POLITIQUE DE SÉCURITÉ DE L'INFORMATION DE TÉLÉ-QUÉBEC

ADOPTÉ PAR LE CONSEIL D'ADMINISTRATION LE jj mm aaaa / RÉSOLUTION NO xxxx

PRÉAMBULE

La présente politique est adoptée par le conseil d'administration. Elle a été rédigée à partir du Guide d'élaboration d'un cadre normatif ministériel de sécurité de l'information du gouvernement du Québec en application de la Directive sur la sécurité de l'information gouvernementale. Cette directive détermine, entre autres, le rôle et les responsabilités du dirigeant d'organisme. Elle prévoit en effet que celui-ci devra, notamment définir clairement les valeurs organisationnelles et les orientations internes en matière de sécurité de l'information, les faire partager par l'ensemble de son personnel et les communiquer à ses partenaires pour s'assurer qu'elles sont respectées.

Cette directive gouvernementale couvre la sécurité de l'information consignée dans des documents sur différents supports – papier, CD/DVD, CD-ROM/DVD-ROM, disque dur, clé USB, carte mémoire SD ou micro SD, etc., – ou échangée directement entre deux ou plusieurs personnes par différents canaux de communication – services de messagerie électronique, téléphone analogique ou numérique, télégraphe, télécopie, etc.

Cette directive témoigne du changement d'orientation gouvernementale en matière de sécurité de l'information, puisqu'elle reflète la prise de conscience de l'importance de protéger l'information, quels que soient son support ou son mode d'expression, et de la nécessité de prendre les mesures appropriées en fonction de sa teneur, selon sa nature confidentielle ou publique, ses caractéristiques, son importance stratégique et sa valeur patrimoniale ou archivistique.

L'information détenue par la Société de télédiffusion du Québec (ci-après « Télé-Québec ») s'avère un actif dont Télé-Québec se doit d'assurer la protection, et ce, tout au long de son cycle de vie.

1. DÉFINITIONS

Actif informationnel : Une information quel que soit son canal de communication – téléphone analogique ou numérique, télégraphe, télécopie, voix, etc., – ou son support – papier, pellicule photographique ou cinématographique, ruban magnétique, 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 constitué 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 : 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.

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.

2. OBJECTIF DE LA POLITIQUE

L'objectif de la politique de sécurité de l'information est d'affirmer l'engagement de Télé-Québec 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. Plus précisément, il s'agit d'assurer, tout au long du cycle de vie de l'information, sa disponibilité, son intégrité et sa confidentialité.

Le présent document constitue la Politique de sécurité des actifs informationnels de Télé-Québec (ci-après la « Politique ») qui établit les pratiques à adopter dans le but de se conformer aux diverses obligations légales et administratives et de protéger tous les actifs informationnels de l'organisation et de prévenir de potentiels incidents 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. De cette manière, Télé-Québec protège l'organisation et atténue les risques liés à la confidentialité, à l'intégrité et à la disponibilité de l'information.

3. CHAMP D'APPLICATION

La présente politique s'adresse aux utilisateurs, 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. L'information visée est celle que Télé-Québec détient dans l'exercice de ses fonctions, que sa conservation soit assurée par elle-même ou par un tiers.

4. ÉNONCÉS DE PRINCIPES GÉNÉRAUX

4.1 Protection de l'information

4.1.1 Télé-Québec adhère au cadre gouvernemental québécois en matière de sécurité de l'information et s'engage 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 à l'échelle nationale et internationale.

4.1.2 Télé-Québec reconnaît que les actifs informationnels qu'elle détient sont essentiels à ses opérations courantes et, de ce fait, doivent faire l'objet d'une évaluation constante, d'une utilisation appropriée et d'une protection adéquate.
Le niveau de protection dont les actifs informationnels doivent faire l'objet est établi en fonction de leur importance, de leur confidentialité et des risques d'accident, d'erreur et de malveillance auxquels ils sont exposés.

4.1.3 Télé-Québec adhère également aux principes directeurs suivants :

- **Responsabilité et imputabilité** : l'efficacité de la sécurité de l'information exige l'attribution claire de responsabilités à tous les niveaux de l'organisation et la mise en place d'un processus de gestion interne de la sécurité permettant une reddition de comptes adéquate.
- **Évolution** : les pratiques et les solutions retenues en matière de sécurité de l'information doivent être réévaluées périodiquement afin de tenir compte des changements juridiques, organisationnels et technologiques, ainsi que de l'évolution des menaces et des risques.
- **Éthique** : le processus de gestion de la sécurité de l'information doit être soutenu par une démarche d'éthique visant à assurer la régulation des conduites et la responsabilisation individuelle.

4.2 Protection des renseignements confidentiels

Toute information confidentielle doit être préservée de toute divulgation, de tout accès ou de toute utilisation non autorisée ou illicite. Sont notamment considérés comme confidentiels, au sens de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, les renseignements personnels ainsi que tout renseignement dont la divulgation aurait des incidences néfastes, notamment sur les relations intergouvernementales, les négociations entre organismes, l'économie, les tiers relativement à leurs renseignements industriels, financiers, commerciaux, scientifiques ou techniques, l'administration de la justice et la sécurité publique, les décisions administratives ou politiques et la vérification.

4.3 Sensibilisation et formation

Télé-Québec s'engage 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 cette matière.

Télé-Québec doit plus précisément s'assurer que :

a. Les personnes chargées de tâches précises en matière de sécurité soient formées de manière appropriée;
b. Les utilisateurs soient informés de leurs privilèges d'accès, des limites reliées à leurs fonctions, ainsi que de leurs responsabilités en matière de sécurité de l'information et que des rappels périodiques soient émis à cet égard.

4.4 Droit de regard

Télé-Québec 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, Télé-Québec 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 incidents 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 incident de même nature.

4.5 Continuité des activités

Télé-Québec doit prévoir un mécanisme de relève des composantes critiques pour assurer la prestation des services jugés prioritaires lors d'une panne informatique ou technique.

5. RÔLES ET RESPONSABILITÉS

La présente politique précise les rôles et les responsabilités en matière de sécurité de l'information attribués aux principaux responsables de Télé-Québec, ainsi qu'aux détenteurs de l'information, aux gestionnaires d'entités administratives et aux utilisateurs.

a. Le dirigeant d'organisme : le président-directeur général est le premier responsable de la sécurité de l'information de Télé-Québec.
b. Le Responsable Organisationnel des Systèmes d'Information (ROSI): Le directeur technologie de l'information assiste le président-directeur général dans la détermination des orientations stratégiques et des priorités d'intervention et agit également à titre de président du Comité de sécurité de l'information. Il est responsable de rendre des comptes au Comité d'audit et à la direction générale de Télé-Québec
c. Le Comité de sécurité de l'information : Sa mission est de s'assurer de l'application des normes, directives et mesures qui découlent de la présente

politique en matière de sécurité de l'information. C'est le dirigeant d'organisme qui est en charge de nommer les membres de ce comité.

d. Le Conseiller Organisationnel en Sécurité de l'Information (COSI): Il est chargé de faire appliquer les mesures, vérifications et contrôles découlant du volet informatique de la présente politique, ainsi que de rendre des comptes périodiquement au Comité. Le Comité utilise les comptes rendus présentés par le COSI comme un élément essentiel pour le suivi du programme de sécurité de l'information.
e. Les propriétaires d'applications: Ils s'assurent de la sécurité de l'information qu'ils détiennent dans le cadre du processus relevant de leur responsabilité et de la sécurité des applications informatiques dont ils sont propriétaires.
f. Les gestionnaires: Ils 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.
g. Les utilisateurs: Ils doivent se conformer à la présente politique et aux règles qui leur sont applicables en prenant connaissance de la Directive pour les utilisateurs quant au respect des règles de sécurité de l'information de Télé-Québec jointe à l'annexe.

D'autres responsabilités ainsi que les structures internes de coordination et de concertation en matière de sécurité de l'information sont définies dans le Cadre de gestion de la sécurité de l'information, en complément à la présente politique.

6. OBLIGATION DES UTILISATEURS

Tout utilisateur a l'obligation de protéger les actifs informationnels mis à sa disposition par Télé-Québec. À cette fin, il doit :

a. Prendre connaissance de la présente politique ainsi que des directives, des standards, des procédures et des autres lignes de conduite en découlant, y adhérer, s'y conformer (Directive pour les utilisateurs quant au respect des règles de sécurité de l'information de Télé-Québec jointe en annexe).
b. Utiliser, à l'intérieur des droits d'accès qui lui ont été conférés et uniquement lorsqu'ils sont nécessaires à l'exercice de ses fonctions, les actifs informationnels mis à sa disposition en se limitant aux fins auxquelles ils sont destinés.
c. Se conformer aux exigences légales portant sur l'utilisation des produits à l'égard desquels des droits de propriété intellectuelle pourraient exister.
d. Au moment de son départ de Télé-Québec, remettre les différentes cartes d'identité et d'accès, les actifs informationnels ainsi que tout l'équipement

informatique ou de téléphonie qui avaient été mis à sa disposition dans le cadre de ses fonctions.

7. 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.

8. DISPOSITIONS FINALES

a. Le conseil d'administration de Télé-Québec approuve la présente politique.
b. La présente politique entre en vigueur le 30 novembre 2018
c. Le président-directeur général est chargé de la mise en œuvre des dispositions de la présente politique et de ses directives d'application.
d. Le secrétaire général doit effectuer la surveillance active du plan d'actions de sécurité de l'information de Télé-Québec. Il confie au Comité de sécurité de l'information la responsabilité d'effectuer des vérifications internes. Le secrétaire général doit informer le Comité d'audit des résultats de ses vérifications.
e. La présente politique sera réexaminée une fois par année en début d'exercice financier, et ce, avant le 30 septembre de chaque année.
f. La présente politique est complétée par le Cadre de gestion de la sécurité de l'information. Les obligations qui en découlent sont précisées par des directives.

ANNEXE

Directive pour les utilisateurs quant au respect des règles de sécurité de l'information

Les utilisateurs ont l'obligation de protéger les actifs informationnels mis à leur disposition par Télé-Québec. À cette fin, ils doivent :

- Se conformer aux directives gouvernementales, à la Politique sur la sécurité de l'information ainsi qu'aux directives, aux standards, aux procédures et aux autres lignes de conduite touchant la sécurité de l'information de Télé-Québec.
- Utiliser, à l'intérieur des droits d'accès qui leur ont été conférés et uniquement lorsqu'ils sont nécessaires à l'exercice de leurs fonctions, les actifs informationnels mis à leur disposition en se limitant aux fins auxquelles ils sont destinés.
- Respecter les mesures de sécurité mises en place sur son poste de travail et sur tout équipement contenant des données à protéger; ne pas modifier la configuration des mesures de sécurité ni les désactiver; ne pas chercher à obtenir des informations touchant aux actifs informationnels dont il n'a pas l'autorisation d'accès, sur support physique ou autre.
- Se conformer aux exigences légales portant sur l'utilisation des produits à l'égard desquels des droits de propriété intellectuelle pourraient exister;
- 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 Télé-Québec; il est entendu que l'identité de l'employé qui fait le signalement sera tenue confidentielle.
- Au moment de leur départ de Télé-Québec, remettre les différentes cartes d'identité et d'accès, les actifs informationnels ainsi que tout l'équipement informatique ou de téléphonie qui avaient été mis à leur disposition dans le cadre de leurs fonctions.

Cadre de gestion
De la Sécurité de L'Information
De TÉLÉ-QUÉBEC

ADOPTÉ PAR LE CONSEIL D'ADMINISTRATION LE jj mm aaaa / RÉSOLUTION NO xxxx

Table des matières

PRÉAMBULE 3
Définitions 4
Cadre légal et administratif 4
2. RÔLES ET RESPONSABILITÉS 6
2.1 Le conseil d'administration 6
2.2 Le dirigeant d'organisme 6
2.3 Le responsable organisationnel de la sécurité de l'information (ROSI) 6
2.4 Les directeurs généraux 7
2.5 Les détenteurs d'information et responsables d'applications 8
2.6 Le Conseiller Organisationnel de la Sécurité de l'Information (COSI) 9
2.7 Le Conseiller Organisationnel en gestion des incidents (COGI) 10
2.8 Le responsable de l'éthique 10
2.9 Le responsable de la protection des renseignements personnels (RPRP) 10
2.10 Le responsable de la sécurité physique 11
2.11 Le responsable de la gestion documentaire 11
2.12 Le responsable des ressources humaines 11
2.13 Le responsable de la continuité des services 12
3 LE COMITÉ DE SÉCURITÉ DE L'INFORMATION 12
4. DISPOSITIONS FINALES 13
4.1 Date d'entrée en vigueur 13

PRÉAMBULE

Le présent cadre de gestion de la sécurité de l'information a été élaboré à la suite de la politique adoptée par le conseil d'administration le 18 juin 2010. Il décrit les rôles et responsabilités des intervenants internes officiels en la matière. Ces documents ont été rédigés à partir du guide d'élaboration d'un cadre normatif ministériel de sécurité de l'information du gouvernement du Québec en application de la directive sur la sécurité de l'information gouvernementale.

Cette directive gouvernementale détermine, entre autres, le rôle et les responsabilités du dirigeant d'organisme. Elle prévoit en effet que celui-ci devra notamment définir clairement les valeurs organisationnelles et les orientations internes en matière de sécurité de l'information, les faire partager par l'ensemble de son personnel et les communiquer à ses partenaires pour s'assurer qu'elles sont respectées.

Cette même directive couvre la sécurité de l'information consignée dans des documents sur différents supports – papier, CD/DVD, CD-ROM/DVD-ROM, disque dur, clé USB, carte mémoire SD ou micro SD, etc. – ou l'information échangée directement entre deux ou plusieurs personnes par différents canaux de communication – services de messagerie électronique, téléphone analogique ou numérique, télégraphe, télécopie, etc.

Cette même directive témoigne du changement d'orientation gouvernementale en matière de sécurité de l'information, puisqu'elle reflète la prise de conscience de l'importance de protéger l'information, peu importe son support ou son mode d'expression. Cette directive reflète également la nécessité de prendre les mesures appropriées en fonction de sa teneur, selon sa nature confidentielle ou publique, ses caractéristiques, son importance stratégique et sa valeur patrimoniale ou archivistique.

L'information détenue par la Société de télédiffusion du Québec (ci-après « Télé-Québec ») s'avère un actif dont elle se doit d'assurer la protection, et ce, tout au long de son cycle de vie.

Définitions

Cadre normatif de sécurité de l'information : Cadre normatif composé de la politique, du cadre de gestion, des directives, des guides et des procédures qui s'appliquent à Télé-Québec en matière de sécurité de l'information.

Détenteur : Personne de l'organisation à qui est assignée la responsabilité de la sécurité d'un actif informationnel ou d'un processus d'affaires.

Information numérique : Terme qui fait référence au stockage de l'information sur un support numérique.

Mesure de sécurité : 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.

Renseignement personnel : Tout renseignement qui concerne une personne physique et permet de l'identifier. Un renseignement personnel qui a un caractère public en vertu d'une loi n'est pas considéré comme un renseignement personnel aux fins de la politique de sécurité.

Système d'information : Système constitué des ressources humaines (le personnel), des ressources matérielles (l'équipement) et des procédures permettant de recueillir, de détenir, d'utiliser, de traiter et de transmettre les éléments d'information pertinents au fonctionnement d'une entreprise ou d'une organisation (OQLF – Grand dictionnaire terminologique).

Technologies de l'information : Tout logiciel et matériel électronique ou toute combinaison de ces éléments utilisés pour recueillir, mémoriser, traiter, transmettre, protéger ou éliminer l'information numérique, ou constituant les infrastructures des télécommunications.

Cadre légal et administratif

- La politique et son cadre de gestion de la sécurité de l'information s'inscrivent principalement dans le cadre des lois, des règlements et des directives énumérés ci-après :
- Loi sur la Société de télédiffusion du Québec, R.L.Q., c. S-12-01;
- Loi sur la gouvernance des sociétés d'État, L.R.Q., c. G-1.02;
- Charte des droits et libertés de la personne, L.R.Q., c. C-12;
- Code civil du Québec, L.Q., 1991, c. 64;
- Loi concernant le cadre juridique des technologies et l'information, L.R.Q., c. C-1.1;
- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, L.R.Q., c. G-1.03;
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, L.R.Q., c. A-2.1;
- Loi sur les archives, L.R.Q., c. A-21.1 1983, c. 38, a. 1.;

- Loi sur la Bibliothèque nationale du Québec, la Loi sur les archives et d'autres dispositions législatives (Lois du Québec, 2004, chapitre 25);
- Loi sur l'administration publique, L.R.Q., c. A-6.01;
- Loi sur le ministère des Services gouvernementaux, L.R.Q., c. M-26.1;
- Loi canadienne sur les droits de la personne, L.R.C., 1985, c. H-6;
- Code criminel (L.R.C. (1985), ch. C-46), Loi à jour 2012-11-18; dernière modification 2012-11-06 ; Loi sur le droit d'auteur, L.R., 1985, c. C-42, Loi à jour 2012-11-18; dernière modification 2012-11-07;
- Règlement sur la diffusion de l'information et sur la protection des renseignements personnels, c. A-2.1, r. 02;
- Directive sur la sécurité de l'information gouvernementale, C.T. 203560 du 11 avril 2006;
- Directive concernant le traitement et la destruction de tout renseignement, registre, donnée, logiciel, système d'exploitation ou autre bien protégé par un droit d'auteur emmagasiné sur un équipement micro-informatique ou sur un support informatique amovible, C.T. 193953 du 19 octobre 1999, modifié par le C.T. 199891 du 27 mai 2003;
- Politique de gestion des documents actifs du gouvernement du Québec, C.T. 157432 du 9 juillet 1985, modifié par le C.T. 158264 du 10 septembre 1985;
- Politique de gestion des documents semi-actifs du gouvernement du Québec, C.T. 167568 du 25 mai 1988;
- Code d'éthique et de déontologie des administrateurs et des dirigeants;
- Règles d'éthique et code de conduite du personnel de la Société de télédiffusion du Québec;
- Règlement sur l'exercice général des pouvoirs;
- Règle de régie interne no 1 relative à la gestion financière;
- Politique de sécurité de l'information, juin 2010;
- Directives de sécurité de l'information

2. RÔLES ET RESPONSABILITÉS

Les principaux rôles et les principales responsabilités en matière de sécurité de l'information sont dévolus aux intervenants suivants.

2.1 Le conseil d'administration

Le conseil d'administration s'assure du respect des lois, des politiques, des règlements et des directives en vigueur. Il approuve la politique sur la sécurité de l'information et le présent cadre de gestion de la sécurité de l'information et les éléments de gouvernance qui en découlent.

2.2 Le dirigeant d'organisme

La présidente-directrice générale est la première responsable de la sécurité de l'information au sein de Télé-Québec. Elle doit principalement :

2.2.1 Assurer l'application de la politique sur la sécurité de l'information;

2.2.2 Définir les orientations internes en matière de sécurité de l'information, qui découlent des directives gouvernementales, des politiques internes de Télé-Québec et des pratiques généralement admises à cet égard;

2.2.3 Nommer un responsable organisationnel de la sécurité de l'information (ROSI), un conseiller organisationnel de sécurité de l'information (COSI), ainsi que les membres du comité de sécurité de l'information et leur attribuer les responsabilités définies par le présent cadre de gestion;

2.2.4 Nommer en début d'exercice financier et ce, avant le 30 septembre de chaque année, un conseiller organisationnel de sécurité de l'information (COSI) chargé de faire appliquer les mesures, vérifications et contrôles faisant l'objet de la politique, ainsi que de rendre des comptes périodiquement au comité de sécurité de l'information;

2.2.5 Définir au besoin des responsabilités ou des privilèges spéciaux en matière de sécurité de l'information.

2.2.6 S'assurer que l'ensemble des responsabilités en matière de sécurité de l'information sont attribuées à des responsables désignés;

2.2.7 Présenter au conseil d'administration les plans d'action et les bilans, conformément aux instructions de celui-ci.

2.3 Le responsable organisationnel de la sécurité de l'information (ROSI)

Le directeur des technologies de l'information est responsable de la sécurité de l'information (ROSI) et représente le président-directeur général en matière de gestion et de coordination de la sécurité de l'information. À ce titre, il doit principalement :

2.3.1 Assister le président-directeur général dans la détermination des orientations stratégiques internes et des priorités d'intervention;
2.3.2 Assurer la présidence du comité de sécurité de l'information;
2.3.3 Rendre des comptes au président-directeur général et au comité d'audit des travaux du comité de sécurité de l'information et de tout autre dossier pertinent;
2.3.4 S'assurer que les systèmes de l'organisation : informatiques, administratifs ou autres, tous supports confondus, auront les qualités nécessaires à une saine gestion du patrimoine informationnel et au respect des lois;
2.3.5 Représenter Télé-Québec en matière de sécurité de l'information;
2.3.6 S'adjoindre une ou des personnes ressources lorsqu'il le juge pertinent.

2.4 Les directeurs généraux

Les directeurs généraux ont l'obligation d'assurer une protection adéquate des actifs informationnels ainsi que des processus d'affaires dont ils sont responsables.

Ils doivent donc s'assurer de la mise en œuvre des dispositions de la politique de sécurité de l'information et de ses directives d'application, auprès du personnel relevant de leur autorité.

Ils doivent donc principalement :

2.4.1 Participer à l'élaboration des orientations stratégiques, des politiques, des directives et des éléments de gouvernance en matière de sécurité de l'information;
2.4.2 Veiller à ce que les mesures de sécurité appropriées soient mises en place, appliquées et périodiquement vérifiées;
2.4.3 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;
2.4.4 S'assurer de l'élaboration et de la mise en œuvre des directives, des guides et des procédures propres à leur domaine d'intervention;
2.4.5 S'assurer que les actifs informationnels dont ils sont responsables, mis à la disposition des utilisateurs, sont utilisés en conformité avec les principes généraux et les exigences de la politique de sécurité;
2.4.6 Aviser dans les meilleurs délais le directeur des technologies de l'information (ROSI) ou en son absence, le directeur général principal ou la directrice des affaires juridiques et secrétaire générale, lorsqu'ils soupçonnent un utilisateur de contrevenir au cadre normatif organisationnel;
2.4.7 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.

2.5 Les détenteurs d'information et responsables d'applications

La direction générale a nommé un propriétaire pour chaque application critique de Télé-Québec. Chaque propriétaire est l'ultime responsable de l'accès à son application; il pourra déléguer ses tâches à une personne autorisée.

Listes des applications critiques et leurs propriétaires	
Louise	Directeur des Technologies de l'information
Cindy	Directeur des Technologies de l'information et Directrice générale des ventes, créativité média et marketing
Virtuo (Finances)	Directrice générale des finances
Médi-Accès -Virtuo SM	Directrice des ressources humaines et directrice générale des finances

Listes des applications importantes et leurs propriétaires	
Inventaire Louise et budget de grille	Directrice de la grille
Productions internes	Directeur des Technologies de l'information et directeur post-production & mise en ondes
Vimbiz	Directeur des Technologies de l'information et Directrice des opérations techniques
Gestion Jules, télé-horaires, salle de presse, journalistes	Directrice générale des communications et image de marque
Numérisation (traitements des médias)	Directrice des opérations techniques et Directeur post-production & mise en ondes
Volicon	
Contrats d'embauche	Directeur des ressources humaines
Paie PC (paie des artistes)	Directrice générale des ressources financières

2.6 Le Conseiller Organisationnel de la Sécurité de l'Information (COSI)

Le conseiller organisationnel de la sécurité de l'information (COSI) soutient le ROSI en matière de gestion et de coordination de la sécurité de l'information. À cet égard, il doit :

2.6.1 Proposer au ROSI des orientations, des plans d'action et présenter des bilans;

2.6.2 Assurer la coordination et la réalisation de projets tels que les analyses de risques, la gestion des incidents, etc.;

2.6.3 Élaborer et mettre en œuvre les directives, les guides et les procédures propres à son domaine d'intervention;

2.6.4 S'assurer que les moyens et les mécanismes de sécurité informatique soient mis en place pour la protection des actifs informationnels, ainsi que le plan de secours informatique qui découle des orientations internes en matière de sécurité de l'information;

2.6.5 S'assurer de l'intégration de la sécurité de l'information dans la mise en service des systèmes informatiques;

2.6.6 Participe aux négociations des ententes de service et des contrats et formule des recommandations quant à l'intégration de dispositions garantissant le respect des exigences de sécurité de l'information.

2.6.7 S'assurer de la tenue à jour d'un registre des incidents ayant pu mettre en péril la sécurité de l'information, et en tenir informé le comité de sécurité de l'information;

2.6.8 Proposer au comité de sécurité de l'information des mesures de surveillance informatique et assurer la mise en œuvre et le suivi des mesures retenues;

2.6.9 Tenir le comité de sécurité de l'information informé de tout problème concernant l'intégrité des données, de toute interruption de service et de tout bris de sécurité de l'information numérique, ainsi que de leurs causes et des conséquences en découlant, et collaborer avec le comité à la résolution des problèmes;

2.6.10 Participer à la détermination des plans d'action et à la production des bilans de sécurité de l'information numérique;

2.6.11 S'assurer de la mise au rebut sécuritaire des supports d'information numériques et des équipements informatiques;

2.6.12 Collaborer avec le comité de sécurité de l'information à l'élaboration et à la mise en œuvre d'un programme de sensibilisation et de formation pour le personnel;

2.6.13 Prendre, en collaboration avec le responsable des ressources humaines, toute mesure de contrôle particulière convenue avec le comité de sécurité de l'information à l'égard d'un utilisateur soupçonné de contrevenir aux politiques, aux directives, aux standards ou aux procédures internes, concernant la sécurité de l'information numérique;

2.6.14 Établir et maintenir un réseau d'échange d'expertise avec les autres ministères ou organismes.

2.7 Le Conseiller Organisationnel en gestion des incidents (COGI)

Le directeur des technologies de l'information est responsable de la gestion des incidents de sécurité informationnelle. À ce titre, il doit :

2.7.1 Participer au réseau d'alerte gouvernemental dont la coordination est assurée par le CERT/AQ;

2.7.2 Être l'interlocuteur officiel de son organisation auprès du CERT/AQ;

2.7.3 Assurer la coordination de l'équipe de réponse aux incidents de son organisation, et du déploiement des stratégies de réaction appropriées;

2.7.4 Apporter au ROSI et au COSI le soutien technique nécessaire dans l'exercice de leurs responsabilités;

2.7.5 Contribuer à la mise en place du processus de gestion des incidents de son organisation.

2.8 Le responsable de l'éthique

Le directeur général principal, responsable de l'éthique, joue un rôle de conseiller en matière d'éthique. À ce titre, il doit :

2.8.1 Vérifier que les processus de gestion de la sécurité de l'information sont conformes à l'éthique, assurant ainsi la régulation des conduites et la responsabilisation individuelle;

2.8.2 S'assurer de la tenue d'une enquête interne et de la prise de mesures particulières de contrôle à l'égard d'un utilisateur, lorsqu'il a des motifs raisonnables de croire que ce dernier contrevient à cette politique ou aux directives, aux standards et aux procédures internes en découlant;

2.8.3 Évaluer avec le gestionnaire concerné l'opportunité d'imposer une sanction et la nature de celle-ci, en cas de contravention au cadre normatif de sécurité de l'information, et ce après avoir entendu l'utilisateur concerné et en tenant compte de la nature ou de la gravité de la faute commise, des dommages qui en découlent, des conséquences réelles ou potentielles pour Télé-Québec et de la récidive.

2.9 Le responsable de la protection des renseignements personnels (RPRP)

Le directeur général principal, responsable 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 au sein de Télé-Québec. Il doit :

2.9.1 Soulever au comité d'éthique et de gouvernance du conseil d'administration les problématiques et les préoccupations de sécurité eu égard à la protection des renseignements personnels ou sensibles;

2.9.2 Assurer la cohérence et l'harmonisation des interventions entre la sécurité de l'information, l'accès aux documents et la protection des renseignements personnels;

2.9.3 S'assurer de faire les recommandations de mesures particulières de protection des renseignements personnels aux directeurs généraux, à l'égard de leurs projets d'acquisition, de développement et de refonte de systèmes d'information ou de prestation électronique de services, qui impliquent l'utilisation ou la gestion des renseignements personnels;

2.9.4 Conseiller le dirigeant d'organisme sur les mesures particulières à respecter en matière de protection des renseignements personnels relatives à une technologie de vidéosurveillance ainsi qu'aux sondages recueillant ou utilisant des renseignements personnels.

2.10 Le responsable de la sécurité physique

Le directeur des ressources matérielles et immeubles, responsable de la sécurité physique, doit:

2.10.1 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;

2.10.2 Concevoir et mettre en œuvre des mesures de protection physique des biens contre les sinistres, les pertes, les dommages et le vol;

2.10.3 Assurer la mise au rebut sécuritaire des supports d'information autres que numériques.

2.11 Le responsable de la gestion documentaire

La directrice des affaires juridiques et secrétaire générale est responsable de la gestion documentaire pour les informations numériques ou non numériques, actives, semi-actives et archivées, pour tous les types de documents (audiovisuels, images, administratifs, etc.). Elle doit principalement :

2.11.1 Agir comme conseiller en gestion documentaire et, à ce titre, collaborer étroitement avec le ROSI et les détenteurs d'information, à la détermination, à la gestion, à la coordination et à la mise en œuvre des mesures de sécurité de l'information, conservées sur tout support numérique ou non numérique.

2.11.2 Assurer la conduite des projets de gestion des documents numériques ou non, à toute étape de leur cycle de vie incluant les archives, en collaboration avec tous les secteurs de la Société ainsi que les services d'exploitation technique et informatique.

2.12 Le responsable des ressources humaines

La directrice des ressources humaines doit :

2.12.1 Collaborer avec le ROSI à l'élaboration et à la mise en œuvre d'un programme de sensibilisation et de formation du personnel, sur les divers aspects de la sécurité de l'information;

2.12.2 Effectuer, à la demande du ROSI. et en collaboration avec le gestionnaire concerné, toute enquête à l'égard de tout utilisateur soupçonné de contrevenir à la politique sur la sécurité de l'information ou aux directives, aux standards et aux procédures internes en découlant;

2.12.3 Recommander au directeur général principal, responsable de l'éthique, toute mesure administrative ou disciplinaire appropriée.

2.13 Le responsable de la continuité des services

Le directeur des technologies de l'information et la directrice des opérations techniques responsables de la continuité des services, assurent la gestion et la coordination du plan de continuité des services de Télé-Québec. Plus particulièrement, ils doivent :

2.13.1 Coordonner l'élaboration du plan de continuité des services, veiller à sa mise en œuvre et en assurer la mise à jour;

2.13.2 Assurer la planification et la coordination des tests initiaux et récurrents;

2.13.3 Assurer les liens avec tout comité de crise ad hoc.

3 LE COMITÉ DE SÉCURITÉ DE L'INFORMATION

Le comité a comme mandat d'agir à titre de mécanisme de concertation et de coordination en matière de sécurité de l'information. Il a notamment pour fonctions :

3.1.1 D'entériner les directives, guides, normes et procédures qui seront élaborés en application de la politique de sécurité de l'information;

3.1.2 De s'assurer de la mise en œuvre des directives, guides, normes et procédures en matière de sécurité de l'information, qui découlent des directives gouvernementales, des politiques internes et des pratiques généralement admises à cet égard;

3.1.3 De constituer des groupes ou des comités de travail sur des questions particulières;

3.1.4 D'analyser les événements ayant pu mettre en péril la sécurité de l'information, de recommander et de s'assurer de la mise en place de solutions appropriées;

3.1.5 D'orienter et de soutenir les travaux des divers intervenants en sécurité de l'information;

3.1.6 De s'adjoindre, s'il y a lieu, toute autre personne dont l'expertise est nécessaire à l'exercice des fonctions du présent comité;

3.1.7 D’agir comme comité de crise ou de constituer un comité de crise, s’il y a lieu, à la demande du dirigeant de l’organisme;

3.1.8 D’instaurer un mécanisme d’évaluation périodique des risques et des mesures de sécurité de l’information en vigueur;

3.1.9 De s’assurer de la révision périodique des directives, guides, normes, procédures en matière de sécurité de l’information, afin de tenir compte des changements juridiques, organisationnels et technologiques;

3.1.10 S’assurer de la mise en œuvre d’un programme de sensibilisation et de formation pour les différents utilisateurs;

3.1.11 Produire les bilans et déterminer les plans d’action en matière de sécurité de l’information et s’assurer de leur mise en œuvre et suivi;

3.1.12 Rendre des comptes annuellement à la direction générale en présentant, avant le 30 septembre de chaque année, un rapport de ses activités.

4. DISPOSITIONS FINALES

4.1 Date d’entrée en vigueur

Le présent cadre de gestion de la sécurité de l’information est complémentaire à la politique sur la sécurité de l’information de Télé-Québec. Il entre en vigueur à la date de son adoption par le conseil d’administration.

N.B. Dans le texte qui précède, l’usage du masculin n’est fait que pour en faciliter la lecture.