POLITIQUE DE SÉCURITÉ DE L'INFORMATION

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

TABLE DES MATIÈRES

HISTORIQUE DES VERSIONS

Adoption

Instance	Date	Numéro de résolution
Conseil d'administration	2006-06-16	1732

Dernières modifications

Instance	Date	Numéro de résolution	Commentaire
Conseil d'administration	2007-11-01	1780	Révision périodique
Conseil d'administration	2010-06-18	1880	Révision afin de tenir compte de nouvelles indications gouvernementales
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

Cette politique encadre les moyens mis en place afin d'assurer la sécurité de l'information détenue par la Société de télédiffusion du Québec (ci-après la « **Société** ») tout en respectant ses obligations légales, notamment celles prévues par la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (ci-après la « **LGGRI** »).

Elle se veut souple et flexible afin que les moyens de réalisation puissent évoluer à travers le temps, permettant ainsi à la Société de s'adapter aux nombreux et rapides changements technologiques et de prévenir les menaces potentielles qui peuvent y être associées.

1. CHAMP D'APPLICATION

La présente politique 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

Dans la présente politique, à moins que le contexte n'indique un sens différent, on entend par :

Actif informationnel : Information, quel que soit son canal de communication ou son support, un système ou un support d'information, une technologie de l'information, une installation ou un ensemble de ces éléments, acquis ou constitué par la Société et ayant une valeur pour elle.

Confidentialité : Propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées.

Cycle de vie de l'information : 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 Télé-Québec.

Détenteur d'actif informationnel : Gestionnaire de la Société ou son représentant désigné à qui est assignée la responsabilité opérationnelle d'un Actif informationnel ou d'un processus d'affaires lié à cet actif.

Disponibilité : Propriété d'une information d'être accessible en temps voulu et de la manière requise par 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.

Mesure de sécurité de l'information : Moyen concret assurant, partiellement ou totalement, la protection des Actifs informationnels contre un ou plusieurs risques et dont la mise en œuvre vise à amoindrir la probabilité de survenance de ces risques, ou à réduire les pertes qui en résultent.

Renseignements personnels : Renseignements qui portent sur une personne physique et permettent, directement ou indirectement, de l'identifier. À titre d'exemple, son nom, son adresse, son adresse de courrier électronique et tout autre renseignement la concernant et permettant de l'identifier, seul ou en les combinant avec d'autres renseignements. Ils sont, par nature, confidentiels. Ils ne peuvent donc, sauf dans le cas d'exceptions particulières prévues par la loi, être divulgués sans le consentement de la personne concernée.

3. OBJECTIFS

La présente politique vise à :

- Affirmer l'engagement de la Société à s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information, quel que soit son support ou son moyen de communication;
- Établir les pratiques à adopter dans le but de se conformer aux diverses obligations légales et administratives, de protéger tous les Actifs informationnels de l'organisation ainsi que de prévenir de potentiels événements de sécurité, incluant la fraude, les fuites d'information, les attaques informatiques, les erreurs accidentelles, les actions délibérées et l'atteinte à la vie privée;
- Protéger la Société et atténuer les risques liés aux bris de Confidentialité, à la perte d'Intégrité et à l'indisponibilité de l'information.

4. CADRE LÉGAL ET NORMATIF

La présente politique est fondée sur les lois suivantes ainsi que les règlements et directives 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) ;
- Loi concernant le cadre juridique des technologies de 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-cadre sur la protection des renseignements personnels
- Politique de gestion de l'information
- Code d'éthique et de déontologie des administrateurs et dirigeants de la Société de télédiffusion du Québec
- Règles d'éthique et code de conduite du personnel de la Société de télédiffusion du Québec

5. PRINCIPES DIRECTEURS

La présente politique s'appuie sur les principes directeurs de la Directive gouvernementale sur la sécurité de l'information :

5.1 Éthique

Le processus de gestion de la sécurité de l'information doit être soutenu par une démarche éthique visant à assurer la régulation des conduites et la responsabilisation individuelle.

5.2 Évolution

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

5.3 Responsabilité et imputabilité

L'efficacité des Mesures de sécurité de l'information exige l'attribution claire des responsabilités à tous les niveaux de l'organisation et la mise en place de processus de gestion de la sécurité de l'information permettant une reddition de comptes adéquate. À ce titre, le Cadre de gestion de la sécurité de l'information de la Société se veut complémentaire à la présente politique en définissant la structure de gestion et en précisant davantage les rôles et responsabilités des principales parties prenantes.

5.4 Transparence

L'information concernant les événements de sécurité, les pratiques et les solutions de sécurité de l'information afférentes doit être communiquée avec fluidité au sein de la Société et des autorités gouvernementales, sous réserve du droit applicable.

5.5 Universalité

Les pratiques et les solutions retenues en matière de sécurité de l'information correspondent, dans la mesure du possible, à des façons de faire reconnues et généralement utilisées à l'échelle nationale et internationale.

6. MOYENS DE RÉALISATION DE LA POLITIQUE

6.1 Gouvernance de la sécurité de l'information

La Société se dote de directives, de guides et/ou de procédures afin de clarifier les attentes et expliciter les Mesures mises en place en matière de sécurité de l'information. Ces documents de gestion peuvent couvrir l'ensemble des domaines touchés, notamment les infrastructures technologiques ou physiques, la télécommunication, les processus ou activités de la Société, les solutions applicatives et les ressources humaines.

6.2 Sensibilisation et formation

La Société s'engage à sensibiliser et à former tous les employés de la Société, de même que l'ensemble des autres utilisateurs ayant un accès aux systèmes de la Société et/ou à qui la Société a créé un compte corporatif. Ce programme de sensibilisation et formation vise particulièrement la sécurité des Actifs informationnels, les conséquences d'une atteinte à leur sécurité ainsi qu'aux rôles et obligations de chacun en cette matière.

Plus précisément, la Société s'assure que :

- Toute personne visée au paragraphe précédent suivra obligatoirement, de façon continue, un programme de formation et de sensibilisation à la cybersécurité. L'objectif est de permettre aux utilisateurs d'adopter les bons comportements en matière de sécurité informatique et ainsi réduire significativement les risques de fraude, d'hameçonnage et de cyberattaque. Des rappels périodiques sont émis à ces égards.
- Les utilisateurs sont informés de leurs privilèges d'accès, des limites reliées à leurs

fonctions, ainsi que de leurs responsabilités en matière de sécurité de l'information.

Les personnes chargées de tâches précises en matière de sécurité de l'information sont formées de manière appropriée. En ce sens, la Société fournit des efforts concernant l'attraction et la rétention des talents afin d'augmenter l'attractivité et la fidélisation des expertises. De plus, la Société encourage son personnel à mettre à niveau ses compétences en continu.

6.3 Protection de l'information en amont

La Société intègre le concept de protection de l'information en amont à ses projets. Ceci permet de sécuriser les systèmes en intégrant les Mesures nécessaires dès leur conception ou leur acquisition. Ces Mesures assurent autant la protection de l'information, tout au long de son Cycle de vie, que la résilience de ses systèmes et de ses infrastructures critiques. Une attention particulière est apportée aux Renseignements personnels, notamment en effectuant une évaluation des facteurs relatifs à la vie privée tel que prévu par la Politique-cadre sur la protection des renseignements personnels.

6.4 Mesures de sécurité de l'information

La Société met en place un ensemble de Mesures de sécurité pour protéger la Confidentialité et assurer l'Intégrité et la Disponibilité de ses Actifs informationnels. Ces Mesures incluent, sans s'y limiter :

- **Contrôle d'accès:** L'accès aux Actifs informationnels est limité aux personnes qui en ont besoin pour accomplir leurs tâches et ces accès sont révisés deux fois par année.
- **Authentification et identification:** Les utilisateurs doivent utiliser la méthode de double authentification et s'identifier avant d'accéder aux Actifs informationnels de la Société.
- **Site de relève :** Les Actifs informationnels sont disponibles en permanence pour les utilisateurs autorisés et l'information qu'ils contiennent est dupliquée dans un site de relève.

Les Mesures de sécurité sont régulièrement mises à jour en fonction des normes et des bonnes pratiques en vigueur, notamment les exigences minimales émises par le ministère de la Cybersécurité et du Numérique (ci-après le « MCN ») et émanant de la collaboration de la Société avec le Centre opérationnel de cyberdéfense (ci-après le « COCD ») du ministère de la Culture et des Communications (ci-après le « MCC »). La Société effectue également des évaluations de la performance des Mesures mises en place, notamment par le biais d'audits externes et de tests d'intrusion et de vulnérabilités.

6.5 Catégorisation des Actifs informationnels

La Société reconnaît que les Actifs informationnels qu'elle détient sont essentiels à ses opérations courantes et sont en évolution. De ce fait, ils doivent faire l'objet d'une évaluation constante pour en assurer une protection adéquate.

Les Mesures de protection à mettre en place doivent être proportionnelles à la valeur établie de l'information et aux risques encourus. Ce niveau de criticité est évalué selon la Confidentialité, l'Intégrité et la Disponibilité (CID) requises et tient compte notamment d'exigences légales, réglementaires et contractuelles. Cette évaluation est faite conjointement avec les Détenteurs d'Actifs informationnels selon les directives et procédures en place et elle est consignée dans un registre à cet effet.

6.6 Droit de regard

La Société exerce, en conformité avec la législation et la réglementation en vigueur, un droit de regard sur tout usage de ses Actifs informationnels et toute information conservée, traitée et exécutée sur ses systèmes et sur ses appareils mobiles.

Afin de surveiller son exposition aux risques, elle met en place une infrastructure et des processus de surveillance afin de permettre de surveiller l'efficacité de ses méthodes, processus et mécanismes de protection de façon constante et de les améliorer en fonction de l'évolution des risques auxquels l'organisation fait face.

Elle doit donc s'assurer que des procédures de compte rendu et d'enquête relativement aux événements de sécurité soient mises en place, afin de déterminer les points faibles et d'apporter des mesures correctives, en réduisant le risque de répétition d'un événement de même nature.

6.7 Continuité des activités

La Société prévoit un ou des mécanismes de relève des composantes critiques pour assurer la prestation des services jugés prioritaires lors d'une panne informatique ou technique.

6.8 Partage et mise en commun

La Société adhère au cadre gouvernemental québécois en matière de sécurité de l'information et prône le partage et la mise en commun des connaissances, de l'expertise et des bonnes pratiques en sécurité de l'information et en cybersécurité. Pour ce faire, la Société collabore avec les autorités gouvernementales pertinentes dans une perspective de protection de l'information et de résilience des systèmes gouvernementaux.

7. RÔLES ET RESPONSABILITÉS DES PRINCIPALES PARTIES PRENANTES

La présente politique précise les rôles et les responsabilités des parties prenantes suivantes en matière de sécurité de l'information. Ceux-ci sont détaillés dans le cadre de gestion de la sécurité de l'information.

7.1 Le conseil d'administration

Le conseil d'administration approuve la présente politique, de même que le cadre de gestion de la sécurité de l'information.

7.2 Le comité d'audit

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

7.3 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 la Société.

7.4 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, dont les membres sont nommés par la présidente-directrice générale, appuie le CSIO dans l'encadrement de la sécurité de l'information au sein de la Société, comme plus amplement prévu au Cadre de gestion de la sécurité de l'information.

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

Le vice-président des technologies de l'information assume le rôle de Chef de la sécurité de l'information organisationnelle (ci-après le « **CSIO** »), dont le rôle est précisé au Cadre de gestion de la sécurité de l'information de la Société. À ce titre, il assiste la présidente-directrice générale dans la détermination des orientations stratégiques et des priorités d'intervention en matière de sécurité de l'information.

7.6 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 et assume le rôle de Coordonnateur organisationnel des mesures de sécurité de l'information (ci-après « **COMSI** »). Il est notamment responsable de la coordination et de l'application des Mesures de sécurité opérationnelles au sein de la Société. Il est appuyé dans ses fonctions par un COMSI adjoint, comme plus amplement prévu au Cadre de gestion de la sécurité de l'information.

7.7 Les gestionnaires

Les gestionnaires de la Société sont chargés de la mise en œuvre, auprès du personnel relevant de leur autorité, des dispositions de la présente politique et de ses directives d'application, comme plus amplement prévu au Cadre de gestion de la sécurité de l'information.

7.8 Les utilisateurs d'Actifs informationnels

Les utilisateurs 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.

8. SANCTIONS

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 d'accès, la réprimande, la suspension, le congédiement ou autre, et ce, conformément aux dispositions des conventions collectives, des ententes ou des contrats. Télé-Québec peut transmettre à toute autorité judiciaire les renseignements colligés et qui le portent à croire qu'une infraction à toute loi ou règlement en vigueur a été commise.

9. DISPOSITIONS FINALES

9.1 Entrée en vigueur

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

9.2 Révision

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