernementales de concertation	
CCGSI	Comité de coordination gouvernementale de la sécurité de l'information
EIMSIG	Équipe intégrée sur les menaces à la sécurité de l'information gouvernementale

Intervenants en sécurité de l'information	
COGI	Coordonnateur organisationnel de gestion des incidents
COSI	Conseiller organisationnel en sécurité de l'information
DPI	Dirigeant principal de l'information
DRI	Dirigeant réseau de l'information
DSI	Dirigeant sectoriel de l'information
RASI	Responsable de l'architecture de sécurité de l'information
RCS	Responsable de la continuité des services
RDASI	Responsable du développement ou de l'acquisition des systèmes d'information
RE	Responsable de l'éthique
RGD	Responsable de la gestion documentaire
RGTI	Responsable de la gestion des technologies de l'information
ROSI	Responsable organisationnel de la sécurité de l'information
RAIPRP	Responsable de l'accès à l'information et de la protection des renseignements personnels
RSP	Responsable de la sécurité physique
RVI	Responsable de la vérification interne

5 RÔLES ET RESPONSABILITÉS

Les responsabilités en matière de sécurité de l'information sont attribuées aux intervenants suivants.

5.1 LES PRINCIPAUX INTERVENANTS

5.1.1 Le président

Le président est le premier responsable de la sécurité de l'information. À ce titre, il veille au respect du cadre gouvernemental de sécurité de l'information et s'acquitte de ses obligations, telles qu'elles sont édictées dans la *Directive sur la sécurité de l'information gouvernementale*.

À cet effet, il :

a) adopte les orientations stratégiques de la sécurité de l'information à la Commission, la politique, le cadre de gestion, les directives et les plans d's en la matière et en assure la mise en œuvre;
b) approuve les bilans de sécurité de l'information;
c) désigne le responsable organisationnel de la sécurité de l'information, le conseiller organisationnel de la sécurité de l'information, le coordonnateur organisationnel de gestion des incidents ainsi que les détenteurs, et leur attribue les responsabilités définies par le présent cadre de gestion;
d) s'assure de la mise en œuvre des processus officiels de sécurité de l'information permettant, notamment, de veiller à la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents;
e) s'assure de la réalisation périodique d'audits de sécurité de l'information et de tests d'intrusion et de vulnérabilités, conformément aux énoncés de la *Directive sur la sécurité de l'information gouvernementale*, et en dégage les priorités d'action ainsi que les échéanciers afférents;
f) favorise l'utilisation des services communs de sécurité de l'information déterminés par le Conseil du trésor;
g) s'assure que les ententes de service et les contrats conclus avec les prestataires de services, les partenaires et les mandataires comprennent des clauses garantissant le respect des exigences de sécurité de l'information;
h) s'assure de la mise en place d'un programme officiel et continu de formation et de sensibilisation du personnel en matière de sécurité de l'information;
i) approuve et présente aux instances gouvernementales concernées les plans d'action et les bilans requis, conformément aux énoncés de la *Directive sur la sécurité de l'information gouvernementale*.

5.1.2 Dirigeant sectoriel de l'information (DSI)

Le dirigeant sectoriel de l'information veille à l'application des règles de gouvernance et de gestion établies en matière de sécurité de l'information.

À cet effet, il :

a) assure le suivi de la mise en œuvre des recommandations émises par le Conseil du trésor ou par le dirigeant principal de l'information;
b) examine les plans d'action de la Commission et propose si nécessaire des modifications à y apporter;
c) contribue, conjointement avec le dirigeant principal de l'information et le CERT/AQ, à la définition et à la mise en œuvre du processus de gestion des incidents à portée gouvernementale.

5.1.3 Responsable organisationnel de la sécurité de l'information (ROSI)

Le responsable organisationnel de la sécurité de l'information représente la Commission auprès du dirigeant principal de l'information, en matière de sécurité de l'information.

À cet égard, il :

a) joue le rôle de porte-parole du dirigeant principal de l'information en matière de sécurité de l'information et lui fait part de ses réalisations;
b) transmet au président de la Commission les orientations et les priorités d'intervention gouvernementales et s'assure de leur mise en œuvre;
c) soumet aux fins de consultation, au comité chargé de la sécurité de l'information, soit le comité sur l'accès à l'information et sur la protection des renseignements personnels et la sécurité de l'information (AIPRP-SI), les orientations, les politiques, les directives, les cadres de gestion, les priorités d'actions, les éléments de reddition de comptes ainsi que tout événement ayant mis ou qui aurait pu mettre en péril la sécurité de l'information;
d) assure, en collaboration avec le comité AIPRP-SI, la coordination et la cohérence des actions de sécurité de l'information menées au sein de la Commission par d'autres intervenants dont, notamment, le responsable de l'accès à l'information et de la protection des renseignements personnels, les détenteurs de l'information ainsi que les unités responsables des ressources informationnelles, de la gestion documentaire, de la sécurité physique et de l'éthique;
e) s'assure de la contribution de la Commission au processus de gestion des risques et des incidents de sécurité de l'information à portée gouvernementale;
f) déclare au dirigeant principal de l'information les risques de sécurité de l'information à portée gouvernementale;
g) déclare au CERT/AQ les incidents de sécurité de l'information à portée gouvernementale;
h) définit et met en œuvre, en collaboration avec le comité AIPRP-SI, les processus officiels de sécurité de l'information tels que la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents;
i) coordonne l'élaboration et la mise en œuvre d'un programme continu de formation et de sensibilisation en matière de sécurité de l'information;
j) participe aux tables de coordination et de concertation gouvernementales en matière de sécurité de l'information;
k) participe à des comités interministériels et représente la Commission en matière de sécurité de l'information.

5.1.4 Le conseiller organisationnel en sécurité de l'information (COSI)

Le conseiller organisationnel en sécurité de l'information apporte, au niveau tactique, son soutien au ROSI, notamment en ce qui concerne la mise en œuvre des mesures de sécurité et la mise en place des processus officiels de sécurité de l'information.

À cet égard, il :

a) met en œuvre les orientations internes découlant des directives gouvernementales, des politiques internes et des pratiques généralement admises à cet égard;
b) produit les bilans et les plans d'action de sécurité de l'information de la Commission;
c) s'assure, en collaboration avec la Direction des affaires juridiques, de l'intégration de dispositions garantissant le respect des exigences de sécurité de l'information dans le cadre des ententes de service et des contrats;
d) assiste les détenteurs dans la catégorisation de l'information relevant de leur responsabilité et dans la réalisation des analyses de risques de sécurité de l'information;
e) élabore et met en œuvre le programme de formation et de sensibilisation en matière de sécurité de l'information;
f) tient à jour le registre d'autorité de la sécurité de l'information;
g) participe au réseau des conseillers organisationnels en sécurité de l'information;
h) propose au ROSI des orientations, des plans d'action et des bilans;
i) assure la coordination et la réalisation de projets de sécurité de l'information.

5.1.5 Le coordonnateur organisationnel de gestion des incidents (COGI)

Le coordonnateur organisationnel de gestion des incidents participe activement au réseau d'alerte gouvernemental et collabore étroitement avec le ROSI et le COSI.

Il a notamment pour responsabilités :

a) de contribuer à la mise en place du processus sectoriel de gestion des incidents de sécurité de l'information et du processus gouvernemental de gestion des incidents;
b) de tenir à jour le registre des incidents ayant pu mettre en péril la sécurité de l'information, de documenter ces incidents et d'en tenir informés le ROSI et le comité chargé de la sécurité de l'information, soit le comité AIPRP-SI;
c) de contribuer à l'analyse des risques de sécurité de l'information, de déterminer les menaces et les situations de vulnérabilité et de mettre en œuvre les solutions appropriées;
d) d'élaborer et de tenir à jour les guides portant sur la sécurité opérationnelle des systèmes et des réseaux de télécommunication.

5.2 LES AUTRES INTERVENANTS

5.2.1 Détenteurs de l'information

Les détenteurs de l'information désignés par le président sont notamment chargés :

a) de catégoriser l'information relevant de leur responsabilité en matière de disponibilité, d'intégrité et de confidentialité;
b) d'agir comme maîtres d'œuvre des analyses de risques et de s'assurer de la prise en charge des risques résiduels;

c) de participer à l'élaboration des orientations stratégiques, des politiques, des directives, des cadres de gestion, des guides, des plans d'action et des bilans;
d) de veiller à la mise en place et à l'application des mesures de sécurité de l'information, y compris celles liées au respect des exigences légales de protection des renseignements personnels;
e) de s'assurer de l'adéquation des mesures de sécurité de l'information en vigueur par rapport aux risques encourus.

5.2.2 Le gestionnaire

Le gestionnaire est responsable de la mise en œuvre, auprès du personnel relevant de son autorité, des dispositions de la politique de sécurité de l'information.

Il doit principalement :

a) informer son personnel des dispositions de la politique sur la sécurité de l'information et de toute directive, de tout standard et de toute procédure en vigueur en matière de sécurité de l'information, ainsi que des modalités liées à leur mise en œuvre, et le sensibiliser à la nécessité de s'y conformer;
b) s'assurer que les actifs informationnels mis à la disposition de son personnel sont utilisés en conformité avec les principes généraux et les exigences de la politique de sécurité;
c) aviser le ROSI dans les meilleurs délais, lorsqu'il soupçonne une violation des règles de sécurité ou toute anomalie pouvant nuire à la protection des actifs informationnels de la Commission;
d) s'assurer, en collaboration avec la Direction des affaires juridiques, que la sécurité de l'information est prise en compte dans tout contrat de service attribué par son unité administrative et voir à ce que tout consultant, partenaire ou fournisseur s'engagent à respecter et respectent les règles de sécurité de l'information de la Commission.

5.2.3 Les utilisateurs

Les utilisateurs jouent un rôle important dans la protection des actifs informationnels de la Commission.

À cette fin, les utilisateurs doivent :

a) prendre connaissance de la politique de sécurité de l'information de la Commission, des directives, des procédures et autres lignes de conduite qui seront prises par la suite par la Commission et s'y conformer;
b) utiliser les actifs informationnels mis à leur disposition en se limitant aux fins auxquelles ils ont été autorisés;
c) éviter tout comportement pouvant porter atteinte aux diverses mesures de sécurité mises en place par la Commission pour assurer la sécurité des actifs informationnels tels que la sécurité des lieux ou des équipements physiques et électroniques;
d) signaler immédiatement à son supérieur tout acte dont il a connaissance, susceptible de constituer une violation réelle ou présumée des règles de sécurité ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels de la Commission;
e) remettre, lorsqu'ils quittent la Commission, les différents actifs informationnels mis à leur disposition par la Commission tels que les cartes d'identité et d'accès aux locaux, les équipements électroniques et de téléphonie.

5.2.4 Responsable de l'architecture de sécurité de l'information

Le responsable de l'architecture de sécurité de l'information doit, notamment :

a) concevoir et mettre en œuvre l'architecture décrivant la fonction, la structure et les interrelations des composantes de sécurité de l'information;
b) arrimer les solutions retenues aux processus organisationnels de sécurité de l'information;
c) participer à la conception et à l'évaluation des composantes de sécurité de l'information des solutions d'affaires, élaborées ou acquises par la Commission.

5.2.5 Responsable de la gestion des technologies de l'information

Le responsable de la gestion des technologies de l'information doit, notamment :

a) contribuer à l'élaboration et à la mise en œuvre de directives contribuant à assurer la sécurité de l'information numérique;
b) mettre en œuvre les mesures permettant d'assurer la sécurité de l'information numérique détenue par la Commission, dont les plans de reprise informatique en cas de sinistre;
c) mettre en place, en collaboration avec le comité AIPRP-SI, un cadre normatif de développement assurant 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, lors de la réalisation d'un projet de développement ou lors de l'acquisition d'un système d'information.

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

Le responsable de l'accès à l'information et de la protection des renseignements personnels 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, il :

a) communique au ROSI, ainsi qu'aux membres du comité AIPRP-SI, les problématiques et les préoccupations de sécurité en matière de protection des renseignements personnels ou à caractère sensible;
b) contribue à assurer la cohérence et l'harmonisation des interventions entre la sécurité de l'information, l'accès aux documents et la protection des renseignements personnels, y compris lors de la mise en œuvre du processus de gestion des risques et des incidents de sécurité de l'information.

5.2.7 Responsable de la gestion documentaire

Le responsable de la gestion documentaire doit, notamment :

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

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

Le responsable du développement ou de l'acquisition de systèmes d'information conçoit, réalise et documente les fonctionnalités de sécurité de l'information, y compris celles liées au respect des exigences légales de protection des renseignements personnels, à intégrer aux systèmes d'information et s'assure de leur bon fonctionnement.

5.2.9 Responsable de la continuité des services

Le responsable de la continuité des services assure la gestion et la coordination du plan de continuité des services de la Commission.

Plus particulièrement, il :

a) coordonne l'élaboration du plan de continuité des services, veille à sa mise en œuvre et en assure la mise à jour;
b) assure la planification et la coordination des tests initiaux et récurrents.

5.2.10 Responsable de la sécurité physique

Le responsable de la sécurité physique met en place les mesures de protection physique des locaux et de sécurisation de leurs accès, notamment lorsqu'ils abritent des systèmes et des installations technologiques stratégiques ou essentielles ou des supports de l'information confidentielle.

Plus particulièrement, le responsable de la sécurité physique :

a) conçoit et met en œuvre les mesures de protection physique des biens contre les sinistres, les pertes, les dommages, le vol ainsi que l'interruption des activités de la Commission;
b) s'assure de la mise au rebut sécuritaire des supports de l'information;
c) élabore et met en œuvre des directives, des guides et des procédures propres à son domaine d'intervention.

5.2.11 Responsable de la vérification interne

Le responsable de la vérification interne 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 et de la gestion des risques d'atteinte à la sécurité de l'information.

À ce titre, il évalue, examine ou vérifie, notamment :

a) l'application, la validité et l'efficacité des règles, des mesures administratives et des moyens technologiques en matière de sécurité de l'information élaborés et mis en œuvre;
b) l'adéquation de l'intégration de la sécurité de l'information dans les processus d'affaires.

5.2.12 Responsable de l'éthique

Le responsable de l'éthique veille 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.

5.3 LES COMITÉS

5.3.1 Comité sur l'accès à l'information et sur la protection des renseignements personnels et la sécurité de l'information (AIPRP-SI)

Ce comité est présidé par le président. Il est composé, notamment, du responsable de l'accès aux documents et de la protection des renseignements personnels, du ROSI, des détenteurs de l'information ainsi que des unités responsables des ressources informationnelles, de la vérification interne, de la gestion documentaire, de la sécurité physique et de l'éthique.

En plus de son rôle en matière d'accès à l'information et de protection des renseignements personnels, ce comité est la principale instance sectorielle de concertation en matière de sécurité de l'information.

Plus particulièrement, en matière de sécurité de l'information, le comité, sous l'autorité du dirigeant sectoriel de l'information :

a) examine et formule des recommandations concernant les orientations, les politiques, les directives, les cadres de gestion, les plans d'action et les bilans de la Commission, ainsi que toute proposition d'action ou état d'avancement de projets en sécurité de l'information;
b) analyse et formule des recommandations concernant les événements ayant mis ou qui auraient pu mettre en péril la sécurité de l'information de la Commission.

5.3.2 Comité de continuité des services

Le comité de continuité des services est principalement composé du responsable de la continuité des services, des détenteurs de l'information, du ROSI, du COSI et du COGI.

Il a pour rôle, notamment :

a) de procéder à l'évaluation des dommages;
b) de recommander au comité de crise l'adoption d'une déclaration de sinistre;
c) d'assurer la mise en œuvre du plan de mobilisation;
d) d'assurer la coordination avec les intervenants externes.

Ce comité peut s'adjoindre toute autre personne en mesure de lui assurer le soutien adéquat dans ses prises de décision. Il est présidé par le responsable de la continuité des services ou son représentant.

5.3.3 Comité de crise

En cas d'incident critique de sécurité de l'information, le comité de crise est le groupe décisionnel appelé à intervenir, notamment 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, il a pour rôle, principalement :

a) d'autoriser la mise en œuvre de stratégies permettant d'assurer la prise en charge des incidents critiques de sécurité de l'information;
b) d'adopter la déclaration de sinistre proposée par le responsable de la continuité des services et d'approuver les budgets spéciaux correspondants;
c) de décider du déploiement ou non des plans de continuité des services;
d) de proposer des orientations à suivre ou des actions à prendre en cas de sinistre;
e) de formuler des recommandations concernant le délestage, en totalité ou en partie, des activités de la Commission;
f) de communiquer avec les médias.

Le noyau permanent de ce comité est composé de représentants de la haute direction, du ROSI, du responsable de la protection des renseignements personnels, du responsable de la sécurité physique et du responsable de la continuité des services. Ce comité peut s'adjoindre toute autre personne en mesure de lui assurer le soutien adéquat dans ses prises de décision. Citons, à titre d'exemple, les détenteurs de l'information ou les conseillers pour les volets juridique, technologique et de communication avec les médias et les ressources humaines.

Le comité de crise est présidé par le président.

6 DISPOSITIONS FINALES

a) le présent cadre de gestion entre en vigueur à la date de son approbation par le président;
b) ce cadre de gestion est complémentaire à la politique de sécurité de l'information de la Commission.

23 juin 2016

Jean Chartier, président **Date**

ANNEXE A – REGISTRE D'AUTORITÉ

Désignation des intervenants en sécurité de l'information	
Dirigeant sectoriel de l'information (DSI)	Rémi Bédard
Responsable organisationnel de la sécurité de l'information (ROSI)	Rémi Bédard
Conseiller organisationnel de la sécurité de l'information (COSI)	Jean-Pierre Philibert
Coordonnateur organisationnel de gestion des incidents (COGI)	Jean-Pierre Philibert
Responsable de l'architecture de sécurité de l'information (RASI)	Jean-Pierre Philibert
Responsable de la gestion des technologies de l'information	Jean-Pierre Philibert
Responsable de l'accès à l'information et de la protection des renseignements personnels	Claire-Élaine Audet
Responsable de la gestion documentaire	Miguel Poiré
Responsable du développement ou de l'acquisition de systèmes d'information	Jean-Pierre Philibert
Responsable de la continuité des services	Jean-Pierre Philibert
Responsable de la sécurité physique	Pierre Jobin
Responsable de la vérification interne	À définir
Responsable de l'éthique	Sophie Giroux-Blanchet

Composition des comités en sécurité de l'information	
Comité sur l'accès à l'information et sur la protection des renseignements personnels et la sécurité de l'information (AIPRP-SI)	Le comité AIPRP-SI est présidé par le président. Il est composé, notamment, du responsable de l'accès aux documents et de la protection des renseignements personnels, du ROSI, des détenteurs de l'information ainsi que des unités responsables des ressources informationnelles, de la vérification interne, de la gestion documentaire, de la sécurité physique et de l'éthique. Ce comité peut s'adjoindre toute autre personne en mesure de lui assurer le soutien adéquat dans ses prises de décision.
Comité de continuité des services	Le comité de continuité des services se tient, au besoin, lors d'une séance spéciale du comité de direction. Il est composé des membres du comité de direction, du responsable de la continuité des services, du COSI et du COGI. Ce comité peut s'adjoindre toute autre personne en mesure de lui assurer le soutien adéquat dans ses prises de décision.
Comité de crise	Le comité de crise se tient, au besoin, lors d'une séance spéciale du comité de direction. Il est composé des membres du comité de direction, du responsable de la sécurité physique et du responsable de la continuité des services. Ce comité peut s'adjoindre toute autre personne en mesure de lui assurer le soutien adéquat dans ses prises de décision.

Actifs informationnels et détenteurs[2]		
Actif	Description	Détenteur
Dossiers juridictionnels	Les dossiers de mission de la section juridictionnelle	Secrétaire général
Dossiers de recours devant les tribunaux civils		Directeur des affaires juridiques
Dossiers de médiation		Directeur des affaires juridiques
Dossiers administratifs de la Direction des affaires juridiques		Directeur des affaires juridiques
Dossiers du Secrétariat général	Les dossiers de mission du secrétariat général (ex. : rapport quinquennal)	Secrétaire général
Dossiers administratifs du Secrétariat général		Secrétaire général
Dossiers de surveillance	Les dossiers de mission de la section de surveillance	Secrétaire général
Dossiers administratifs de la Direction de la surveillance		Directeur de la surveillance
Dossiers en ressources humaines		Directeur de l'administration
Dossiers en ressources informationnelles		Directeur de l'administration
Dossiers en ressources financières		Directeur de l'administration
Dossiers en ressources matérielles		Directeur de l'administration
Dossiers en communication		Directeur de la surveillance
Fichier de traitement des demandes médiatiques		Directeur de la surveillance
Système de gestion des appels aux préposées (GAP)		Directeur de la surveillance
Fichier des demandes d'accès		Président
Fichier de traitement des plaintes		Président
Dossiers de la Présidence		Président

[2] À revoir lors de la catégorisation des actifs informationnels de la Commission.

Commission
d'accès à l'information
du Québec

DIRECTIVE SUR L'UTILISATION DES TECHNOLOGIES DE L'INFORMATION

Mars 2018

Table des matières

1. OBJECTIFS

La présente directive est adoptée conformément à la politique et au cadre de gestion de la sécurité de l'information de la Commission d'accès à l'information (la Commission) qui sont entrés en vigueur le 23 juin 2016.

Ses objectifs sont :

a) d'établir les règles d'utilisation des outils informatiques à la Commission d'accès à l'information;

b) de préserver la disponibilité, l'intégrité et la confidentialité des actifs informationnels de la Commission et assurer la dimension éthique des communications reliant la Commission aux citoyens et aux organisations publiques et privées;

c) d'assurer le respect de toute législation à l'égard de l'usage et du traitement de l'information et de l'utilisation des technologies de l'information.

Pour plus d'information sur les composantes du cadre normatif de sécurité de l'information, reportez-vous à l'annexe C de la politique de sécurité de l'information de la Commission.

2. CHAMPS D'APPLICATION

La présente directive s'applique à tous les utilisateurs des actifs informationnels et des outils informatiques de la Commission.

3. DÉFINITIONS

Actif informationnel

Une information, quel que soit son canal de communication ou son support (papier, électronique, etc.), un système ou un support d'information, une technologie de l'information, une installation ou un ensemble de ces éléments, acquis ou constitués par une organisation.

Outil informatique

Serveurs, ordinateurs, mini-ordinateurs, micro-ordinateurs, postes de travail informatisés et leurs unités ou accessoires périphériques de lecture, d'emmagasinage, de reproduction, d'impression, de transmission, de réception et de traitement de l'information. Tout équipement de télécommunication dont les téléphones intelligents, les logiciels et le système de courrier électronique placé sur un équipement ou sur un média informatique appartenant à la Commission ou ne lui appartenant pas, mais utilisé dans ses locaux, peu importe leur localisation.

Système d'information

Système constitué des ressources humaines, des ressources matérielles et des procédures permettant d'acquérir, de stocker, de traiter et de diffuser les éléments d'information pertinents pour le fonctionnement d'une entreprise ou d'une organisation.

Utilisateur

Toute personne, physique ou morale, qui est dûment autorisée à accéder aux actifs informationnels de la Commission ou qui les utilise.

Clavardage

Activité permettant à un internaute d'avoir une conversation écrite, interactive et en temps réel avec d'autres internautes par claviers interposés.

Droit d'utilisation

Autorisation accordée à une personne définissant l'usage qu'elle peut faire des actifs informationnels et des outils informatiques.

Internet

Réseau informatique mondial constitué d'un ensemble de réseaux nationaux, régionaux et privés, qui sont reliés par le protocole de communication TCP/IP et qui coopèrent dans le but d'offrir une interface unique à leurs utilisateurs.

Intranet

Réseau informatique utilisé à l'intérieur d'une entreprise ou de toute autre entité organisationnelle qui utilise les mêmes protocoles qu'Internet (TCP/IP, HTTP, SMTP, IMAP, etc.). Parfois, le terme se réfère uniquement au site Web interne de l'organisation, mais c'est souvent une partie bien plus large de l'infrastructure informatique d'une organisation.

4. RÔLES ET RESPONSABILITÉS

Le président	Adopte la présente directive et est responsable de son application. Approuve l'application de mesures de contrôle et de surveillance du contenu et de l'utilisation des actifs et des outils informatiques de la Commission et de sanctions.
Le responsable organisationnel de la sécurité de l'information (ROSI)	Assure la mise en œuvre de la présente directive, assiste le président lors des vérifications de l'utilisation et assure la gestion de l'accès aux actifs informationnels et aux outils informatiques.
Le responsable de la protection des renseignements personnels	Supervise le COSI lors de l'application de mesures de contrôle du contenu et de l'utilisation des actifs informationnels et des outils informatiques de la Commission.

Le responsable de l'éthique	Exerce, au besoin, un rôle-conseil auprès du président dans l'application de mesures de vérification ponctuelle du contenu et de l'utilisation des actifs informationnels et des outils informatiques de la Commission par un utilisateur.
Le coordonnateur organisationnel en sécurité de l'information (COSI)	Informe les utilisateurs de l'existence de la présente directive et en assure la mise à jour. Applique les mesures de contrôle et de surveillance du contenu et de l'utilisation des actifs informationnels et des outils informatiques.
Le gestionnaire	Informe son personnel des dispositions de la directive ainsi que des modalités liées à leur mise en œuvre et les sensibilise à la nécessité de s'y conformer. Informe le ROSI dans les meilleurs délais, lorsqu'il soupçonne une violation des règles de cette directive.
L'utilisateur	Prend connaissance de la présente directive et s'y conforme. Utilise les actifs informationnels et les outils informatiques mis à sa disposition en se limitant aux fins auxquelles leur utilisation a été autorisée. Évite tout comportement allant à l'encontre des règles de la présente directive. Remet, lorsqu'il quitte la Commission, les différents actifs informationnels et les outils informatiques mis à sa disposition par la Commission.

5. ÉNONCÉS GÉNÉRAUX

a) L'utilisation des actifs informationnels et des outils informatiques de la Commission est un privilège et non un droit. Il peut être révoqué en tout temps à tous les utilisateurs qui ne se conforment pas à la présente directive;

b) Toute information stockée ou consignée sur les outils informatiques de la Commission au moyen d'un courriel, d'un collecticiel, des services d'internet ou par tout autre moyen est réputée constituer une information à laquelle la Commission peut accéder;

c) La Commission se réserve le droit, sur demande du président, de contrôler le contenu et l'utilisation de ses actifs informationnels et de ses outils informatiques lorsqu'elle a des motifs sérieux de croire qu'un utilisateur n'agit pas conformément aux règles de la présente directive;

d) L'utilisation des outils informatiques de la Commission rend possible son identification ou l'identification du gouvernement du Québec par un interlocuteur externe. L'utilisateur doit en tenir compte;

e) L'utilisateur signale immédiatement à son gestionnaire tout acte dont il a connaissance, qui est susceptible de constituer une violation réelle ou présumée des règles.

6. CONDITIONS D'UTILISATION GÉNÉRALES

a) L'utilisation des actifs informationnels et des outils informatiques de la Commission à des fins illicites, illégales, lucratives, commerciales, de publicité, de propagande, de harcèlement, de diffusion de propos diffamatoires, haineux, offensants, perturbants, dénigrants ou de contenu sexuellement explicite ou obscène ou incompatible avec la mission ou l'image de la Commission est strictement interdite;

b) L'utilisateur doit prendre les moyens disponibles pour voir à la sécurité de l'information et la protection des renseignements auxquels il a accès conformément aux lois, à la réglementation et aux directives en vigueur[1] lors de l'utilisation des actifs informationnels et des outils informatiques de la Commission;

c) L'utilisateur a l'obligation de respecter les mesures de sécurité, notamment et non limitativement les filtres Internet et les coupe-feux, mis en place à la Commission;

d) L'utilisateur a l'obligation de s'identifier clairement lors de toute utilisation des actifs informationnels et des outils informatiques de la Commission en utilisant le code d'accès qui lui a été alloué;

e) L'utilisateur ne doit pas donner son code d'accès ni ses mots de passe et est responsable de toute forme de communication qui pourrait être effectuée avec ceux-ci dans le cas contraire;

f) Les actifs informationnels et les outils informatiques de la Commission sont mis à la disposition des utilisateurs pour la réalisation de leurs fonctions professionnelles et demeurent la propriété de la Commission. Un usage à des fins personnelles est admis dans la mesure où il ne réduit pas la sécurité des actifs informationnels, la productivité de l'utilisateur et ne nuit pas aux intérêts ou à l'image de la Commission;

g) Le stockage de documents (photos, vidéos, courriels, etc.) personnels est permis. Toutefois, il ne doit pas avoir pour effet de limiter l'accès, d'interrompre le fonctionnement ou de diminuer le rendement des actifs informationnels et des outils informatiques de la Commission;

[1] Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ., c. A-2.1);
Loi concernant le cadre juridique des technologies et l'information (RLRQ, c. C-1.1);
Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, chapitre G-1.03);
Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;
Politique et cadre de gestion de la sécurité de l'information de la Commission d'accès à l'information;
Directive sur la sécurité de l'information gouvernementale.

h) L'utilisateur ne peut utiliser les actifs informationnels et les outils informatiques de la Commission pour expédier des messages destinés à tous les utilisateurs sur des sujets qui ne sont pas d'ordre professionnel;

i) Chaque consultation que l'utilisateur fait sur Internet et chaque message électronique qu'il transmet identifie et associe la Commission et le gouvernement du Québec à cette consultation ou cette transmission. Ainsi, l'utilisateur doit protéger l'image et la réputation de la Commission et du gouvernement. Ses communications doivent être empreintes de courtoisie, de respect et de civisme et être faites dans un langage adéquat.

7. CONDITIONS D'UTILISATION SPÉCIFIQUES

7.1. POSTE DE TRAVAIL

a) L'utilisateur doit verrouiller son poste de travail à chaque fois qu'il s'absente de son bureau;

b) L'utilisateur doit déconnecter son poste de travail à la fin de chaque journée de travail et le redémarrer au moins une fois par semaine afin que les mises à jour de sécurité puissent être appliquées correctement;

c) L'utilisateur ne doit pas télécharger, partager ou copier des logiciels, des fichiers entraînant l'installation d'un programme (.exe, .bat, .com, etc.), des outils ayant pour tâche d'analyser, de traduire et d'exécuter les programmes (.js, .vbs, etc.) ou des fichiers non reliés aux applications bureautiques autorisées, des économiseurs d'écran, des jeux ou des images (à l'exception des photos personnelles);

d) L'installation de logiciels autres que ceux installés par la Commission sans le consentement du ROSI est interdite. L'installation ou l'utilisation de logiciels sans licence ou sur un nombre de postes plus élevés que le nombre de licences détenues par la Commission d'accès à l'Information est également interdite. La reproduction de logiciels n'est autorisée qu'à des fins de copies de sauvegarde, et ce, en conformité avec les normes de la licence d'utilisation les régissant;

e) Il est interdit d'installer et d'utiliser un logiciel acquis pour un usage externe à la Commission sans que la licence ou le droit de propriété n'ait été transféré au nom de la Commission.

7.2. APPAREIL MOBILE (TÉLÉPHONES INTELLIGENTS ET ORDINATEURS PORTABLES)

a) Tout appareil mobile doit être protégé par un mot de passe et un mécanisme de chiffrement;

b) L'utilisateur doit verrouiller son appareil mobile dès qu'il cesse de l'utiliser et ne pas le laisser sans surveillance;

c) L'utilisateur ne doit pas prêter son appareil à qui que ce soit;

d) L'utilisateur doit prendre les précautions nécessaires pour se prémunir du vol de son appareil mobile, par exemple, il ne doit pas laisser l'appareil mobile dans la voiture;

e) Le partage de connexion à partir d'un appareil appartenant à la Commission vers un autre appareil est interdit;

f) À partir des rapports de consommation mensuelle de téléphonie mobile transmis à son gestionnaire par la direction de l'administration, l'utilisateur rembourse à la Commission tout frais découlant de l'utilisation de services non-inclus dans le forfait standard et lié à une utilisation à des fins personnelles.

7.3. SERVICES INTERNET

a) L'accès et la consultation de sites Internet qui véhiculent des messages obscènes, haineux, racistes, diffamatoires, harcelants ou violents ainsi qu'à des sites contenant du matériel érotique ou pornographique sont interdits. Il en va de même pour tout envoi et toute réception de courriels (autres que ceux non sollicités) qui auraient une semblable connotation;

b) La participation à des activités de piratage (musique, jeux, logiciels, etc.), des jeux de hasard, des paris, des concours ou des groupes de discussion ou de clavardage, sauf si ces groupes portent sur des sujets d'ordre professionnel et que la participation est autorisée par le gestionnaire, est interdite;

c) L'utilisation de logiciels ou de services de partage de fichiers (Torrent, Kaza, Usenet, Dropbox, etc.) est interdite;

d) L'utilisation de services Internet doit se faire, en priorité, par câble. À défaut d'avoir accès à un réseau par câble, l'utilisation de réseaux sans-fil sécurisés (accessibles avec mot de passe) est possible. Toutefois, l'utilisateur doit redoubler de vigilance. L'utilisation de réseaux sans-fil non-sécurisés (accessibles sans mot de passe) est à proscrire;

e) La Commission se réserve le droit de mettre en place des mécanismes de filtrage afin de limiter l'accès aux sites Internet dont le contenu est incompatible avec la mission de la Commission ou avec les règles de la présente directive;

f) L'écoute d'émissions de radio ou de télévision de même que l'écoute de musique diffusées numériquement sur Internet (streaming) pendant les heures de travail est interdite, sauf pour les cas reliés à l'exercice des fonctions de l'utilisateur et que l'écoute est autorisée par le gestionnaire;

L'écoute de telles émissions sur les téléphones intelligents de la Commission est interdite en tout temps sauf pour les cas reliés à l'exercice des fonctions de l'utilisateur et que l'écoute est autorisée par le gestionnaire.

7.4. MESSAGERIE ÉLECTRONIQUE ET COURRIEL

a) L'utilisateur doit faire preuve de vigilance lors de l'ouverture d'un courriel dont il ignore la provenance, dont l'expéditeur est inconnu ou dont il doute de l'authenticité. Il s'assure de

communiquer avec le COSI avant de cliquer sur un lien Internet ou sur une pièce jointe inséré dans ledit courriel;

b) L'utilisateur doit s'identifier dans ses communications professionnelles en indiquant son nom et ses coordonnées selon la façon ci-dessous (Police :Arial , 10 points, prénom et nom en gras) :

Prénom Nom, (titre professionnel s'il y a lieu)
Votre fonction

Votre unité administrative
Commission d'accès à l'information
Bureau 2.36
525, boulevard René-Lévesque Est
Québec (Québec) G1R 5S9
Téléphone: 418 numéro
Télécopieur: 418 numéro
adresse courriel@cai.gouv.qc.ca
www.cai.gouv.qc.ca

Prénom Nom, (titre professionnel s'il y a lieu)
Votre fonction

Votre unité administrative
Commission d'accès à l'information
Bureau 18.200
500, boulevard René-Lévesque Ouest
Montréal (Québec) H2Z 1W7
Téléphone: 514 numéro
Télécopieur: 514 numéro
adresse courriel@cai.gouv.qc.ca
www.cai.gouv.qc.ca

En sus de ces standards, la Commission peut au besoin demander à l'utilisateur d'ajouter d'autres éléments pour des besoins ponctuels.

8. CONTRÔLE DU CONTENU ET DE L'UTILISATION

Une vérification de la capacité de stockage globale est effectuée de façon continue sur le réseau. Lorsque l'espace utilisé est de 80 % ou plus, la Commission se réserve le droit d'effectuer une vérification ponctuelle de l'espace de stockage réseau utilisé par chaque utilisateur. La Commission se réserve également le droit de demander aux utilisateurs prenant le plus d'espace de procéder à une opération de gestion des fichiers jusqu'à ce que l'espace utilisé soit inférieur à 80 %.

Sous la supervision de responsable de la protection des renseignements personnels, une vérification ponctuelle du contenu et de l'utilisation des actifs informationnels et des outils informatiques de la Commission par un utilisateur peut être effectuée, sans le consentement de ce dernier, sur autorisation du président, lorsque celui-ci a des motifs sérieux de croire que l'utilisateur n'agit pas conformément aux règles de la présente directive. Le président détermine la fréquence des vérifications et la période d'application allant jusqu'au maintien d'une surveillance constante.

Le COSI est chargé d'appliquer les mesures de contrôle, sous la supervision du responsable de la protection des renseignements personnels, et fait rapport au ROSI et au président.

9. SANCTIONS

L'utilisateur qui contrevient à la présente directive s'expose à des mesures disciplinaires, administratives ou légales, en fonction de la gravité de son geste. Ces mesures peuvent inclure la suspension ou le retrait des privilèges, la réprimande, la suspension, le congédiement ou toute

autre mesure nécessaire, et ce, conformément aux dispositions des conventions collectives, des ententes ou des contrats.

La Commission peut transmettre à toute autorité compétente les renseignements colligés et qui lui portent à croire qu'une infraction à toute loi ou règlement en vigueur a été commise sous réserve des dispositions de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

10. DISPOSITIONS FINALES

a) La présente directive entre en vigueur à la date de son approbation par le président;

b) La présente directive remplace les *Règles d'éthique dans l'utilisation de l'informatique* (juin 2009) et la *Politique d'utilisation de l'inforoute et de la messagerie électronique* (avril 2003) de la Commission;

c) Le ROSI est chargé de la mise en œuvre des dispositions de la présente directive;

d) La présente directive doit être révisée à l'occasion de changements qui pourraient l'affecter.

	4 décembre 2018
Jean Chartier, président	**Date**

Commission
d'accès à l'information
du Québec

POLITIQUE DE SÉCURITÉ DE L'INFORMATION

Juin 2016

Table des matières

1 PRÉAMBULE

Le 15 janvier 2014 entrait en vigueur la nouvelle *Directive sur la sécurité de l'information gouvernementale* du Conseil du trésor. Cette directive fixe les objectifs à atteindre, énonce les principes directeurs devant être appliqués et établit les obligations des organismes publics pour assurer la sécurité de l'information gouvernementale. Elle est appuyée par un cadre gouvernemental de gestion de la sécurité de l'information, un cadre de gestion des risques et des incidents à portée gouvernementale et une approche stratégique triennale 2014-2017 de sécurité de l'information.

C'est en application de l'article 7 de cette directive que la Commission d'accès à l'information (la Commission) se dote de la présente politique de sécurité de l'information. Cette politique est complétée par un cadre de gestion de la sécurité de l'information. Les obligations qui en découlent sont précisées dans des directives, des guides ou encore des procédures. Ces documents sont disponibles sur le site intranet de la Commission.

Pour plus d'information sur la hiérarchie des principales composantes du cadre normatif de sécurité de l'information, reportez-vous à l'Annexe B – Cadre normatif de sécurité de l'information.

2 CADRE LÉGAL ET ADMINISTRATIF

La politique de sécurité de l'information est assujettie, entres autres, aux cadres légaux et administratifs suivants :

- la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, chapitre A-2.1);
- le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* (RLRQ, chapitre A-2.1, r. 02);
- la *Loi concernant le cadre juridique des technologies et l'information* (RLRQ, chapitre C-1.1);
- la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, chapitre G-1.03);
- la *Loi sur l'administration publique* (RLRQ, chapitre A-6.01);
- la *Loi sur la fonction publique* (RLRQ, chapitre F-3.1.1);
- la *Loi sur les archives* (RLRQ, chapitre A-21.1);
- le *Code civil du Québec*;
- le *Code criminel* (LRC, 1985, chapitre C-46);
- la *Loi sur le droit d'auteur* (LRC, 1985, chapitre C-42);
- la *Charte des droits et libertés de la personne* (RLRQ, chapitre C-12);
- la *Loi canadienne sur les droits de la personne* (LRC, 1985, chapitre H-6);
- la *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics*;
- la *Directive sur la sécurité de l'information gouvernementale*.

3 DÉFINITIONS

Actif informationnel[1]	Une information, quels que soient son canal de communication ou son support (papier, support électronique, etc.), un système ou un support d'information, une technologie de l'information, une installation ou un ensemble de ces éléments, acquis ou constitués par une organisation.
Confidentialité	Propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées.
Cycle de vie de l'information[2]	L'ensemble des étapes que franchit une information et qui vont de sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation de la Commission.
Disponibilité	Propriété d'une information d'être accessible en temps voulu et de la manière requise pour une personne autorisée.
Intégrité	Propriété associée à une information de ne subir aucune altération ou destruction sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité.
Renseignement personnel	Les renseignements personnels sont ceux qui portent sur une personne physique et permettent de l'identifier. Ils sont confidentiels. Sauf exception, ils ne peuvent être communiqués sans le consentement de la personne concernée.
Utilisateur	Toute personne, physique ou morale, qui est dûment autorisée à accéder aux actifs informationnels de la Commission ou qui les utilise.

[1] Inspirée de la définition de l'OQLF – Grand dictionnaire terminologique. La politique utilise le terme « actif informationnel » au sens d'un « élément d'actif informationnel ».

[2] Directive sur la sécurité de l'information gouvernementale, Conseil du trésor, 23 janvier 2014.

4 OBJECTIF DE LA POLITIQUE

La politique de sécurité de l'information (la politique) vise à affirmer l'engagement de la Commission à s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information, quel que soit le support ou le moyen de communication utilisé. Plus précisément, il s'agit d'assurer, tout au long du cycle de vie de l'information, sa disponibilité, son intégrité et sa confidentialité.

5 CHAMP D'APPLICATION

La politique s'adresse à tous les utilisateurs des actifs informationnels de la Commission.

La politique s'applique à l'information que la Commission détient, peu importe le support sur lequel elle est recueillie, conservée, utilisée ou communiquée, que sa conservation soit assurée par elle-même ou par un tiers.

6 ÉNONCÉS DE PRINCIPES DIRECTEURS

La politique s'appuie sur les principes directeurs suivants en matière de sécurité de l'information.

6.1 PROTECTION DE L'INFORMATION

a) Les actifs informationnels de la Commission sont essentiels et doivent être protégés afin de lui permettre d'exercer ses activités, de réaliser sa mission et de respecter ses obligations légales. Le niveau de protection dont les actifs informationnels doivent faire l'objet est établi en fonction de leur importance pour les activités de la Commission, de leur confidentialité et des risques d'accident, d'erreur et de malveillance auxquels ils sont exposés. Les risques en matière de sécurité de l'information doivent faire l'objet d'une évaluation constante afin que les actifs informationnels bénéficient d'une protection adéquate;
b) Toute information de nature personnelle ou autrement confidentielle doit être préservée de tout accès, toute divulgation ou de toute utilisation non autorisée;
c) la Commission adhère aux orientations et objectifs stratégiques gouvernementaux en matière de sécurité de l'information et veille à ce que les pratiques et les solutions retenues en la matière correspondent, dans la mesure du possible, à des façons de faire reconnues et généralement utilisées, tant à l'échelle nationale qu'à l'échelle internationale;
d) La protection des actifs informationnels de la Commission repose sur la responsabilisation et l'implication de tous les utilisateurs, les gestionnaires et les détenteurs d'informations.

6.2 SENSIBILISATION ET FORMATION

La Commission s'engage, sur une base régulière, à sensibiliser et à former les utilisateurs à la sécurité des actifs informationnels, aux conséquences d'une atteinte à leur sécurité ainsi qu'à leur rôle et leurs obligations en la matière.

6.3 DROIT DE REGARD

Le Commission exerce un droit de regard sur tout usage de ses actifs informationnels. Les moyens de contrôle et de surveillance mis en place sont déterminés et utilisés dans le respect des lois et règlements en vigueur. Soucieuse du droit à la vie privée des utilisateurs, la Commission se garde d'utiliser des moyens de contrôle ou de surveillance excessifs et les circonstances pour lesquelles ce droit de regard peut être exercé sont définies et diffusées auprès des utilisateurs.

7 RÔLES ET RESPONSABILITÉS

La politique résume les rôles et responsabilités des intervenants clés en matière de sécurité de l'information. Une description détaillée de ces rôles et responsabilités, les rôles et les responsabilités attribués à d'autres intervenants ainsi que les structures internes de coordination et de concertation sont définis dans le cadre de gestion de la sécurité de l'information.

Le président	Premier responsable de la sécurité de l'information détenue par la Commission.
Le responsable organisationnel de la sécurité de l'information	Assiste le président dans la détermination des orientations stratégiques et des priorités d'intervention.
Les détenteurs de l'information	Les détenteurs sont des gestionnaires qui assurent la sécurité de l'information des actifs informationnels impliqués dans les processus relevant de leur unité administrative.
Les gestionnaires	Chargés de la mise en œuvre des dispositions de la présente politique auprès du personnel relevant de leur autorité.
Les utilisateurs	Contribuent à la protection des actifs informationnels de la Commission en se conformant aux directives gouvernementales, à la présente politique et aux règles qui leur sont applicables, en signant la déclaration jointe en annexe.

8 NON-RESPECT DE LA POLITIQUE ET DES DIRECTIVES

Lorsqu'un utilisateur contrevient à la présente politique ou aux directives en découlant, il s'expose à des mesures disciplinaires, administratives ou légales, en fonction de la gravité de son geste. Ces mesures peuvent inclure la suspension des privilèges, la réprimande, la suspension, le congédiement ou autre, et ce, conformément aux dispositions des conventions collectives, des ententes ou des contrats.

La Commission peut transmettre à toute autorité judiciaire les renseignements colligés et qui lui portent à croire qu'une infraction à toute loi ou règlement en vigueur a été commise.

9 DISPOSITIONS FINALES

a) la présente politique entre en vigueur à la date de son approbation par le président;
b) la présente politique remplace *la Politique de sécurité des actifs informationnels* (avril 2003) de la Commission;
c) le responsable organisationnel de la sécurité de l'information est chargé de la mise en œuvre des dispositions de la présente politique et de ses directives d'application;
d) la présente politique doit être révisée à l'occasion de changements qui pourraient l'affecter;
e) Les obligations qui en découlent sont précisées dans des directives, des guides ou encore des procédures.

23 juin 2016

Jean Chartier, président **Date**

ANNEXE A – OBLIGATIONS DES UTILISATEURS QUANT AU RESPECT DES RÈGLES DE SÉCURITÉ DE L'INFORMATION

Les utilisateurs jouent un rôle important dans la protection des actifs informationnels de la Commission.

À cette fin, les utilisateurs doivent :

a) prendre connaissance de la politique de sécurité de l'information de la Commission, des directives, des procédures et autres lignes de conduite qui seront prises par la suite par la Commission et s'y conformer;
b) utiliser les actifs informationnels mis à leur disposition en se limitant aux fins auxquelles ils ont été autorisés;
c) éviter tout comportement pouvant porter atteinte aux diverses mesures de sécurité mises en place par la Commission pour assurer la sécurité des actifs informationnels telle la sécurité des lieux ou des équipements physiques et électroniques;
d) signaler immédiatement à son supérieur tout acte dont il a connaissance, susceptible de constituer une violation réelle ou présumée des règles de sécurité ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels de la Commission;
e) remettre, lorsqu'ils quittent la Commission, les différents actifs informationnels mis à leur disposition par la Commission tels que les cartes d'identité et d'accès aux locaux, les équipements électroniques et de téléphonie.

Je soussigné(e), _____,
reconnais avoir lu et compris les obligations reproduites ci-dessus.

Signature : _____ Date : _____

ANNEXE B – CADRE NORMATIF DE SÉCURITÉ DE L'INFORMATION

Le schéma présenté ci-dessous illustre la hiérarchie des principales composantes[3] du cadre normatif de sécurité de l'information. Ces composantes se traduisent notamment :

- au niveau stratégique, par la politique de sécurité de l'information;
- au niveau tactique, par le cadre de gestion, les directives et les guides;
- au niveau opérationnel, par des procédures décrivant les étapes d'un processus d'implantation ou de mise en œuvre d'une mesure de sécurité.

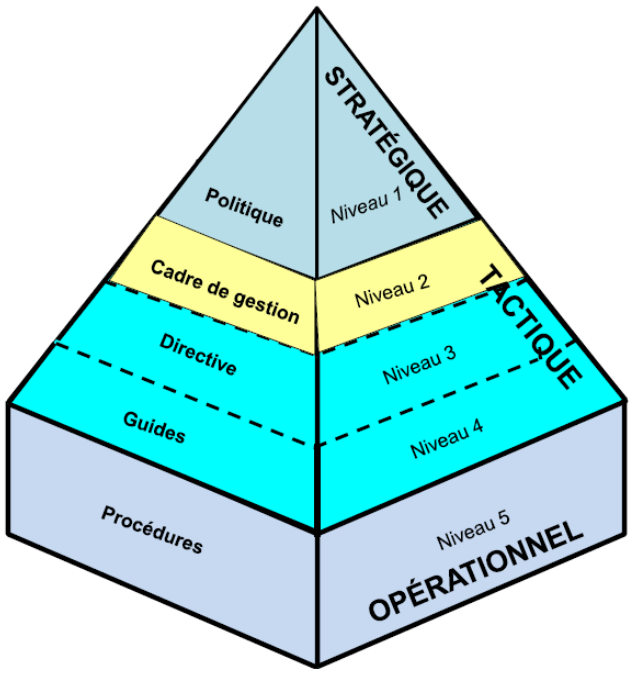

Figure 1 - Structure du cadre normatif de sécurité de l'information

[3] Schéma tiré du *Guide d'élaboration d'un cadre de gestion de la sécurité de l'information (PR-75)* du Conseil du trésor. Ce guide prend lui-même appui sur les normes internationales de sécurité de l'information, particulièrement les normes ISO/CEI 27000.

Niveau 1 : Politique de sécurité de l'information	La politique de sécurité de l'information témoigne de l'importance accordée par la Commission à la protection de l'information. Elle énonce des principes généraux et fixe des responsabilités à l'endroit de certains intervenants clés, notamment, à l'égard du président, du responsable organisationnel de la sécurité de l'information (ROSI), des détenteurs de l'information, des gestionnaires et des utilisateurs.
Niveau 2 : Cadre de gestion de la sécurité de l'information	Le cadre de gestion de la sécurité de l'information vise à compléter les dispositions de la politique. À cet effet, il précise l'organisation fonctionnelle en matière de sécurité de l'information et décrit les responsabilités de divers intervenants ainsi que les rôles des comités en sécurité de l'information.
Niveau 3 : Directives	D'application obligatoire, une directive vise à préciser, pour un domaine d'application particulier de sécurité de l'information, les dispositions à respecter aux fins d'assurer la sécurité de l'information (ex. : directive sur l'utilisation du courriel, d'un collecticiel ou d'Internet).
Niveau 4 : Guides	Les guides visent à faciliter l'application des prescriptions d'une politique, d'une directive ou éventuellement d'une norme, sans en avoir un caractère contraignant.
Niveau 5 : Procédures	Une procédure est un ensemble d'étapes à franchir, de moyens à prendre et de méthodes à suivre dans l'exécution d'une tâche. Elle décrit en détail les étapes d'un processus humain ou technologique d'implantation ou d'application d'une mesure de sécurité, qu'elle soit administrative ou technologique.

ANNEXE C – COMPOSANTES DU CADRE NORMATIF DE SÉCURITÉ DE L'INFORMATION DE LA COMMISSION

Document	**Adopté le**
Politique de sécurité de l'information	23 juin 2016
Cadre de gestion de la sécurité de l'information	23 juin 2016
Directive sur l'utilisation du courriel, d'un collecticiel ou d'Internet	

Commission
d'accès à l'information
du Québec

Processus de gestion des incidents en sécurité de l'information

Février 2019

Table des matières

1. PRÉAMBULE

Le 15 janvier 2014 entrait en vigueur la nouvelle *Directive sur la sécurité de l'information gouvernementale* du Secrétariat du Conseil du trésor. Cette directive fixe les objectifs à atteindre, énonce les principes directeurs devant être appliqués et établit les obligations des organismes publics pour assurer la sécurité de l'information gouvernementale. Elle est appuyée par un cadre gouvernemental de gestion de la sécurité de l'information, un cadre de gestion des risques et des incidents à portée gouvernementale et une approche stratégique triennale 2014-2017 de sécurité de l'information.

C'est en application de l'article 7 de cette directive que la Commission d'accès à l'information (la Commission) se dote du présent processus de gestion des incidents en sécurité de l'information.

2. OBJECTIFS

Les objectifs du processus de gestion des incidents sont :

a) d'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;
b) d'assurer l'intégrité de l'information, de manière qu'elle ne soit pas détruite ou altérée de quelque façon sans autorisation, et que le support de cette information lui procure la stabilité et la pérennité voulues;
c) de limiter la divulgation de l'information aux seules personnes autorisées à en prendre connaissance, assurant ainsi une stricte confidentialité;
d) de permettre de confirmer l'identité d'une personne ou l'identification d'un document ou d'un dispositif;
e) de se prémunir contre le refus par une personne de reconnaître sa responsabilité à l'égard d'un document ou d'un autre objet, dont un dispositif d'identification avec lequel elle est en lien;
f) de renforcer les mécanismes d'atténuation des risques et, advenant un incident, de s'assurer que les actions appropriées sont menées.

3. CHAMPS D'APPLICATION

Le présent processus s'applique à tous les utilisateurs des actifs informationnels et des outils informatiques de la Commission.

4. DÉFINITIONS

Actif informationnel

Une information, quel que soit son canal de communication ou son support (papier, électronique, etc.), un système ou un support d'information, une technologie de l'information, une installation ou un ensemble de ces éléments, acquis ou constitués par une organisation.

Outil informatique

Serveurs, ordinateurs, mini-ordinateurs, micro-ordinateurs, postes de travail informatisés et leurs unités ou accessoires périphériques de lecture, d'emmagasinage, de reproduction, d'impression, de transmission, de réception et de traitement de l'information. Tout équipement de télécommunication dont les téléphones intelligents, les logiciels et le système de courrier électronique placé sur un équipement ou sur un média

informatique appartenant à la Commission ou ne lui appartenant pas, mais utilisé dans ses locaux, peu importe leur localisation.

Incident en sécurité de l'information

Un événement pour lequel il y a un risque d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information gouvernementale. Un incident n'est pas obligatoirement lié à l'utilisation des technologies de l'information. Par exemple, il peut s'agir :

a) du vol ou la perte d'une carte d'accès, de matériel informatique ou de documents papier;
b) d'un accès non autorisé aux locaux de la Commission, aux salles informatiques ou aux voûtes;
c) d'une utilisation non autorisée, d'une altération ou de la destruction de documents papier, d'équipements informatiques, de données, de logiciels ou d'applications;
d) du piratage (ou d'une tentative), d'une fraude informatique, d'une intrusion dans un système informatique, de l'infection d'un poste de travail par un virus ou d'autres codes malicieux, d'un vol d'identité;
e) de la divulgation non autorisée de renseignements personnels;
f) de toute violation à la Politique de sécurité de l'information ou à la Directive sur l'utilisation des technologies de l'information de la Commission.

5. RÔLES ET RESPONSABILITÉS

Le président	Adopte le présent processus et est responsable de son application. Approuve la mise en œuvre des stratégies permettant d'assurer la prise en charge des incidents. Il approuve également les communications avec les médias.
Le coordonnateur organisationnel de gestion des incidents (COGI)	Contribue à la mise en place du processus sectoriel de gestion des incidents de sécurité de l'information et du processus gouvernemental de gestion des incidents. Applique les stratégies de prise en charge des incidents. Tiens à jour le registre des incidents. Contribue à l'analyse des risques, détermine les menaces et les situations de vulnérabilité et met en œuvre les solutions appropriées.
Le responsable organisationnel de la sécurité de l'information (ROSI)	Assure la mise en œuvre du présent processus. Coordonne la mise en œuvre des stratégies de prise en charge des incidents.
Le responsable de la protection des renseignements personnels	Supervise les intervenants lors de l'application des stratégies de prise en charge des incidents afin de s'assurer que la protection des renseignements personnels est correctement prise en compte au moment de la mise en œuvre du processus de gestion des incidents. Participe au processus de traitement d'un incident associé aux renseignements personnels;
Le responsable de la sécurité physique	Participe au processus de traitement d'un incident associé à un problème d'accès physique aux biens de

	l'organisation. Veille à la mise en place des moyens de sécurité des accès aux locaux abritant notamment des actifs informationnels. Veille à la mise en œuvre de mesures de protection physique des biens contre les sinistres, les pertes, l'endommagement, le vol ainsi que l'interruption des activités de son organisation; élabore les documents normatifs propres à son domaine d'intervention.
Le gestionnaire	Informe son personnel des dispositions du présent processus et le sensibilise à la nécessité de s'y conformer.
L'utilisateur	Prend connaissance du présent processus et s'y conforme. Informe son gestionnaire et le COGI de tout incident de sécurité de l'information dont il est responsable ou dont il a connaissance dès sa constatation.

6. PROCESSUS DE GESTION

a) L'utilisateur rapporte tout incident de sécurité de l'information à son gestionnaire dès sa constatation;
b) L'utilisateur rapporte ensuite tout incident de sécurité de l'information au COGI de la Commission en complétant les sections A, B et C du formulaire en annexe. Il transmet le formulaire par courriel à l'adresse informatique@cai.gouv.qc.ca;
c) Sur réception du formulaire, le COGI procède à une première analyse de l'incident;
d) Le COGI informe le ROSI de l'incident et des résultats de son analyse;
e) Le COGI déclare l'incident au CERT/AQ après avoir inscrit le numéro de l'incident et complété la section D1 du formulaire transmis par l'utilisateur;
f) Le ROSI informe le président de l'incident lorsque, selon le tableau ci-dessous, le niveau de gravité de celui-ci est important ou critique.

Niveau de gravité	Caractéristiques	Exemples
Négligeable	Événement pouvant avoir des conséquences plutôt négligeables, limitées à un secteur administratif de l'organisation.	Vol ou perte d'une carte d'accès.
Mineur	Événement pouvant avoir des conséquences notables, limitée à un secteur administratif de l'organisation.	Utilisation non autorisée, altération ou destruction d'équipements informatiques, de données, de logiciels ou d'applications.
Important	Événement pouvant avoir des conséquences notables pour l'organisation ou la clientèle, ne menaçant pas l'intégrité de l'organisation dans son ensemble ni la vie ou la santé des personnes.	Vol ou perte de documents ou de matériel informatique ne contenant pas de renseignements personnels. Virus informatique.
Critique	Événement menaçant la vie, la santé des personnes, l'intégrité de l'organisation dans son ensemble ou pouvant avoir des conséquences	Vol, perte ou divulgation renseignements qui pourraient être utilisés pour

	graves pour la clientèle ou d'autres organisations.	obtenir frauduleusement des services (vol d'identité) auprès d'un autre organisme public.

g) Le COGI applique les stratégies de prise en charge des incidents et, le cas échéant, les recommandations du CERT\AQ. À défaut de pouvoir le faire, il en informe le ROSI qui demande l'assistance de ressources externes;
h) Dans les cas où le président a été informé d'un incident, le ROSI le tient informé de l'évolution et des résultats de l'application des stratégies de prise en charge des incidents;
i) Le président, en collaboration avec le responsable des communications, coordonne les communications avec les médias et le ministre responsable le cas échéant.

7. DISPOSITIONS FINALES

a) Le présent processus entre en vigueur à la date de son approbation par le président;

b) Le ROSI est chargé de la mise en œuvre des dispositions du présent processus;

c) Le présent processus doit être révisé à l'occasion de changements qui pourraient l'affecter.

13 mars 2019

Diane Poitras, vice-présidente **Date**

(CONFIDENTIEL)

Incident numéro :
(jj-mm-aaaa) (Numéro séquentiel)

A – RENSEIGNEMENTS SUR L'IDENTITÉ DU DÉCLARANT

Nom :	**Prénom :**
Unité administrative :	**Qualité du déclarant :** ☐ Utilisateur ☐ Personnel en TI
Déclaré auprès de : ☐ Gestionnaire ☐ COGI	

B – DÉTAILS DE L'INCIDENT

Début de l'incident (jj-mm-aaaa hh :mm)	**Début de la prise en charge** (jj-mm-aaaa hh :mm)	**Localisation** (adresse complète)

Type d'incident

- ☐ Vol ou sabotage
- ☐ Intrusion logique (accès ou tentative d'accès non autorisée)
- ☐ Divulgation de renseignements personnels ou confidentiels
- ☐ Déni de service :
- ☐ Piratage, virus ou canular
- ☐ Perte de carte d'accès, de matériel informatique ou de documents papier
- ☐ Intrusion physique
- ☐ Altération ou destruction de documents, de données ou d'équipements

Description de l'incident :

C – CONSÉQUENCES DE L'INCIDENT

Dommages constatés :

Objet visé (Système d'information, données numériques ou non, autres) :

D – DÉTAILS DE L'INTERVENTION ET DEMANDE D'ASSISTANCE	
D-1. Partie réservée au personnel en RI	**Détails de l'intervention :** **Nous demandons l'assistance du CERT/AQ** ☐ OUI ☐ NON **Situation urgente** ☐ OUI ☐ NON **Nous recommandons de faire appel au dirigeant de l'organisme** ☐ OUI ☐ NON
D-2. Partie réservée au CERT/AQ	**Détails de l'intervention :** **Nous recommandons de faire appel au comité de crise** ☐ OUI ☐ NON Situation urgente ☐ OUI ☐ NON
D-3. Partie réservée au dirigeant de l'organisme	**Détails de l'intervention :**