CADRE DE GESTION DE LA SÉCURITÉ DE L'INFORMATION

UNITÉ ADMINISTRATIVE RESPONSABLE :
Vice-présidence technologies, du numérique et des opérations

TABLE DES MATIÈRES

HISTORIQUE DES VERSIONS

Adoption

Instance	Date	Numéro de résolution
Conseil d'administration	2013-11-22	1995

Dernières modifications

Instance	Date	Numéro de résolution	Commentaire
Conseil d'administration	2018-11-30	2178	Révision afin de tenir compte de nouvelles indications gouvernementales
Conseil d'administration	2024-04-05	2354	Révision afin de tenir compte de nouvelles indications gouvernementales et d'assurer une cohérence avec les récentes *Politique de gestion de l'information* et *Politique-cadre sur la protection des renseignements personnels* de la Société

CONTEXTE

Conformément à la réglementation en vigueur, le présent cadre se veut complémentaire à la Politique de sécurité de l'information en définissant la structure de gestion et les rôles et responsabilités des intervenants en matière de protection et de sécurité de l'information au sein de la Société de télédiffusion du Québec (ci-après la « **Société** »).

1. CHAMP D'APPLICATION

Le présent cadre de gestion s'adresse aux utilisateurs des Actifs informationnels, c'est-à-dire à tout le personnel peu importe son statut, à toute personne physique ou morale qui, à titre d'employé, de consultant, de partenaire ou de fournisseur, utilise les Actifs informationnels de Télé-Québec ou y a accès ainsi qu'à toute personne dûment autorisée à y avoir accès.

2. DÉFINITIONS

À moins que le contexte n'indique un sens différent, les définitions prévues à la Politique de sécurité de l'information s'appliquent également au présent cadre de gestion.

3. CADRE LÉGAL ET NORMATIF

La présente politique est fondée sur les lois suivantes et les règlements qui en découlent :

- Loi sur la Société de télédiffusion du Québec, (RLRQ, c. S-12.01) ;
- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, (RLRQ, c. G-1.03) (ci-après « **LGGRI** ») ;
- Loi concernant le cadre juridique des technologies et l'information, (RLRQ, c. C-1.1) ;
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, (RLRQ c. A-2.1) ;

Au-delà des lois, la sécurité de l'information de la Société est soumise aux politiques de l'organisme et aux documents normatifs pertinents en découlant, notamment ceux-ci :

- Politique de sécurité de l'information
- Politique-cadre sur la protection des renseignements personnels
- Politique de gestion de l'information
- Code d'éthique et de déontologie des administrateurs et des dirigeants de la Société de télédiffusion du Québec;
- Règles d'éthique et code de conduite du personnel de la Société de télédiffusion du Québec;

4. RÔLES ET RESPONSABILITÉS DES PRINCIPALES PARTIES PRENANTES

Les principaux rôles et les principales responsabilités en matière de sécurité de l'information sont dévolus aux parties prenantes suivantes.

4.1 Le conseil d'administration

Le conseil d'administration approuve la politique sur la sécurité de l'information et le présent cadre de gestion de la sécurité de l'information.

4.2 Le comité d'audit

Le présent cadre de gestion et la politique de sécurité de l'information sont soumis au comité d'audit qui peut ultimement recommander leur adoption au conseil d'administration.

4.3 La présidence-direction générale

En tant que dirigeant d'organisme aux fins de la LGGRI, la présidente est la première responsable de la sécurité de l'information au sein de Télé-Québec.

Elle doit principalement :

- Assurer l'application de la politique sur la sécurité de l'information;
- S'assure de l'application, au sein de la Société, des orientations, des stratégies, des politiques et autres indications d'application découlant de la LGGRI.
- Désigner, parmi son personnel d'encadrement, un chef de la sécurité de l'information organisationnelle (ci-après « **CSIO** »), soit le vice-président des technologies, du numérique et des opérations
- Nommer des répondants en matière de sécurité de l'information, pour des domaines spécifiques en matière de sécurité de l'information, à la demande du chef gouvernemental de la sécurité de l'information (ci-après « **CGSI** »).
- Définir, au besoin, des responsabilités ou des privilèges spéciaux en matière de sécurité de l'information;
- S'assurer que l'ensemble des responsabilités en matière de sécurité de l'information sont attribuées à des responsables désignés.

4.4 Le comité de gestion de l'information, de la sécurité de l'information et de la protection des renseignements personnels (ci-après « comité GISIPRP »)

Le Comité GISIPRP est chargé de voir à l'encadrement de la sécurité de l'information. À ce titre, il a notamment pour fonctions :

- D'être porteur des meilleures pratiques en matière de sécurité de l'information;
- De s'assurer de la mise en œuvre de plans d'action en matière de sécurité de l'information et, à la demande du CSIO, participer à la réflexion guidant l'élaboration de tels plans;
- En collaboration avec les gestionnaires des différents secteurs de la Société, de contribuer à l'opérationnalisation et à l'application des politiques, directives et autres documents connexes en matière de sécurité de l'information, notamment :
    - En s'assurant de la formation du personnel en matière de sécurité de l'information;
    - En tenant compte de la rétroaction des gestionnaires quant aux pratiques de

leurs équipes en matière de sécurité de l'information.

- D'être informé de tout événement ayant pu mettre en péril la sécurité de l'information et, lorsque pertinent, de recommander et de s'assurer de la mise en place de solutions appropriées.
- De s'assurer que l'évaluation du niveau de criticité des Actifs informationnels est régulièrement mise à jour.

4.5 Le vice-président des technologies, du numérique et des opérations

Le vice-président des technologies, du numérique et des opérations assume le rôle de Chef de la sécurité de l'information organisationnelle (CSIO) et représente la présidente-directrice générale en matière de gestion et de coordination de la sécurité de l'information. À ce titre, il doit principalement

- Assumer la responsabilité de la prise en charge globale de la sécurité de l'information au sein de la Société et assurer le lien avec les répondants gouvernementaux en la matière, en leur assurant la collaboration de la Société;
- Assister la présidente-directrice générale dans la détermination des orientations stratégiques internes et des priorités d'intervention;
- Piloter les fonctions relatives à la sécurité de l'information au sein du Comité GISIPRP;
- Représenter la Société en matière de sécurité de l'information.

En tant que responsable de la continuité des services, il doit également :

- Coordonner l'élaboration du plan de continuité des services, veiller à sa mise en œuvre et en assurer la mise à jour;
- Assurer la planification et la coordination des tests initiaux et récurrents;
- Assurer les liens avec tout comité de crise ad hoc et constitué afin de prendre des décisions permettant à la Société de mettre en œuvre les Mesures nécessaires pour contenir les effets négatifs d'une crise et de la résoudre dans les meilleurs délais afin de permettre un retour à la normale des activités.

4.6 Le directeur de l'informatique, de l'infrastructure et de la cybersécurité

Le directeur de l'informatique, de l'infrastructure et de la cybersécurité agit à titre de répondant (rôle de Coordonnateur organisationnel des Mesures de sécurité de l'information (ci-après « **COMSI** »)). Il est responsable de la coordination et de l'application des Mesures de sécurité opérationnelles au sein de la Société. À ce titre, il travaille en étroite collaboration avec le CSIO et doit principalement :

- Assumer la responsabilité de la coordination et de l'application des Mesures de sécurité opérationnelles au sein de la Société;
- Représenter la Société et participer activement au Réseau d'alerte gouvernemental, coordonné par l'Équipe de réponse aux incidents de sécurité de l'information de l'Administration québécoise (CERT/AQ);
- Identifier les menaces, vulnérabilités et incidents touchant la Société, en tenir informé le

CSIO de la Société et les escalader selon les conditions définies par le Processus de gestion des menaces, des vulnérabilités et des incidents (GMVI), si nécessaire;

- S'assurer de l'élaboration, de la mise à jour et de l'application d'un plan interne de réponse aux menaces, vulnérabilités et incidents;
- S'assurer de la réalisation d'analyses de risques de sécurité;
- Collaborer étroitement avec le CSIO de la Société et le responsable opérationnel de cyberdéfense (ROCD) désigné en leur fournissant, notamment, le soutien technique nécessaire à l'exercice de leurs responsabilités.

4.7 L'architecte infrastructure TI

L'architecte infrastructure TI assume le rôle de Coordonnateur organisationnel des Mesures de sécurité de l'information adjoint (ci-après « **COMSI adjoint** »). À ce titre, il supporte le COMSI et agit à titre de substitut si ce dernier n'est pas joignable ou dans l'impossibilité de jouer son rôle opérationnel.

4.8 Les gestionnaires

Les gestionnaires ont l'obligation d'assurer le respect des dispositions de la Politique de sécurité de l'information et de ses directives d'application dans leurs équipes respectives. Ils doivent s'assurer de la comprendre et de la communiquer. Ils doivent donc principalement :

- Veiller à ce que les Mesures de sécurité appropriées soient mises en place, appliquées et périodiquement vérifiées;
- Informer les utilisateurs dont ils sont responsables, des dispositions de la politique sur la sécurité de l'information et des directives, standards et 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;
- S'assurer que les Actifs informationnels dont ils sont responsables à titre de Détenteur d'actif informationnel sont utilisés en conformité avec les principes généraux et les exigences de la politique de sécurité;
- Aviser dans les meilleurs délais le vice-président des technologies, du numérique et des opérations (CSIO) ou en son absence, le directeur de l'informatique, de l'infrastructure et de la cybersécurité (COMSI) lorsqu'ils soupçonnent un utilisateur de contrevenir au cadre normatif organisationnel;
- S'assurer que la sécurité de l'information est prise en compte dans tout contrat de service attribué par l'organisation et voir à ce que tout consultant, partenaire ou fournisseur s'engage à respecter et respecte effectivement les règles de sécurité de l'information.

4.9 La vice-présidente des finances et administration

En tant que responsable de la sécurité physique, la vice-présidente des finances et administration et son directeur des ressources matérielles et immeubles, doivent:

- Mettre en place des Mesures de protection physique et d'accès pour les salles abritant les systèmes ou les installations technologiques stratégiques ou essentielles, ainsi que

les supports de stockage de l'information confidentielle;

- Concevoir et mettre en œuvre des Mesures de protection physique des biens contre les sinistres, les pertes, les dommages et le vol;
- Assurer la mise au rebut sécuritaire des supports d'information autres que numériques.

4.10 Les utilisateurs d'Actifs informationnels

Les utilisateurs d'Actifs informationnels doivent se conformer à la présente politique et aux règles qui leur sont applicables en prenant connaissance de toute directive ou autre document de nature similaire et relatif à la sécurité de l'information.

5. DISPOSITIONS FINALES

5.1 Entrée en vigueur

La présente politique entre en vigueur à la date de son adoption par le conseil d'administration.

5.2 Révision

La présente politique pourra être révisée ponctuellement selon les changements législatifs et les besoins de la Société.